The end of chaos and leaks.

SecureWork for Microsoft 365 – powered by Swiss IT Security AG.

Modern collaboration tools are an essential hub for everything you need to productively work with your teams – shared folders, knowledge management, video conferences, group chats and more in one single location. It's also what puts you in the crosshairs for potential attacks.

Swiss IT Security AG secures your Microsoft 365 environment with our all-new SecureWork package, combining custom-made security software with a safety and governance strategy to allow for a productive – and highly secure – collaboration.

Collaboration tools: A Single Point of Entry

The strength of collaboration tools like Teams, SharePoint or OneDrive is also their greatest weakness:
As a central hub for data, chats, video conference transcripts and file shares, an attacker needs to gain access to only one login to attain business-wide internal data.

Furthermore, the wide use of M365 and Teams without any form of governance has led to uncontrolled growth: Your employees might create Teams workspaces for a specific purpose and then quickly leave them abandoned. What happens when no one feels responsible for safe data disposal? What if the creator or group member has left the company? Over time, you've got abandoned data silos in your ecosystem that, best-case leads to chaos, and worst case to unauthorized access.

Our **SecureWork** package dramatically improves the security of all your collaboration tools using a combination of governance strategies and custom-build tools to securely store files, manage guest accounts, and govern Microsoft Teams – all from one centralized source.

SecureWork – Our 3 Core Components

#1 – TEAMS GOVERNANCE USING VALO TEAMWORK

Our Swiss IT Security AG experts develop a 360° governance strategy based on Valo teamwork, IAM, lifecycle management and more, in only three phases:

- Phase I – Defining potential weak points
- Phase II – Implementation of our end to end security strategy
- Phase III – Go Live & Support

#2 – GUEST MANAGEMENT USING GUEST LIFECYCLE FOR AZURE AD

Our Guest Lifecycle for Azure AD (GL4AAD) solution handles secure management and enrolment of guests, partners, and external service providers. It covers the creation of guest accounts in Azure AD, assigning responsibility to employees, and manages the automatic deletion or lockdown of inactive guest accounts.

#3 – SECURE FILE EXCHANGE WITH INDIVIDUAL FILESHARING

Our in-house solution **Individual Filesharing for SharePoint Online (IF4SPO)** allows secure file sharing via SharePoint online. It allows for safe folder storage inside anonymous libraries, behavior- and access-based privileges, and rules for automatic deletion and archival.

Find out all the details down below. Your needs are our top priority:
All three core components can be implemented based on your company's specific needs.

#1 – The Risk of Abandoned Collaboration Tools: 7 Strategies for Secure Productivity

Microsoft Teams and SharePoint requires a strong governance strategy to remain a productive tool for your business, otherwise you will face orphaned workspaces or sites, unmanaged access privileges, and data chaos with old files. Our comprehensive MS Teams Security & Governance strategy brings safety and order into chaos in seven steps:

1. Securing your tenants:
Assessment of all security-relevant components of M365, such as tenant settings, conditional access, PIM or the creation of a requirement catalogue, which fulfils all possible security standards (CIS benchmarks, best practices). In short, we ensure that Teams and SharePoint can be safely controlled.

2. Collaboration security:
To further strengthen the security of Teams, SharePoint Online, and OneDrive for Business, we create a requirement catalogue. It includes security-related specifications for usage of chats, apps in Teams, or file sharing.

