# Office 365 Security Guide.

1. Establish main tenant administrator with strong password and MFA.
2. Enable/Verify that modern authentication is enabled.
3. Setup tenant profile with organization information: https://admin.microsoft.com/AdminPortal/Home#/companyprofile
4. Configure Account Recovery Options: https://aka.ms/ssprsetup
5. Grant Delegated Admin to CSP (if MS Partner)
6. **Configure Tenant alerts email addresses**
   Set-AzureADTenantDetail -SecurityComplianceNotificationMails "alerts@domain.com" -TechnicalNotificationMails "alerts@domain.com" -MarketingNotificationEmails "alerts@domain.com"

7. **Enable Unified Audit Logging**
   Set-AdminAuditLogConfig -UnifiedAuditLogIngestionEnabled $True

8. **Enable Mailbox Audit Logging**
   $AuditSettings = @{
   AuditEnabled = $True
   AuditLogAgeLimit = 365
   AuditOwner = "Create,HardDelete,MailboxLogin,Move,MoveToDeletedItems,SoftDelete,Update,UpdateCalendarDelegation,UpdateFolderPermissions,UpdateInboxRules"
   AuditDelegate = "Create,FolderBind,HardDelete,Move,MoveToDeletedItems,SendAs,SendOnBehalf,SoftDelete,Update,UpdateFolderPermissions"
   AuditAdmin = "Copy,Create,FolderBind,HardDelete,Move,MoveToDeletedItems,SendAs,SendOnBehalf,SoftDelete,Update,UpdateCalendarDelegation,UpdateFolderPermissions,UpdateInboxRules"
   }

   Get-Mailbox | Set-Mailbox @AuditSettings

8. **Set Language and Time Zone for All Users**
   Get-Mailbox | Get-MailboxRegionalConfiguration | ? {$_.TimeZone -eq $null} | Set-MailboxRegionalConfiguration -Language 1033 -TimeZone "Central Standard Time"

9. **Increase Deleted Item Retention from 14 to 30 Days**
   Get-Mailbox -ResultSize unlimited | Set-Mailbox -RetainDeletedItemsFor 30

10. **Show MailTip for External Recipients**
    Set-OrganizationConfig -MailTipsExternalRecipientsTipsEnabled $True

11. **Show MailTip for Large # of Recipients (Shows tip Beyond threshold)**
    Set-OrganizationConfig -MailTipsLargeAudienceThreshold 10

12. **Outbound Spam Notifications**

a. Set-HostedOutboundSpamFilterPolicy Default -NotifyOutboundSpam $true -NotifyOutboundSpamRecipients “alerts@domain.com”

13. **Prevent Inbox Rules Forwarding Messages Externally**

    a. Set-RemoteDomain Default -AutoForwardEnabled $false

14. **Prepend Disclaimer on External Messages**

```
$TransportSettings = @{
        Name = 'External Sender Warning'
        FromScope = 'NotInOrganization'
        SentToScope = 'InOrganization'
        ApplyHtmlDisclaimerLocation = 'Prepend'
        ApplyHtmlDisclaimerText = "<p><div style='border:solid #9C6500
1.0pt;padding:2.0pt 2.0pt 2.0pt 2.0pt'><p class=MsoNormal style='line-
height:12.0pt;background:#FFEB9C'><b><span style='font-
size:10.0pt;color:#9C6500'></span></b><span style='font-
size:10.0pt;color:black'>[EXTERNAL]<o:p></o:p></span></p>"
        ApplyHtmlDisclaimerFallbackAction = 'Wrap'
}

New-TransportRule @TransportSettings
```

15. **Increase OneDrive Deleted User Retention** (up to 3650 days)
    Set-SPOTenant -OrphanedPersonalSitesRetentionPeriod 180

16. **Disable IMAP / POP Protocols**

    a. # Current Users
    Get-CASMailbox -Filter {ImapEnabled -eq "true" -or PopEnabled -eq "true" } | Select-Object @{n = "Identity"; e = {$_.primarysmtpaddress}} | Set-CASMailbox -ImapEnabled $false -PopEnabled $false

    b. # Future Users
    Get-CASMailboxPlan -Filter {ImapEnabled -eq "true" -or PopEnabled -eq "true" } | set-CASMailboxPlan -ImapEnabled $false -PopEnabled $false

17. Restrict inbound mail to Office 365 from only your external spam filters (prevent bypassing your spam filters)
    a. Proofpoint:
    https://support.proofpointessentials.com/Knowledgebase/Article/View/340
    b. Barracuda:
    https://campus.barracuda.com/product/essentials/doc/53674931/restrict-inbound-mail-to-the-barracuda-email-security-service-ip-range

18. Have an Office 365 Backup Policy in place.

19. Enable DKIM and DMARC

20. Setup Anti-SPAM and Anti-Phishing policies

21. Use email encryption

22. Setup Alert Polices. (Creation of forwarding/redirect rule, permissions changes, Unusual volume of external file sharing etc)

23. Use MDM for all mobile devices that store company data.

24. Use Rights Management.

25. Setup compliance reviewers for eDiscovery and Supervision.

26. DLP Policies:
    a. Setup External Sharing Polices
    b. Define what data is important (SSN, CC, Health Records, Salaries, Account #s, PST MSG etc)
    c. Create notifications when users share external data based on your defined criteria.
    d. Take it to the next level in your policy and prevent data from being sent that matches the criteria.

27. Secure SharePoint with multiple doc libraries.

28. Always use group level permissions. Use custom permission levels. (i.e. edit but not delete)

29. Disable anonymous guest link sharing

**Azure AD Notes** (Some features may require advanced licensing like Azure AD Premium P1)

- Enable Group-Based Licensing to automatically assign O365 Licenses based on AD group
- Branding: Customize logos and colors to provide a branded and recognizable logon experience. Train users to not enter their password if they don't see the branding
- MFA: Enable MFA for all users
- Trusted IPs: Configure trusted IPs to bypass MFA for the office; This will ease resistance to the MFA burden for end users
- Review Secure Score and work to increase it: https://securescore.office.com/
- Use Conditional Access to prevent all access from outside your country (be sure to exclude an account as a safety measure against accidentally locking yourself out of the whole tenant)

**Reporting Audits (PowerShell)**

- LicenseReconciliationNeeded (Mailboxes at risk of being deleted due to lack of license)
- Tenants with more licenses than consumed (wasting money)
- Users without MFA Enabled/Enforce