MICROSOFT 365
SECURITY SUGGESTIONS

The following suggestions are intended to provide ideas on improving the overall security of your instance of Microsoft 365. Some of these suggestions will also work on more traditional Microsoft Exchange Systems. The list is not intended to be comprehensive, there are other controls not included here. As an example, Microsoft has a tool that will evaluate your Microsoft 365 risks and provide control suggestions. You can find that tool here: https://security.microsoft.com/securescore/. The Center for Internet Security (CIS) also provides system hardening guidelines and is a great resource in improving security: www.cisecurity.org.

Suggested Controls:

- ✓ Secure user accounts
  - Enable multi-factor authentication (MFA) for all accounts
  - Enable strong password settings
    - We encourage 14 characters, complex, changed every 90 days
  - Disable user's ability to authorize third-party app's access to Microsoft 365 information
    - Prevents users from accidentally allowing malicious applications that, once authorized, can access user emails and data, even after their credentials are changed
  - Restrict access to specific devices or locations (Conditional Access)
    - IP whitelist
    - AD or Azure AD domain-joined machines only
    - Devices enrolled in mobile device management (MDM)
- ✓ Enable audit logging in the Microsoft 365 Defender portal
- ✓ Enable alert policies in the Microsoft 365 Defender portal (examples below)
  - Alert when a user or admin creates an email forwarding/redirect rule
  - Alert when an admin starts or exports an eDiscovery search
  - Alert when a user is assigned elevated Exchange admin permissions
  - Alert when a malware campaign is detected, or a large amount of email is reported as phishing
  - Alert when a user externally shares or deletes a large number of files in a short period of time
  - Alert when an external user performs a large number of activities on files shared with them
- ✓ Enable alert policies in Microsoft Defender for Cloud Apps (examples below)
  - Impossible travel
  - Activity from infrequent country
  - Activity from known anonymous IP addresses (proxy servers)
  - Activity from suspicious IP addresses
  - Unusual user or administrative activities
  - Multiple failed login attempts

- ✓ Configure threat management policies in the Microsoft 365 Defender portal
  - Anti-spam rules
    - Enabled SPF hard-fail and filtering email by language/geo IP
    - Increase bulk mail sensitivity
  - Anti-malware rules
  - Anti-phishing rules
    - Enable protection for all domains / users
    - Enable safety tips
  - Safe attachments and Safe Links rules
- ✓ Prevent data loss
  - Data loss prevention (DLP) rules in the Microsoft Defender for Cloud Apps
    - Alerts and/or prevents emailing and sharing of documents containing sensitive information
  - Mail flow rules in the Exchange Admin Center
    - Create a rule to prevent external email forwarding/redirection (you can whitelist specific addresses)
  - Data retention rules in the Microsoft Defender for Cloud Apps
    - Preserve deleted email and files for X number of days
  - Restrict external sharing from OneDrive, SharePoint and Exchange
    - Disable anonymous external sharing, limit sharing to specific external domains, or disable it entirely
    - Require external shares to expire after X days or prevent external editors from sharing with additional users
  - Restrict guest access to Teams to specific domains
  - Encrypt sensitive emails and documents using Microsoft Purview Message Encryption
- ✓ Improve email deliverability and help external recipients determine if emails were legitimately sent by your organization
  - Sender Policy Framework (SPF)
    - DNS record instructs recipient servers what IP addresses legitimate email can originate from
  - Domain Keys Identified Mail (DKIM)
    - Enable DKIM signing the Microsoft 365 Defender portal
    - DNS record gives recipient servers a key that all legitimately received email should be signed by (enforcement requires a DMARC record)
  - Domain Message Authentication Reporting & Conformance (DMARC)
    - Requires both SPF and DKIM to be properly configured
    - DNS record instructs recipient servers how to handle spoofed email purporting to be from your organization and how such incidents can be reported to you
  - Verify these DNS records exist and are following RFCs (internet standards) by using SPF/DKIM/DMARC record checkers
- ✓ User education and notifications
  - Enable email banners for messages originating from outside the organization
  - Train users on security controls and phishing scenarios using a tool like KnowBe4