SWISS INFOSEC

M365 Security Checklist

Inhalt

Microsoft 365

30.06.2025, Version 1.0

1. General information

The measures listed in this document are not exhaustive, as organisational circumstances, compliance re-quirements and contractual regulations must be taken into account in addition to technical aspects. How-ever, if you implement the points described here, you will create a solid foundation for the basic protec-tion of your Microsoft 365 environment.

2. Organisational measures

Microsoft 365	**Consideration of CSPM (Cloud Security Posture Management) and resource planning**
Rationale	Continuous monitoring and maintenance of the Cloud Security Posture Management (CSPM) components is required to ensure a consistently high security and compliance posture in the Microsoft 365 environment.
Recommendation	The tools used, in particular Microsoft Secure Score, Microsoft Defender for Cloud and the Compliance Manager, must be evaluated regularly so that identified vulnerabilities are prioritised and appropriate measures are implemented promptly.
Config	N/A
Reference	https://learn.microsoft.com/en-us/azure/defender-for-cloud/concept-cloud-security-posture-management

Microsoft 365	**Roles and authorisation assignment**
Rationale	Global administrator rights in Microsoft 365 represent the highest level of authorisation and must be assigned in a strictly controlled manner. In addition, the handling of all other administrator roles must also be carefully organised, as each administrative role entails extended rights over certain services or areas of the environment. Uncontrolled or unjustified assignment of such roles increases the risk of misconfigurations, data loss or security incidents.
Recommendation	Familiarise yourself with the Entra ID roles available as standard (e.g. User Administrator, Exchange Administrator or Global Administrator). Define which Entra ID roles are required in which business units (e.g. the helpdesk has to manage users and is therefore assigned the User Administrator role). The number of global administrators should be limited to the necessary minimum - Microsoft recommends a maximum of two to four.
Config	N/A
Reference	https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference

Microsoft 365	**Secure assignment and verification of administrator rights**
Rationale	Administrator groups, especially those with global rights, pose a high security risk if they are not checked regularly. Without control, outdated or unauthorised access can persist.
Recommendation	Check the administrator groups used, especially those containing global administrators, at regular intervals. Role checks should be carried out regularly, ideally with the help of access reviews in Entra ID. Temporary assignment of rights via Privileged Identity Management (PIM) with authorisation processes further increases security. Administrators must be trained accordingly and sensitised to their responsibilities.
Config	N/A
Reference	https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-configure

Microsoft 365	**Securely manage guest access**
Rationale	External users (guests) pose a potential security and compliance risk as they are outside of organisational control. Without clear guidelines and regular review, there is a risk of excessive or outdated access rights.
Recommendation	Check whether and to what extent external users (guests) should have access to your Microsoft 365 environment. Define clear guidelines for handling guest accounts, including authorisation processes, usage restrictions and retention periods. Guest accounts should be reviewed regularly and removed or customised if necessary. If licensed, use Access Reviews from Entra ID Governance for this purpose. These make it possible to periodically evaluate access rights and automatically obtain feedback from those responsible. Avoid permanent privileged rights for guests and restrict access to what is necessary (principle of minimum authorisation). If necessary, use conditional access policies (more information below) to further minimise risks (e.g. restriction to certain IP ranges or device platforms).
Config	N/A
Reference	https://learn.microsoft.com/en-us/microsoft-365/admin/create-groups/manage-guest-access-in-groups?view=o365-worldwide https://learn.microsoft.com/en-us/entra/id-governance/create-access-review

Microsoft 365	**Security Monitoring**
Rationale	The early detection of attacks in Microsoft 365 requires a continuous and structured evaluation of security-relevant data. Reports such as risky logins or the Identity Security Score provide valuable insights into potential vulnerabilities and attempted attacks.
Recommendation	Microsoft provides various security reports, including risky logins and the Identity Secure Score. These should be analysed regularly and systematically. Monitoring must be carried out tenant-wide and include Entra ID (e.g. login logs), Microsoft Defender and other security-relevant services. All activities of privileged accounts must be logged and analysed regularly. The organisation should ensure that sufficient resources are available for the continuous review and adjustment of these measures.
Config	N/A
Reference	https://learn.microsoft.com/en-us/entra/id-protection/howto-identity-protection-investigate-risk https://learn.microsoft.com/en-us/entra/identity/monitoring-health/concept-identity-secure-score

3. Technical measures

3.1 Microsoft Entra Admin Center

Recommendation for managing access controls
Access controls and access conditions, such as multi-factor authentication (MFA), location-based re-strictions (geolocation), device status or risk-based access criteria, should be managed and monitored centrally via the Microsoft Entra Admin Centre. This enables consistent implementation, better traceability of changes and seamless logging for monitoring and compliance purposes. The use of other configura-tion paths (due to the historical growth of the environment, Microsoft 365 often offers different ways of carrying out a configuration) should be avoided in order to prevent fragmentation and misconfigurations.

