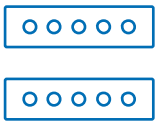
PASSWORD SAFE

... and the Works Council

INFORMATION FOR WORKS COUNCIL

Access Control

Prevent access by unauthorised people: By storing the passwords of data processing systems in Password Safe, only authorised employees will have access to your passwords! Access to Password Safe can be doubly secured by means of multi-factor authentication.

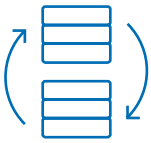


Password Control

Specify particularly which employees are given access to which passwords: You can create an appropriate rights concept in Password Safe and assign access rights to employees according to their authorisation/role. Thanks to visual protection, the passwords cannot be viewed. Particularly sensitive passwords can also be subject to a release process. They can only be used after they have been released by authorised persons.

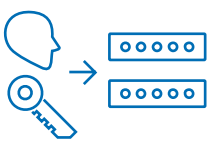
Input Control

„Which employee has used which password and when?“ Use the logbook to track all transactions. Precaution is better: If necessary, the system will also warn you automatically in case of unusual behaviour, so that you can react in time.



Availability Control

Thanks to SQL Clustering, the database and thus the passwords are always available. If one system fails, the second one is automatically activated. You can also use multiple application servers so that employees can still access their passwords in the event of a server failure. Automatic backups secure all users and passwords stored in Password Safe, as well as configured roles and authorisations.



No personal Data Storage

You only need a user name and password to enter Password Safe. Further data is only optional.

Data Protection

Each user only sees the data to which he is authorized to. This also applies to the entries in the logbook. Entries can also be deleted automatically on a regular basis.