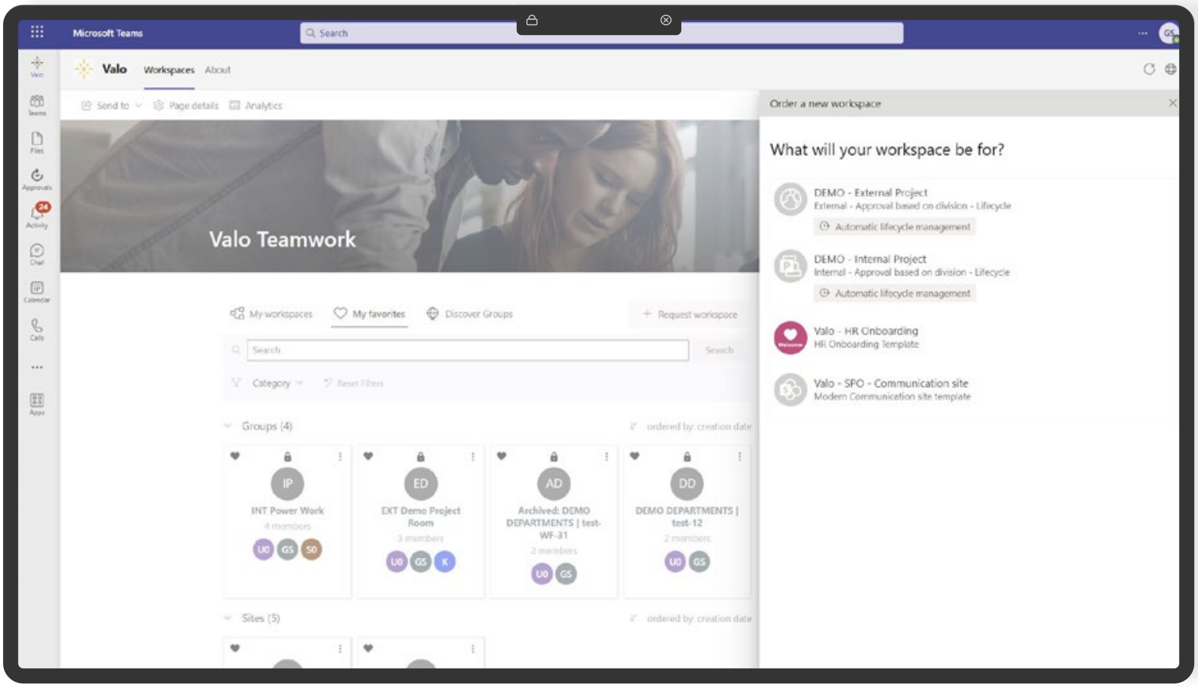
3. Data vaults for secure information:
Since all your data does not require equal protection, we define data vaults based on privilege levels. Each vault includes individual access rights and shares for external people to improve security while keeping a healthy balance between protection and productivity.

4. Teams and SharePoint governance:
Creation of governance strategies to ensure secure usage of Teams and SharePoint while improving productivity through a simplified overview and management.

5. Access verification:
Owners of Teams work spaces are required to update privileges for all their workspaces and contents, ensuring that only the relevant people have access to the data they truly are supposed to see.

6. Data loss protection:
Optimization of data loss prevention rules based on the concept of data vaults. If these rules are not in place, we will create these based on your requirements to ensure files aren't accessed by anyone who doesn't have permission.

7. Lifecycle Management:
Every single Teams workspace or SharePoint site was once created for a specific purpose, which can be fulfilled or changed over time – including who has access to the data therein. If the purpose has been fulfilled, the workspace or site should be archived or even deleted properly. This helps prevent contents from falling into the wrong hands.



The experts of Swiss IT Security AG take care of every single step along the way – from the first consultation to the creation of a governance strategy, to implementing Valo Teamwork and configuring M365 services, including end-to-end support. The implementation is divided into three steps:

PHASE I	PHASE II	PHASE III
Identification of weaknesses and potential points of failures in your Teams workspaces or SharePoint Online sites. If your business is not set up in Teams and has a desire to do so, we can easily set it up safely and securely.	Implementation of a strong pre-defined Teams & Sharepoint governance strategy via Valo Teamwork.	Go live support for MS Teams and our governance solution via trainings and 2nd/3rd level support.

#2 – The Risk of Guest Accounts: Secure management with Guest Lifecycle for Azure AD

Collaborating with partners, guests, and external contractors via M365 is usually being done via OneDrive, SharePoint, and Teams. To avoid data leaks and unprivileged access, guest accounts in Azure AD need to be handled separately.

Swiss IT Security AG has developed its own **Guest Lifecycle for Azure AD (GL4AAD)** solution to take care of this scenario: Based on Microsoft's Power Platform and relevant Azure services, it integrates seamlessly in your Microsoft 365 tenant to tackle the following tasks:

1. Onboarding:
Guests will be onboarded using the four-eyes principle, including critical security, trust, and behavior-based rules. Onboarding includes all relevant settings and security configuration within Azure AD.