	Conditional Access
Rationale	In modern, cloud-based environments, traditional access control based on user names and passwords is no longer sufficient. Users are increasingly accessing company resources from different devices, networks and locations - which significantly increases the attack surface. Conditional access offers the possibility of controlling access based on context, for example depending on location, device, user role or login risk.
Recommendation	Conditional Access Use Conditional Access Policies to specifically control access to your Microsoft 365 en-vironment. The following Microsoft Conditional Access Policies templates should be configured and enforced where possible: • **Multifactor authentication (MFA)** The use of multi-factor authentication should be a mandatory requirement for all users. The logon frequency should be defined and configured for this (e.g. daily for administrators, weekly for standard users) • **Legacy authentication** Blocks insecure authentication protocols such as IMAP or POP that do not support MFA. • **Secure registration of security information** Secures the registration process for security information (e.g. phone numbers, authenticator app) through conditions such as MFA. • **Require conformity of devices** Only allows access from devices that comply with company policies (e.g. managed by Intune and compliant). • **Geolocations** Control access based on geographic location, e.g. block logins from high-risk regions. • **Access to Azure Admin-Portal** Restricts access to the Azure portal to certain user groups, locations or devices. • **Conditional access policy für risky sign-ins und risky user** Activates MFA only for high-risk sign-ins, based on Microsoft's risk detection.
Config	Entra Admin Center ⇨ Protection ⇨Conditional Access ⇨ create new policy from templates ⇨*
Reference	https://learn.microsoft.com/en-us/entra/identity/conditional-access/overview https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-conditional-access-policy-common?tabs=secure-foundation

	Managing privileged accounts
Rationale	Administrative tasks should never be performed with regular user accounts. Instead, it is necessary to use separate administrator accounts that are intended exclusively for administrative purposes. These accounts must not be given access to user-specific applications such as email, Teams or SharePoint in order to minimise the risk of potentially vulnerable services.
Recommendation	Access should be strictly limited to administrative functions. As a technical measure, the use of Privileged Identity Management (PIM) is recommended in order to assign administrator rights only temporarily, if required and, if necessary, with authorisation.
Config	N/A
Reference	https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-configure

	Activate user-defined blocked passwords
Rationale	Users tend to choose weak or obvious passwords - often directly related to the organisation. By combining global and user-defined blocklists, Entra Password Protection helps to effectively block common and organisation-specific risky passwords and thus sustainably increase account security.
Recommendation	Microsoft Entra Password Protection (custom banned password list) checks by default whether users want to use passwords that are on a global banned list. Such passwords are blocked for all users of a client. To support business and security-related requirements, custom banned password lists can also be created. When a password is changed or reset, the system checks whether it is on one of these lists in order to enforce the use of secure passwords.
Config	Entra Admin Center ➪ Protection ➪ Authentication Methods ➪ Password Protection
Reference	https://learn.microsoft.com/en-us/entra/identity/authentication/tutorial-configure-custom-password-protection

	Realise corporate branding
Rationale	Phishing attacks often aim to trick users into revealing their credentials via fake login pages. Customised company branding on the login page strengthens visual recognition and reduces the likelihood of users falling for fake login pages.
Recommendation	Use the company branding in Office 365 to customise the standard login pages with your own logos, images and colours. This significantly reduces the risk of confusion with a frequently imitated login page and reduces the risk of phishing attacks.
Config	Entra Admin Center ➪ User experience ➪ Company Branding
Reference	https://learn.microsoft.com/en-us/microsoft-365/admin/setup/customize-sign-in-page?view=o365-worldwide

3.2 Microsoft Admin Center

	Block sign-in for shared mailboxes
Rationale	Shared mailboxes are not intended for direct sign-in but should only be used via delegated access. Direct login represents a security risk as these accounts often have system-generated, unmodified passwords and are not secured by multi-factor authentication. Blocking login prevents potential misuse and increases the security of the environment.
Recommendation	Shared mailboxes are used when several people need access to the same email address, e.g. for support or reception. The associated accounts have a system-generated password that is unknown. It is recommended to block the login for shared mailboxes.
Config	Microsoft Admin Center ➪ Active Users ➪ Filter for unlicensed ➪ block sign in for shared mail-box
Reference	https://learn.microsoft.com/en-us/microsoft-365/admin/email/about-shared-mailboxes?view=o365-worldwide

