**Remedial Action Plan for Cyber Security**

1. **Does your institution maintain current versions of preventative software addressing threats from malicious code (including, but not limited to, viruses, trojans/worms, spyware, malware, and rootkits)?**
   1. Currently we only have basic antivirus and we need to add advanced protection that enforces Zero-Trust.
      1. We will purchase Morphisec Zero trust Endpoint security and install on all college owed pc’s. We estimate completion by 1 June 2022.
2. **Does your institution have a proactive program that monitors for critical security patches?****Do you have patch management procedures?**
   1. Currently we let Windows take care of it since local users had admin access.
      1. We will purchase PDQ Inventory and PDQ Deploy to manage software patching. We estimate completion by 1 May 2022.
3. **Does your institution maintain a comprehensive Information Security and Privacy Policy that is updated and enforced on a continual basis?**
   1. The Information Security Policies have been rewritten and are currently being reviewed by the President’s Cabinet.
4. **Does your institution have encryption tools to enhance the integrity and confidentiality of confidential information for each of the following:**
   1. Data at rest?
      1. All of the Desktop on campus are secured in locked offices that have key card access into the building. We rely on physical security for data at rest.
      2. Currently none of out laptops are encrypted. We will start enabling Bitlocker on all of our laptops. We estimate complication by 1 Aug 2022.
   2. Data transferred to removable media (CDs, Backup Tapes, USB Devices, etc)?
      1. We have created a policy that mandates the use of “Approved” removable media. We will procure USB drives and external hard drives that use Full-disk 256-bit AES XTS Hardware Encryption.
5. **Are you using any software / hardware that is no longer supported by the vendor?**
   1. Many of our work studies students are using Windows 7 pc’s. Those systems will be retired and we will replace them with Windows 10 PC’s from classroom replacements.
6. **Do you have multifactor authentication (MFA) in place for remote methods used to access systems and data including Remote Desktop Protocol and VPN technologies?** 
   1. E-mail/ cloud
      1. We will turning on MFA on all staff/faculty google accounts
         1. We are waiting for a directive from president’s cabinet. Once we receive the directive we will immediately force MFA. We expect to be finished by 1 Apr, 2022.
   2. Secure Shell (SSH) access to Linux servers
      1. We will disable remote “root” access and implement non-priveleged Key based access from 3 specific IP addresses. Once attached to the server we will then be able to switch user (SU) into “root”. All servers will have a different password that will be at least 14 characters long. We expect to be finished 1 Mar, 2022.
      2. Virtual Private Network(VPN) access
         1. We will be implementing MFA using OKTA on our Firewall. We expect to be finished 1 Aug 2022.
7. **Does the offline backup include your business-critical data that is less than a month old?****Can you recover all of your business critical data and systems in 10 days?**
   1. We will increase in-house backup capability to 30 days. We will be completed with this task 4 weeks after the delivery of the additional storage server.
   2. We will add Backupify Backup service for Google Apps for Education. We expect to be completed by 1 Mar, 2022.
8. **Are employees provided annual cyber security awareness training?**
   1. We will require baseline training for all employees(also on-boarding) and have monthly refresher training(3-5 min) utilizing NINJIO Cyber Security training.
      1. We will perform monthly Random Phishing test utilizing NINJIO. We will enroll folk that fail in remedial training.
9. **Do System Administrators use unique, privileged credentials when performing administrative tasks (separate from their user credentials for everyday access, email, etc.)?** 
   1. Privileged accounts
      1. Windows
         1. We will remove admin access from all local users
         2. This directive will come from the President’s cabinet and it includes everyone including faculty and VP’s. We expect to be completed with this by 1 Aug, 2022
         3. If exceptions are needed we WILL use an additional elevated user account (separate login)
      2. Domain Admin
         1. We will remove domain admin rights from all IT personnel
         2. We will require use of separate elevated account only used when needed. We will be completed with this by 1 Feb, 2022.
10. **Is there a log of all privileged accounts use for the last 30 days?** 
    * 1. We will need to utilize the Enterprise version of BitWarden to track the use of all privileged accounts.