Suggested Security Controls

Reference credit to Amber Smith, Executive Director of Information Technology and Chief Information Security Officer; Ohio Chirstian University.

These suggested enterprise security controls serve as a great starting set for any organization, not just educational institutions.

Access Controls:

- Block all Cloud Storage sites and USB/external portable drives – even for students (especially if students are not on their own network segment)
- Use Conditional Access Policies, such as geofencing - block logins from outside home-country (e.g., USA) unless implicitly allowed by user account (an alternate option is to just block those countries listed on the sanctioned list for home-country)
    - Even if a hacker gained credentials, they couldn't use them from outside the U.S. to gain access unless that user account had been exempted from the policy at the time of the login)
- Practice least-privilege/need-to-know – users only have access to what they should at the time they should have access to it.
- Conduct annual access/permissions audits – ensure only those who should have permissions still have permissions
- Control and monitor installed software through whitelists/blacklists (even installation of browser add-ons must be approved).
    - users can only install software for which they've been given whitelist permissions
    - While it doesn't stop a user from clicking on a link and going to a malicious website, entering credentials, it does help prevent them from installing items they receive
- Strong password policy: minimum 16-character passwords on all accounts – even on disabled accounts
    - Update all passwords when updating password policy - run a script to update all passwords on all disabled accounts as well, so that all accounts meet the minimum standard.

        - For instance, ensure all alumni and withdrawn student account passwords meet the minimum standard - without waiting for a log in and prompt to update their password to the new requirement. Who knows when (or if) they will log in again and those accounts are vulnerable until they meet the new standard.
    - Prohibit password reuse for 24 reiterations with minimum password age of at least one day, prohibit use of words specific to institution, user account automatically locks after 5 failed attempts, user sessions auto terminate after 15 minutes of inactivity, etc.
- Control BYOD (Bring Your Own Device) access to network resources (Microsoft Intune or equivalent product)

Access/Encryption Strategies/Solutions:

- Phishing-Resistant MFA on everything, to everything, by everyone, including to access network via VPN
- Windows Hello on all devices (biometric security feature)
- All sites require HTTPS and use the latest encryption protocols
    - Use Post-Quantum Cryptography as soon as possible
        - “Harvest Now Decrypt Later”
        - Currently able to use PQC internally, inside network
        - Waiting on Browser Community to get onboard to be able to use PQC external to network
- LAPS (Local Administrator Password Solution) on all devices (or equiv product) to prevent lateral movement
- PII (private data) is not allowed on mobile devices or mobile computing platforms
- Encryption
    - Encrypt everything that can be encrypted – using the latest encryption protocols (as important as patching)
    - BitLocker (drive encryption) on all hard drives
    - all PII (personally identifiable information) data, in transit and at rest
    - all remote access sessions – use encrypted VPN
    - all Wi-Fi connections
    - all backups and disaster recovery images

User Training/Monitoring/Controls:

- Users are our weakest link
- Monthly cybersecurity training with quiz
    - Participation is Required/Mandatory and tied to performance reviews (consequences ensures compliance/participation)
    - Collect Metrics from participation and quiz results
- Monthly phishing emails/testing with rewards for turning in a phish
- High-risk/vulnerable processes (grants, banking) or people (CFO, CEO) = additional/tighter security controls
- Insider Risk Management and Microsoft Information Protection – help prevent accidental data leakage
    - Monitors behaviors, alerts, and actions of people on the network, particularly higher risk people.
    - Sudden changes in behavior like bulk downloads of data, bulk deletions of data, accessing data not usually accessed, and all kinds of other such activities will trigger an alert for further investigation.
- **MOST IMPORTANT**: Change the culture of your institution by instilling a focus on data protection throughout entire institution, at every level, so everyone is equipped to analyze and appropriately handle any situation that falls outside their training (all activities end up being as secure as possible).