	Password Policy
Rationale	A clearly defined password expiration policy contributes to compliance with internal security policies and helps to ensure the regular renewal of weak or compromised passwords.
Recommendation	Whether and after how many days a password expires can be set. A conscious decision must be made as to whether a password expiry period is activated and this should be adapted to the company's internal password policy.
Config	Microsoft Admin Center ➪ Settings ➪ Org Settings ➪ Security & Privacy ➪ Password expiration policy
Reference	https://learn.microsoft.com/en-us/microsoft-365/admin/manage/set-password-expiration-policy?view=o365-worldwide

3.3 Exchange Admin

	Disable automatic forwarding
Rationale	Automatic email forwarding poses a significant security and data protection risk, as confidential information can be sent to external recipients in an uncontrolled manner. Attackers often use this function to exfiltrate data from the company unnoticed. By specifically deactivating or restricting automatic forwarding, this risk can be significantly reduced and control over email traffic can be improved.
Recommendation	Exchange Online offers various options for controlling email traffic, including remote domains, transport rules and anti-spam policies for outgoing emails. These can be used to prevent automatic forwarding via various channels - for example via inbox rules, out-of-office notes, Outlook on the web (Outlook Web App), administrator for-warding or Power Automate Flows. Make sure that transport rules and anti-spam policies are used specifically to prevent unwanted forwarding. If the forwarding function is nevertheless absolutely necessary, notifications about such processes should at least be activated.
Config	Exchange Admin Center ➪ Mail Flow ➪ Rules
Reference	https://learn.microsoft.com/en-us/exchange/security-and-compliance/mail-flow-rules/manage-mail-flow-rules

3.4 Microsoft 365 Defender

	Anti-Phishing Policy
Rationale	Phishing is one of the most common gateways for security incidents in Microsoft 365 environments. The integrated protection mechanisms form an important basis but are often not sufficient to reliably recognise targeted attacks such as identity or domain spoofing. Customised anti-phishing policies can be used to tailor protection to particularly vulnerable user groups or business-critical areas. This significantly reduces the risk of successful attacks.
Recommendation	Office 365 contains integrated functions for protection against phishing attacks as standard. To improve this protection, anti-phishing policies should be set up, for example through targeted settings to recognise and prevent identity or spoofing attacks. The default policy applies to all users in the organisation and provides a central way to fine-tune phishing protection. In addition, customised policies can be created for specific users, groups or domains, which then take precedence over the default policy.
Config	Microsoft Defender ➪ email & collaboration ➪ Policies & rules ➪ Threat policies ➪ Anti-Phishing ➪ create ➪ add users for impersonation protection; select all recommended check-boxes
Reference	https://learn.microsoft.com/en-us/defender-office-365/anti-phishing-policies-about

	Malware detection in email traffic - Enable notifications
Rationale	An automatic notification when malware is detected enables a quick response to potential security incidents. Infected accounts can be identified and isolated at an early stage and further damage can be prevented. This increases the speed of response and supports effective incident response.
Recommendation	Exchange Online Protection (EOP) is the cloud-based filter service for protection against spam, malware and other email threats and is included in all Microsoft 365 tenants with Exchange Online. Ensure that EOP is enabled and configure customised anti-malware policies that detect suspicious activity and automatically notify administrators.
Config	Microsoft Defender ⇨ email & collaboration ⇨ Policies & rules ⇨ Threat policies ⇨Anti malware ⇨ default ⇨ edit protection settings ⇨ enable admin notifications
Reference	https://learn.microsoft.com/en-us/defender-office-365/anti-malware-policies-configure

3.4 SharePoint Admin Center

	Restrict link sharing in SharePoint and OneDrive
Rationale	This setting defines the default link type that a user sees when sharing content in OneDrive or SharePoint. This does not exclude or restrict other options.
Recommendation	The „Specific people“ setting is recommended (only the recipients specified by the user)
Config	SharePoint Admin Center ⇨ Policies ⇨ Sharing
Reference	https://learn.microsoft.com/en-us/sharepoint/turn-external-sharing-on-or-off

	External sharing of content
Rationale	Centrally controlled sharing settings ensure that external access to content remains controlled and traceable. The specification that individual SharePoint sites may not have more generous sharing settings than the organisation itself ensures that no unintentional external data sharing takes place. The recommended setting „New and existing guests“ enables a secure exchange with external partners with simultaneous proof of identity.
Recommendation	The sharing settings for external sharing apply to the entire organisation. Individual SharePoint sites can have their own settings but must not be more open than the organisation's settings. The recommended setting is „New and existing guests“. Invited persons must confirm their identity via Microsoft account, business/school account or verification code. New guests are automatically added to the Entra ID directory.
Config	SharePoint Admin Center ⇨ Policies ⇨ Sharing
Reference	https://learn.microsoft.com/en-us/sharepoint/external-sharing-overview