Saltmarsh Top Office 365 Security Implementations

The following list is our recommendations for providing the best basic security for Office 365 in the cloud. An additional spreadsheet is provided with this list which will have all of Microsoft's current security options to apply to Office365 based on the security score site. These are recommendations and you will need to evaluate if some or all these recommendations fit well in our client's business processes. Although we highly recommend implementing this list as a basic best practice for Office 365 in all cases.

If you are not already familiar with the Microsoft Security Score and how to utilize it to deploy security best practices, here is the link to the recommendations from Microsoft for the first 30, 60, and 90 days and beyond for rolling out Office 365 Security. This is a recommended reading:
https://docs.microsoft.com/en-us/office365/securitycompliance/security-roadmap

Although Microsoft's Security Roadmap is a great document to follow, Saltmarsh has decided on the following as the top priority security settings for our clients:

1. Turn on audit logging for Office 365 – Mandatory
   a. How to UI: https://support.microsoft.com/en-us/help/4026501/office-auditing-in-office-365-for-admins
   b. How to Power Shell and other information about Audit logging: https://docs.microsoft.com/en-us/office365/securitycompliance/turn-audit-log-search-on-or-off

2. Require MFA for Azure AD privileged roles – Mandatory
   a. How to: https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-require-mfa
   b. Additional reading: https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-admin-roles-secure
   c. Where to go: https://portal.azure.com/#blade/Microsoft_AAD_IAM/ConditionalAccessBlade/Policies

3. Require MFA for all users – Highly Recommended
   a. Options for MFA: https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-userstates
   b. Basic How to: https://docs.microsoft.com/en-us/office365/admin/security-and-compliance/set-up-multi-factor-authentication?view=o365-worldwide
   c. Powershell setup option: https://blogs.technet.microsoft.com/office365/2015/08/25/powershell-enableenforce-multifactor-authentication-for-all-bulk-users-in-office-365/
   d. NOTE – Consult with a Project Manager or Lead IT Consultant before deploying MFA.

4. Remove remote powershell from O365 – Mandatory
   see https://www.petri.com/managing-remote-powershell-access-exchange-online

5. Disabled/block legacy email protocols or make sure they are limited to specific users/accounts
   a. Make sure you consult with a senior tech and the client before implementing and you know all the implications to disabling legacy protocols.
   b. block older Microsoft Office clients and protocols including POP, IMAP, SMTP and others that includes ACS
   c. Some scan to email systems may require legacy protocols to be enabled for MFP/printer/copiers/scanners. And there may be other applications that require legacy SMTP authentication. In this case a special account/user should be setup and the legacy protocol limited to that account.

   d. How to: https://blogs.technet.microsoft.com/cloudready/2018/11/21/part-16-disable-office-365-legacy-email-authentication-protocols/

6. Apply Data Loss Prevention Policies- Recommended for most clients, Mandatory for Clients that must meet Compliance regulations
   a. How to Create DLP from a template to meet compliance: https://docs.microsoft.com/en-us/office365/securitycompliance/create-a-dlp-policy-from-a-template
   b. How to Create DLP policies in general: https://docs.microsoft.com/en-us/office365/securitycompliance/create-test-tune-dlp-policy
   c. Security and Compliance Center insight-Driven creation option: https://docs.microsoft.com/en-us/office365/securitycompliance/get-started-with-dlp-policy-recommendations

7. Designate more than one and less than 5 global admins -Mandatory in most cases
   a. read this: https://docs.microsoft.com/en-us/office365/enterprise/protect-your-global-administrator-accounts
   b. make changes here: https://portal.office.com/AdminPortal/Home#/users

8. Set Passwords to expire – Highly Recommended
   a. Consult with client for time frame – 180 days should be best with MFA enabled.
   b. Read Microsoft Password Guidance and provide to client for policy guidance: https://www.microsoft.com/en-us/research/wp-content/uploads/2016/06/Microsoft_Password_Guidance-1.pdf
   c. Enable Password Hash Sync if hybrid - https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnectsync-implement-password-hash-synchronization#enable-password-hash-synchronization and also read more here: https://www.petri.com/how-to-secure-hybrid-office-365-authentication
   d. If a client insists on setting passwords to not expire, MFA is mandatory

9. Enable policy to block legacy authentication - Highly Recommended
   a. Read: https://techcommunity.microsoft.com/t5/Azure-Active-Directory-Identity/Azure-AD-Conditional-Access-support-for-blocking-legacy-auth-is/ba-p/245417 concerning the affect for older programs like Outlook 2010.
   b. How to: https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/block-legacy-authentication

10. Turn on sign-in risk policy- Highly Recommended
   a. How to: https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-sign-in-risk-policy

11. Turn on user risk policy- Highly Recommended
   a. How to: https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-user-risk-policy

12. Enable self-service password reset- Highly Recommended
   a. How to: https://docs.microsoft.com/en-us/azure/active-directory/authentication/quickstart-sspr
   b. https://outlook.office365.com/ecp/?Realm=%tenantdomain%exsvurl=1mkt=en-USrfr=Admin_o365

Other security considerations for Office 365 security roll out:

1. O365 Anti-Phishing prevention-
   a. https://blogs.technet.microsoft.com/cloudready/2018/07/31/introduction-email-phishing-protection-guide-enhancing-your-organizations-security-posture/ - This Technet blog has a wealth of information about how to apply security to Office365 most of which are mentioned above and in this section. The last part of the article provides links to a 2018 training course from Microsoft Ignite.

2. Delete/block accounts not used in last 30 days- Good Practice –
   a. https://github.com/OfficeDev/O365-InvestigationTooling/blob/master/InactiveUsersLast90Days.ps1

3. Do not use mail forwarding rules to external domains- Good Practice–
   a. Requires additional consult with the client before rolling out. Why this is important: https://blogs.technet.microsoft.com/office365security/mitigating-client-external-forwarding-rules-with-secure-score/
   b. How to: https://blogs.technet.microsoft.com/exchange/2017/12/22/the-many-ways-to-block-automatic-email-forwarding-in-exchange-online/

4. Set up Office 365 ATP Safe Attachment policies- Do this if O365 licenses allow it- https://protection.office.com/#/safeattachment

5. Set up Office 365 ATP Safe Links to verify URLs- Do this if O365 licenses allow it- https://portal.office.com/AdminPortal/Home?switchtomoderndefault=true#/catalog

6. Use Cloud App Security to detect insider threat, compromised account, and brute force attempts - https://portal.cloudappsecurity.com/#/alerts?resolutionStatus=eq(i:0,)&risk=eq(i:0,)

7. Setup Azure Sentinel and configure alerts –
   a. This will possibly require an additional purchase of storage space in Azure so it may not suite your environment, but the new Sentinel part of the Azure portal provides for a central collection of logs that will be analyzed for the purpose of setting alerts. https://docs.microsoft.com/en-us/azure/sentinel/