NDSU Policy 710 Audit

Server Host Name: _______________________________

Physical Location: _______________________________

IP Address: _______________________________

MAC Address: _______________________________

Department/College _______________________________

Technical Contact: _______________________________

Purpose of Server: _______________________________

Standards:

Account Control Plan: ☐

Strong passwords/pass-phrases are used and their use enforced. Accounts on the server are unique and those that are not needed are disabled or removed. Access to data is on a need to know basis.

Patching Plan: ☐

Operating System Patches are installed in a timely fashion and given a priority. This plan also includes the application that the server is going to be using and any other 3rd party applications.

Access Controls: ☐

All servers have some network access controls enabled, capable of limiting network and Internet access to the server. The server is in a secured location with limited physical access. When possible, the applications and services will work in a non-administrative mode.

Malware Controls: ☐

Operating Systems that are historically susceptible to malware attacks have protection installed, enabled, and be able to be updated.

Logging: ☐

Operating System level and Application level events are be logged to assist in troubleshooting and forensic investigations.

Backup Plan: ☐

A plan is in place for the backup/recovery of data. Data backups should be stored in an off-site secure location.

Secondary:

Offsite Logging: ☐

Store logs in a different location or a central repository so they are not lost due to failure or breach.

Repurposing Plan: ☐

A plan is in place to ensure data protection, either physical destruction of the storage media or digital data destruction when the server repurposed or retired.

Data Encryption: ☐

Ensure that if data needs to be protected based on data classification and standards, it is encrypted both at rest and in transit.

By signing, I agree that I am responsible for the management and maintenance of this server, application, or services and that the information in this form is accurate to the best of my knowledge.

Data Encryption: ☐

Ensure that if data needs to be protected based on data classification and standards, it is encrypted both at rest and in transit.

By signing, I agree that I am responsible for the management and maintenance of this server, application, or services and that the information in this form is accurate to the best of my knowledge.

Dean/Department Chair Signature: _______________________________

Technical Contact Signature: _______________________________

Print Name: _______________________________

Print Name: _______________________________

Date: _______________________________

Date: _______________________________

Official Use Only:

Approved: ☐

Reason Denied: _______________________________

Denied: ☐

Reason Denied: _______________________________

Citso Signature: _______________________________

Date: _______________________________

VIPT Signature: _______________________________

Date: _______________________________