Backup/Recovery:

- Offsite backups, encrypted
- Disaster Recovery (and DRP) – offsite snapshots of all critical servers, encrypted
    - Example: snapshots of all critical servers, taken every 7 seconds, transmitted to offsite location, encrypted on both ends
- Secondary copies of backups and DR data stored in secondary off-site location(s), encrypted
- Redundancy built throughout all the systems, network, and infrastructure (as much as possible).
    - Example: two different ISPs coming into campus in case one goes down, two campus cores with automatic failover in case one goes down, etc.
    - Think through scenarios: What would happen if this went down? What could I do to reduce (or even eliminate) the impact of that? For instance, campus staff have never noticed the loss of one ISP because traffic automatically shifts over to the other. What

can you do around your campus to build this kind of redundancy into your systems (just little by little, over time)?

- Departmental continuity plans (especially around student processing) – each department submits their own continuity plan that has aspects incorporated into the larger institutional BCP.
- Institutional Business Contingency Plan and Disaster Recovery Plan
- Incident Response Plan/Team with regular training, exercises, and drills
- Perform a Business Impact Analysis/Assessment (BIA) and base your Incident Response Plan (IRP), Business Contingency Plan (BCP), and Disaster Recovery Plan (DRP) on the findings of your BIA.

Security Tools:

- Web and Email filtering (catch most of the bad stuff before it enters the network)
- Install all the various Microsoft Defenders and all other Microsoft security products/tools available with licenses on all devices – have them feeding back into Microsoft Sentinel (or other SIEM)
    - Attack Surface Reduction Policies, External Attack Surface Management, Microsoft Purview, Threat Intelligence, anti-malware, anti-phishing, anti-spam, Safe Links, Safe Attachments, etc.
- Data Loss Prevention Policies (in Microsoft Purview)
    - Sensitivity Labels – data classification is required
        - Sensitivity labels in Microsoft with Data Loss Prevention policies can help with data classification.
        - Each label can be associated with a policy that will control what happens with each “classification” or label.
        - Best practice is to enforce/require their use (or else they won’t be used) and to have the most restrictive labels set to automatically encrypt files/emails
    - Records Retention Labels – assists in Records Reduction policies and procedure efforts
        - Records reduction practices reduce attack surface, exposure, and financial impact
        - Due to the value of student data to hackers, this is incredibly important. Any inactive records should be archived off the network, so they are no longer accessible.
            - Number of records in one swipe
            - “clean” histories (esp with K-12)

        - Multiple victims per record (data of student, parents, step-parents, grandparents, siblings, anyone allowed to pick up the child, etc.).
        - Then you also have medical information, employment information of the parents, etc.
    - The RISK surrounding this data is incredibly high, so records reduction is even more important in Academia than almost any other industry, especially knowing that educational institutions are disproportionately represented when it comes to data breaches.
    - While “Records Retention” in Microsoft Purview can help with tracking and deletion reminders on files that have been assigned a Records Retention label, other more complex steps may need to be taken to do a bulk archive of old records (such a writing a script to archive those to another off-network system).

Network/Infrastructure Security:

- Implement network segmentation to manage network risks (ex: students on separate network from faculty/staff)
- Microsoft Intune/MDM to control what happens on devices
    - Control BYOD access to network
    - Company Portal app (controlled by Intune)
        - Staff/Faculty required to install app in order to access network resources from personal devices. Institutions control what network resources are available on personal devices through the app.
        - Company data stored on separate containers from personal data. Institutions have no access to personal data, only institutional data/resources inside the container stored on personal devices.
        - Allows Institution to remotely wipe container from lost/stolen device. Also allows institutions to do a factory reset on the device if the user requests such.
- All servers that can go behind VPN should be behind VPN – reduce external IP addresses/direct access as much as possible (then require MFA for authentication of VPN access).
- Ensure all systems/software/devices are patched ASAP
    - Security patches are applied immediately, others are scheduled according to their criticality
- Replace old devices before they reach EOL (an unpatched device is a vulnerable device). Most hackers make their way into networks through unpatched or EOL devices (that are unpatched by definition).

