DOCUMENTATION SECURITY FRAMEWORK
THE SANDWICH APPROACH

Your knowledge and customer information are the most valuable assets of your business, and this should never fall into the wrong hands. To protect your valuable information, you need to focus on security as a whole. Your documentation platform should adhere to strict measures to protect the ongoing security and privacy of your valued data.

As a framework to ensure maximum documentation security, we're going to take a look at the sandwich approach to security, where the principles and the foundation make up the fundaments (aka the "buns") of your secured documentation.

Additional user-controlled security measures make up the "ingredients" of the security sandwich to further secure your data, password and knowledge in your documentation platform.

Together, they provide a layered approach to data security, giving you an extra boost of confidence.

PRINCIPLES

Compliance & Security Framework:

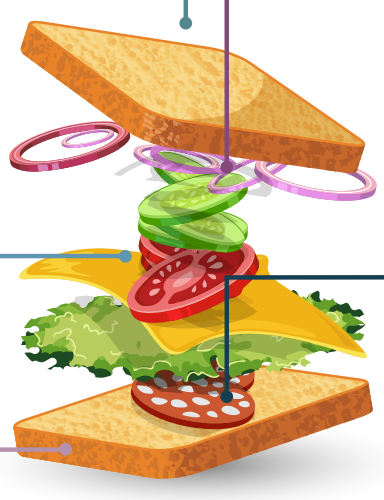
When you consider how fast technology companies are moving to and expanding in the cloud, and the proliferation of cloud-based security threats, compliance is no longer a nice-to-have. SOC 2 is one of the more common compliance goals for technology companies and is specifically designed for service providers storing data in the cloud.

PASSWORD SECURITY

An inevitable part of your security is ensuring that the keys to the kingdom are well-protected.

FOUNDATION

When choosing a cloud provider for documentation, look at the security mechanism and stack as a whole – including hosted platform, encryption, policy, guided security principles, security controls, security architecture, availability, disaster recovery, among others.



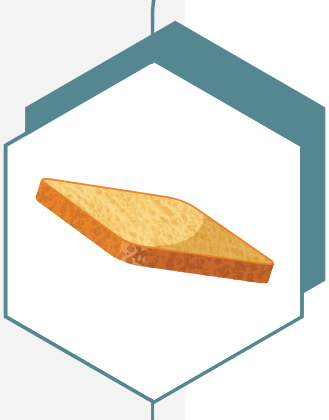
DATA SECURITY

Here is our recommendation of how you can implement a layered approach to data security. A layered approach to data security gives you confidence that only those who are authorized can access information.

KNOWLEDGE

In addition to mitigating data compromise, preventing institutional knowledge from getting lost in people's heads is also key to protecting the most valuable asset of your business.

PRINCIPLES



SOC 2 (Type II) Compliance

- The SOC 2 designation is specific to organizations that store data in the cloud and ensures that systems and processes meet a gold standard.
- SOC 2 mandates that companies establish and follow a rigorous standard of policies and procedures that meet the five information technology Trust Services Principles (TSPs) relevant to client data. The five TSPs are security, availability, processing integrity, privacy and confidentiality.
- A company that has SOC 2 (Type 1) is a company that was verified to have acceptable security processes at a specific point in time. The further you are from that specific point in time, the less likely that company is to have those security processes still in place.
- SOC 2 (Type 2) is granted to organizations that have implemented SOC 2 controls effectively over a period of six months.

DATA SECURITY

You can implement one or more of the following controls based on your requirements.

IP access control: It starts with only allowing access from trusted sources. By restricting access to only allowed IP addresses, you can greatly reduce the surface of your IT Glue account.

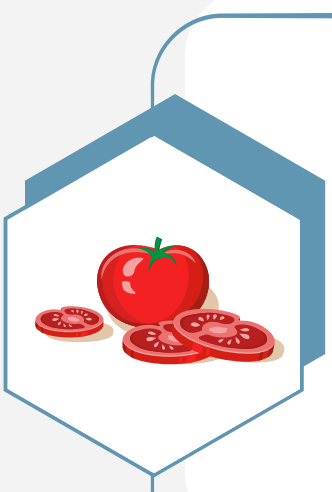
SSO and/or MFA: If the account has single sign-on configured, users will be redirected to the identity provider where they can complete authentication based on the conditional access policies in your single sign-on provider. Otherwise, they can use their username and password to sign in to IT glue and complete the multifactor authentication.

Roles & permissions: Based on a user's role and access permissions, they will have specific access to certain assets in the system.

Host-proof hosting: Even for assets that users have access to, host-proof hosting can be implemented so that users can't decrypt them unless a user-based passphrase is entered.

Audit & activity logs: Lastly, even after these layers, if something does happen, immutable audit logs can help during an investigation to determine the who, what, when and where.

PASSWORD SECURITY



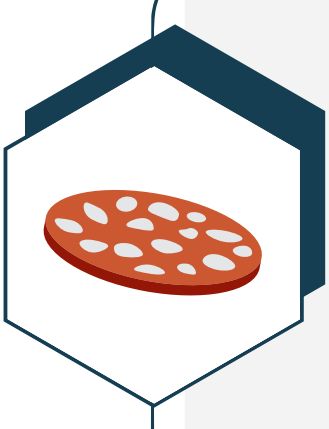
To keep passwords safe, IT Glue recommends a combination of the following measures.

Host-proof hosting (IT Glue Vault): Set up Vault and put sensitive passwords and Quick Notes inside the Vault. This ensures that you are fully in charge of your security, and even the webserver where you store your data (host) cannot access your data without your key.

Team-based & business personal passwords: Easily store both your team-based and business personal passwords in a centralized location.

Password accessed/changed: Set up workflows to be notified when a sensitive or important password is accessed, added, updated or destroyed.

KNOWLEDGE



To help with your business continuity, IT Glue recommends the following measures:

Completeness: Ensure documentation completeness for all your locations or clients. This way, regardless of which of your technicians is working on it, they have all the information they need.

Segmentation: Segment your internal documentation from external documentation to ensure company-sensitive information is segregated.

Approval & expiration: Have a policy in place for approving documentation and reviewing expired documentation.

Archive: Archive outdated information to keep your documentation fresh and up to date.

Export: Schedule regular account export so you always have access to the latest data to ensure business continuity.

HOW IT GLUE CAN HELP

As the industry standard for documentation and trusted by thousands of Managed Service Providers and IT professionals, we at IT Glue take our commitment to security seriously. IT Glue abides by strict measures to protect the ongoing security and privacy of your valued data. In addition, we understand that having reliable access to your data with no downtime is critical for your business.

To ensure both of these main objectives are met, we have adopted industry-leading security measures, including SOC 2 (Type II), multifactor authentication (MFA), single sign-on (SSO), host-proof hosting and IP access control, among others.

To know more about how IT Glue can help build your IT documentation security posture, request a demo. ORDER

IT Glue