saasnow
powered by amsio

SECURITY MEASURES

Data is fully isolated in a per customer environment

Every SaasNow instance is a separate secured system in which data is saved for that specific environment. No “shared” storage is used for storing customer data.

All traffic from and to the environment is encrypted with strong encryption

Traffic to the environment is encrypted with a valid, strong HTTPS certificate and data transferred is possible by using sFTP, also encrypted. This prevents eavesdropping end-to-end.

The environment is build and hardened by SAS headquarters

SAS invests a lot of effort in hardening, securing and configuring the software and prove this by having third parties performing penetration tests on every release. SaasNow also performs these security and penetration tests on a regular basis.

All datacenters as well as the SaasNow organization are ISO27001 certified

ISO27001 is an international standard for information security. It specifies the implementation and maintenance of an Information Security Management System (ISMS). SaasNow is also fully certified for all services she provides to customers.

No physical access unless employees of SaasNow that need to do maintenance

All datacenters are secured by 24x7 security on site. Nobody can get in without proper identification or proper registration. The locations from where SaasNow hosts her services are only accessible by certified personnel working for SaasNow. All personnel is properly screened and must possess a valid certificate of conduct.

Only HTTPS is accessible from the internet

We work of the principle that only the necessary ports and applications are opened that need to be opened to access and use the application. All traffic is terminated on a hardware SSL off loader. Traffic gets decrypted and inspected before ever reaching the environment. This means we have a lot of insight on what kind of traffic is actually accessing the environments.

24x7 monitoring for unexpected behavior

We monitor the application 24x7. This means that the environment is monitored permanently and that every interruption or unexpected behavior is directly alerted to our 24x7 monitoring team. We can intervene or solve any problems that might occur in the running environments.

Cancellation of contract with data removal

After deleting the environment the customer data is also permanently deleted. After a grace period of 7 days, the backups are also deleted in a way they can never be recovered.

ISO 27001
ISO 9001
NEN 7510

sas