## NDSU Policy 710 Audit

<table>
<thead>
<tr>
<th>Server Host Name:</th>
<th>Physical Location:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IP Address:</th>
<th>MAC Address:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Department/College</th>
<th>Technical Contact:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

### 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.

- **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.

- **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.

- **Multifactor Authentication:**
  - Multifactor authentication will be used for servers handling or storing sensitive data.

---

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

---

### Official Use Only:

- **Approved:**
  - [ ]

- **Denied:**
  - [ ]
    - Reason Denied: 

- **CISO Signature:** 
  - Date:

- **VPI Signature:** 
  - Date:

---

**Vice President or Dean Signature / Print Name / Date:**

---

**Technical Contact Signature:**

---

**Director or Department Chair Signature / Print Name / Date:**

---

**Print Name/Date/Contact phone number:**