- Regular (weekly/monthly) vulnerability scans and Pentesting allow for quick remediation or mitigation and staying on top of vulnerabilities
- Annual third-party Vulnerability Assessment, Pentest, and At-Risk Assessments (required by regulation and provides outside perspective)
- Continuous network monitoring – that triggers an alert on any detected issues
- Halcyon agents on all devices for ransomware resilience
    - Automated encryption key capture – automatically captures encryption keys when something is encrypted, so it captures the encryption key used as part of any ransomware attempt, making paying any ransom mute since we can decrypt our own data using the key they used to encrypt it.
    - Prevents disabling security controls – which is the first thing a hacker does when gaining access to a system.
    - Monitors workload increases – any workload increases at odd times, like 2am on a holiday weekend, will trigger an alert for us to investigate. Why has this one device suddenly spiked up some activity in the middle of the night?
- Continue to improve network/infrastructure
    - Learn more:
        - Read articles, join groups, follow cybersecurity channels, watch YouTube videos, etc.
        - Read through the NIST publications referenced in the “NIST References” document (published to the website along with this one)
        - Attend webinars/seminars/conferences/summits to increase knowledge
    - Apply everything learned:
        - Is my network able to withstand this sort of attack? How would we be able to handle this?
        - If the answer is not favorable, figure out what you can do to fix it or what you can apply to mitigate/remediate/reduce the risk or impact of such an attack.
    - Great starting places to begin learning about cybersecurity and controls:
        - NIST 800-100
        - NIST 800-12

Policies, Practices, and Documentation:

- Documentation (you can’t protect what you don’t know you have):

        - Inventories with classifications on all data, devices, software, and vendors (complete with details of each, such as criticality, contact information, security controls implemented/or not, etc.)
        - Maps, diagrams, and data flows of all systems (and the network as a whole) – document as much as you possibly can.
        - Build detailed data-flow diagrams of the data-flows between specific systems (such as which fields are transferred between two systems that sync data multiple times a day – like your SIS to your LMS). Document these details, which fields, when the syncs occur, how they occur, etc.
            - Know where your data is and where it's going (especially your PII or proprietary data)
- Policies, procedures, standards, plans, and other documentation
    - Based on GLBA, FIPS, NIST, and others specific to Higher Education
    - Cyber-insurance, auditors, and regulators want to see these formalized in writing and published.
- Learn and practice Zero-Trust
- Microsoft Purview Compliance Manager – assists with managing compliance to selected framework(s)
    - Microsoft Priva - assists with finding PII in your network based upon the applied frameworks and templates. Also allows automatic handling based upon what it finds. It's a great tool to quickly get control of the years of files stored on the network (the wild west of data stored without protection), but tread lightly with its application. Very powerful, should be used carefully.
    - Records Retention controls found in Microsoft Purview
    - Security Labels and data loss prevention policies also found here

Third-Party Risk Management is Essential:

- Contracts: everything needs to be detailed.
    - Know who is responsible for what (roles and responsibilities) for outsourced activities, like building rentals, OT/IoT systems, etc.
    - If it isn't in the contract, it doesn't exist should there be an issue, so make sure everything is detailed, up front, in writing.
- **MOST IMPORTANT TO NOTE**: You are responsible for what your vendors do with your data!

- So, make sure that you are working with someone who will care about your data the same way you do.
- Know what happens with your data once the contract is over. Make sure that is included/detailed in the contract. Have a way to confirm that has occurred.
- You are not relieved of duty just because you've outsourced your data processing to someone else. Their security controls could be the weakest link in your chain, so it's up to you to ensure that isn't the case.
    - Perform a HEKVAT analysis and/or review SOC2 or other reports they're willing to share. Their "willingness to share" is "telling" in itself.
    - Interview/talk to their IT/Security team (not their salesperson) in detail about their security controls, etc.
    - Check their references:
        - Don't just collect references but actually make calls and have conversations with these references.
        - Don't be afraid to ask for more references if you feel you haven't gathered enough information.
    - Always remember why you are doing this.
    - Make sure you feel fully confident in them before you make the decision to hand over access to your most precious assets.