Handout on the safe use of Citavi

Version: 1.0
Date: March 11, 2024
Classification: NOT PUBLIC
Status: in progress / submitted / **released**
Author: Sebastian Zimmermann
Distribution list: Researchers, teachers and students

Introduction

Citavi is a valuable tool for reference management and knowledge organization. This guide offers practical tips on how to use Citavi safely while protecting your privacy.

Simple steps for using Citavi safely

Installation: Only download Citavi from this link and install it on devices that are protected by up-to-date antivirus software.
Updates: Update Citavi regularly to benefit from the latest security features.
Access control: Assign access rights carefully and only to people who are directly involved in your project.
Backups: Create regular backups of your projects on external storage media or encrypted cloud services. Here you will find information on the options available to you.
If necessary, please contact the ZIMT support team for advice (support@zimt.uni-siegen.de).

Focus on data protection

Avoiding personal data: Do not store any research data or personal data in the Citavi Cloud. Departmental NAS drives are currently available for this purpose. If the data is to be shared with people outside the University of Siegen, SharePoint can also be used. Both services are available via the ZIMT.
Anonymization: Remove or alienate identifying features from your data.

Handling sensitive research data

Confidentiality: Treat all data confidentially, especially if it contains sensitive information. The same applies here: Do not store any research or personal data in the Citavi Cloud! Departmental NAS drives are currently available for this purpose. If the data is to be shared with people outside the University of Siegen, SharePoint can also be used. Both services are available via the ZIMT.
Non-published research data is always considered at least confidential!
Classification: Classify your data according to confidentiality: (public, non-public, confidential and strictly confidential). Further information on classifying your data can be found here.
Authorizations: Make sure that only authorized team members have access to sensitive data.

Practical application tips

Cloud use: Choose cloud services based in the EU to synchronize your database for data protection reasons. Preferably use systems provided by ZIMT, as these have already been checked by the University of Siegen's information security and data protection department.
Teamwork: Use team functions for joint projects and ensure that people have the appropriate authorization roles.
Use encryption: Encrypt your data both during transmission and storage. This also applies to Sciebo in particular.
If you require further information, please refer to the handout on encryption.
Please contact the ZIMT support team for advice if required!

Observe the legal framework

Check compliance with GDPR: Make sure that your work with Citavi complies with the GDPR.
Consider national laws: Also observe national data protection laws and your university's guidelines.

Checklist for everyday life

- Used an official source for downloading and installing Citavi?
- Regular updates carried out?
- Checked and adjusted access rights?
- Backed up the Citavi database?
- VVT (list of processing activities) carried out when processing personal data?
- If you have any questions or uncertainties, please contact the information security and data protection team.

datenschutz@uni-siegen.de
ciso-team@uni-siegen.de

Status: 03/2023 Review: 03/2026
Classification of confidentiality: non-public
Author: Sebastian Zimmermann
Storage: CITRIX drive data protection