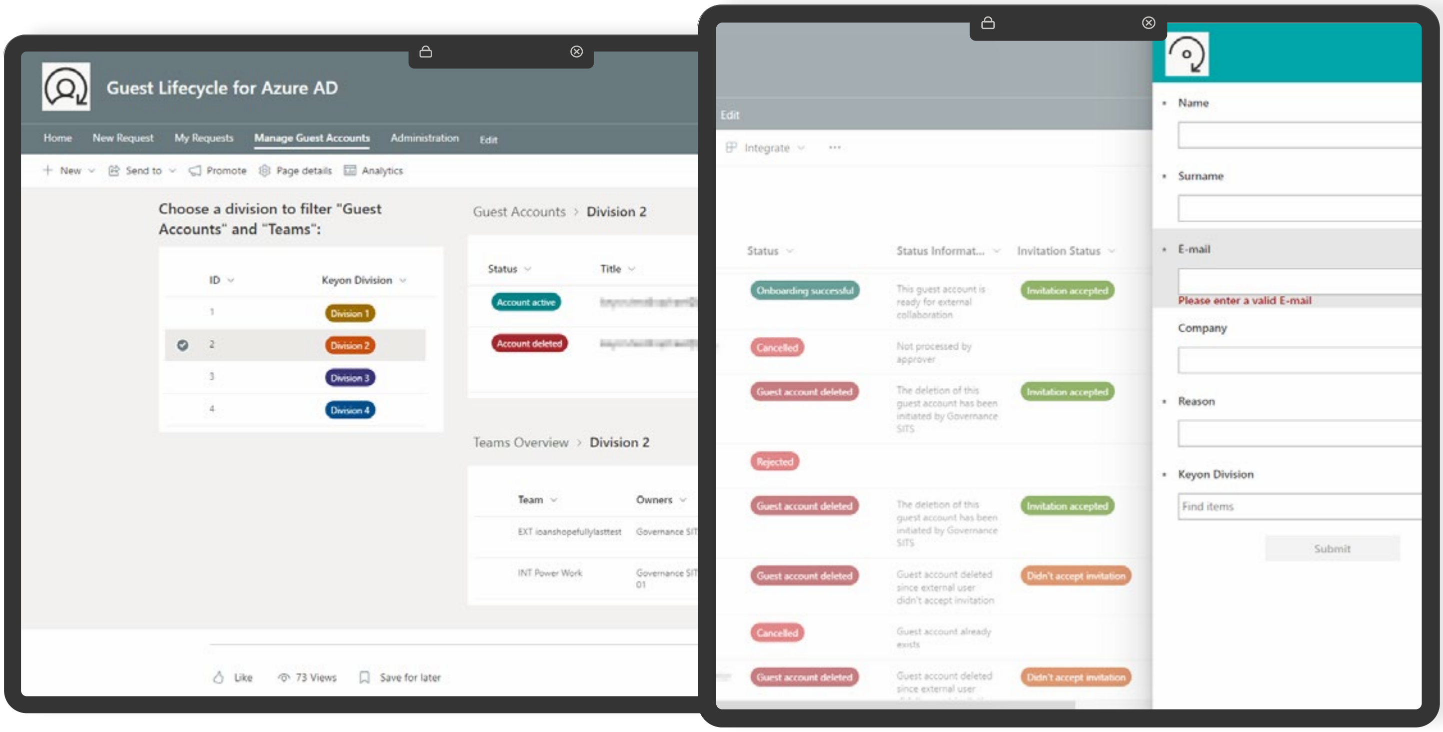
2. Guest account assignment:
Guest account assignment to a dedicated department or person who will be responsible for lifecycle and security procedures.

3. Regular certificate renewal:
Guest certificates need to be either removed or renewed to prevent former guest accounts from still having access to internal resources.

4. Multi-factor authentication:
Setup and management of MFA guidelines for secure login and limiting external users.

5. Removal of non-existing users:
Guest accounts that are no longer required will be removed after a certain period of inactivity.

GL4AAD handles these admin tasks for you, according to your requirements and needs. Our product can easily be added to companies that are not using E5 (A5) Azure AD Access Package licenses and can even be combined with an existing access package.



Choose a division to filter "Guest Accounts" and "Teams":

ID	Keyon Division
1	Division 1
2	Division 2
3	Division 3
4	Division 4

Guest Accounts › Division 2

Status	Title
Account active	[redacted]
Account deleted	[redacted]

Teams Overview › Division 2

Team	Owners
EXT ioanshopefullylasttest	Governance SIT
INT Power Work	Governance SIT 01

Status	Status Informat...	Invitation Status
Onboarding successful	This guest account is ready for external collaboration	Invitation accepted
Cancelled	Not processed by approver	
Guest account deleted	The deletion of this guest account has been initiated by Governance SITS	Invitation accepted
Rejected		
Guest account deleted	The deletion of this guest account has been initiated by Governance SITS	Invitation accepted
Guest account deleted	Guest account deleted since external user didn't accept invitation	Didn't accept invitation
Cancelled	Guest account already exists	
Guest account deleted	Guest account deleted since external user	Didn't accept invitation

• Name	
• Surname	
• E-mail	Please enter a valid E-mail
Company	
• Reason	
• Keyon Division	Find items

