Sample Security Implementation List – Identity and Email

Azure Active Directory

- Administrator access set up
- Create standard groups
- Configure allowed MFA methods
- Configure Azure AD Connect (if hybrid)
- Create Conditional Access Policies
    - Require MFA for all Admins
    - Require MFA for all users
    - Require MFA for Azure management
    - Block legacy authentication
    - Require MFA for enrollment of devices to Azure AD (disabled)
    - Restrict guest access
    - Block persistent browser sessions for admins
    - Require managed device compliance (disabled)
    - Require approved apps for mobile devices (disabled)
    - Secure security info registration (disabled)
- Set passwords to not expire
- Configure collection of AAD logs
- Allow only admins to register 3rd party applications
- Enable self-service password reset (SSPR)

Microsoft Teams

- Eliminate option for external participants to remote control computer
- Eliminate option for anonymous users to start meetings and not allow automatic admittance
- Block Skype usage
- Block 3rd party file storage options
- Only allow meeting organizer to record meetings

Microsoft Exchange

- Disable automatic forwarding to external domains
- Configure email authentication records (SPF, DKIM, and DMARC)
- Disable SMTP
- Restrict calendar and contact sharing

- Apply external sender warnings to incoming emails
- Disable IP allow lists
- Configure mailbox auditing

SharePoint Online

- Set file and folder default sharing to Specific People
- Set external sharing to New and Existing Guests

OneDrive

- Turn off anyone links

Microsoft 365 Defender

- Configure security alerting
- Set attachments to be scanned for malware
- Set link protection
- Set attachment filtering by file type
- Set zero-hour auto purge for malware
- Set phishing protection
- Set inbound anti-spam protection
- Set safe link policies
- Set safe attachment policies