Submit

Overview – Guest Lifecycle for Azure AD (GL4AAD) Highlights

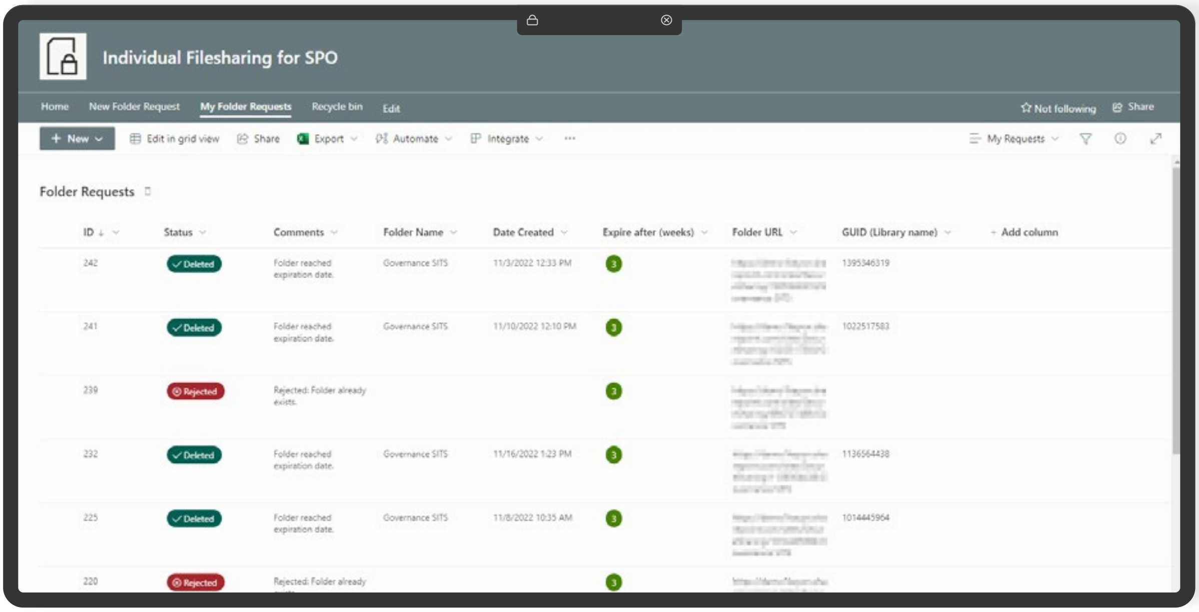
- Simple Azure AD guest account management.
- Easy assignment of responsibilities for guests, approval processes, and lifecycle definitions to ensure that all guest accounts are being deleted or set to inactive after a certain period.

#3 – Risk of Non-Privileged Access: Secure file exchange via Individual Filesharing

Sending and receiving privileged files internally or externally ranks among the highest risks for any business. Our own tailor-made **Individual Filesharing for SharePoint Online (IF4SPO)** makes file exchange easy and safe by adding secure data transfer to existing Microsoft 365 environments. Your employees and partners can use our solution to send confidential information and store them at a safe location.

IF4SPO allows users to store folders in anonymized libraries based on pre defined rules. Users can quickly configure who can see their files and set expiration rules for their data.

Long story short: **Individual Filesharing for SharePoint Online** guarantees simple and safe file transfers when dealing with internal or external users.



Folder Requests

ID ↓	Status	Comments	Folder Name	Date Created	Expire after (weeks)	Folder URL	GUID (Library name)	+ Add column
242	✓ Deleted	Folder reached expiration date.	Governance SITS	11/3/2022 12:33 PM	3	[redacted]	1395346319	
241	✓ Deleted	Folder reached expiration date.	Governance SITS	11/10/2022 12:10 PM	3	[redacted]	1022517583	
239	⊗ Rejected	Rejected: Folder already exists.			3	[redacted]		
232	✓ Deleted	Folder reached expiration date.	Governance SITS	11/16/2022 1:23 PM	3	[redacted]	1136564438	
225	✓ Deleted	Folder reached expiration date.	Governance SITS	11/8/2022 10:35 AM	3	[redacted]	1014445964	
220	⊗ Rejected	Rejected: Folder already			3	[redacted]		

Feature Overview

- Storing folders in anonymous libraries: The name of the library does not hint at what it's used for.
- Strict and clearly-defined privileges based on the purpose of each user's access.
- Automatic deletion and archival based on your rules.
- Optional: **IF4SPO** and Microsoft 365 Data Loss Prevention integration.

The Result: SecureWork.

Swiss IT Security AG makes your M365 more secure, more productive, and easier to use. Curious?
We'll put together a tailor-made package dedicated to your needs to help your workforce collaborate efficiently and safely.

Get Started: Safe Collaboration with **SecureWork** – powered by Swiss IT Security AG

If you need further assistance or have any questions related to the offer, please do not hesitate to contact our team of experts.