Guidelines for Websites of Kiel University (CAU)
University Computing Centre and Press Office on behalf of the University Board, 02.03.2023 – This document replaces all previous editions

Websites: Web presences and Web applications

Web presences are websites that primarily serve to convey information and present content, with comparatively little interactivity. Example: www.uni-kiel.de

Web applications are websites like application programmes that follow the client-server model. The focus here is on interactivity. Example: HISinOne

In principle, web presences are a special form of web applications, but for the sake of simplicity we distinguish them from each other in the way described above.

Technical specifications

1. **public web applications** shall be set up, configured, documented and maintained in accordance with the respective state of the art, taking into account general and local security recommendations.

   - The latest versions of operating systems and application software must be used, and security updates must be applied promptly.
   - When configuring the software, the current recommendations on security settings must be observed.
   - Current encryption methods shall be used for communication.
   - Security recommendations can be found at organisations such as the Federal Office for Information Security (BSI), in the documentation of the respective systems as well as in the further guidelines of the CAU/the University Computing Centre.

2. **Web presences** of CAU institutions and projects are to be realised in the CAU content management systems (CMS) offered centrally free of charge for the institutions and thus also use the CAU’s central corporate design on the web.

   - Through central maintenance, the systems used by the institutions can be kept at a uniform, up-to-date technical level, and a uniform, functional design is also guaranteed. Both technical and design developments can be carried out centrally without the involvement of the institutions.
3. The establishment of parallel technical structures should be avoided as a matter of principle. The use of existing central offers and services should be examined at all levels; the Press Office and University Computing Centre offer advice on this.

- The installation of own CMS instances is to be avoided because central instances are provided free of charge.
- Whenever central offers are available, parallel technologically comparable offers for the same purpose should be avoided as far as possible. This applies at all levels, e.g. regarding the installation of content management systems, general hosting environments for web applications, special applications or the installation of servers.

Design specifications

1. web presences in the central CMS systems of the university use the corporate design of the CAU. The implementation of the corporate design in the central CMS systems is the responsibility of the Press Office and the University Computer Centre.

2. web applications use elements of the corporate design where possible and feasible with reasonable effort. The Press Office provides the necessary design guidelines and materials for adapting web applications to the CAU corporate design and offers training.

- Elements of CAU’s corporate design are logos, colours, shapes, fonts.
- Adaptations of third-party applications should only be made where intended (e.g. setting logos, colours, etc.). The creation of special versions (fork) that can no longer be maintained by standard updates should be avoided.

Legal specifications

1. When processing personal data, the applicable laws and regulations on data protection, in particular also on documentation requirements, must be complied with.

- In particular, the State Data Protection Act and the EU Data Protection Regulation (DSGVO / GDPR) must be observed.
- In particular, a register of processing activities must be drawn up and filed with the CAU data protection officer. Advice on data protection issues is also provided there.
- In particular, technical and organisational measures pursuant to Section 32 of the EU GDPR must also be documented.
2. **In the case of commissioned processing by third parties, a commissioned processing agreement shall be drawn up, and in the case of support services by third parties, confidentiality agreements shall be concluded where appropriate.**

   - The minimum requirements of § 38 LDSG [SH] and § 28 EU-DSGVO must be met. In the area of legal issues, CAU's legal advisor offers advice here if required.

3. **Liability: Christian-Albrechts-Universität zu Kiel is a public corporation. It is legally represented by the President.**

4. **Web presences in the central CMS systems refer to the central CAU imprint:** [https://www.uni-kiel.de/en/imprint](https://www.uni-kiel.de/en/imprint)

5. **Web presences that are not created and/or operated as part of CAU’s central services may not refer to CAU’s central imprint.** Compliance with the applicable laws and regulations on the operation of a website and on data protection is the responsibility of the respective operator. In this case, CAU is exempt from liability.

6. **All web applications must comply with other contractual agreements (e.g. licence agreements), laws (e.g. copyright) and internal university guidelines.**

   - In the area of legal issues, CAU's legal advisor offers advice if required.
   - Internal content requirements can be, for example, the use of gender-appropriate language, prohibition of discrimination or the CAU Code of Conduct.

7. **As a matter of principle, CAU’s websites must be designed to be barrier-free. The applicable laws and regulations on the accessibility of websites must be complied with.**

   - In particular, the [Act on Equal Opportunities for Persons with Disabilities in Schleswig-Holstein](https://www.uni-kiel.de/en/imprint) (Landesbehindertengleichstellungsgesetz - LBGG), the [Directive (EU) 2016/2102 of the European Parliament and of the Council of 26 October 2016 on the accessibility of the websites and mobile applications of public sector bodies](https://www.uni-kiel.de/en/imprint), and the [Ordinance on the Creation of accessible Information Technology in accordance with the Act on Equal Opportunities for Persons with Disabilities](https://www.uni-kiel.de/en/imprint) (Barrierefreie-Informationstechnik-Verordnung - BITV 2.0) must be observed.
• If a web application already purchased or operated externally is not accessible, the institutions must encourage the software provider to create the greatest possible accessibility. In this case, CAU institutions are themselves responsible for creating a legally required accessibility declaration. The University Computing Centre and Press Office support the institutions in this as far as they can.

Organisational specifications

1. CAU institutions and projects must ensure continuous technical support for their own web applications. In particular, it must be ensured that persons with suitable training are responsible for the operation and maintenance of the respective web applications and that job substitution arrangements are in place. The relevant persons are to be named to the University Computing Centre. Any change of personnel must be reported.

• Technical support is an ongoing task, which is why it is not enough to only take care of the initial setup of a software.
• A single person cannot be responsible for the support on a permanent basis, because even during the time of annual leave, security-critical updates may have to be installed and corrections have to be made.

2. CAU institutions and projects that realise and use web presences in the services offered centrally free of charge for the institutions must ensure that continuous editorial support for the content of the web presences is provided. In particular, it must be ensured that there is a continuous job substitution arrangement. The relevant persons must be named to the Press Office and the University Computing Centre. Any change of personnel must be reported.

3. The University Computing Centre provides technical and organisational guidelines and recommendations.

• Examples of urgent recommendations are the use of central accounts also for own services, examples of specifications could be rules for the separation of IP address ranges.

4. For websites (web presences as well as web applications) that are managed decentrally in whole or in part, a central registration with URL, purpose of the application as well as contact persons is carried out.

• It must be possible to contact persons in charge quickly, especially for a decentralised application, in order to be able to react quickly in case of a discovered or reported security vulnerability.
• It must also be possible to contact those responsible in the event of a problem with the content, such as a formal or content-related error or suspected infringement of regulations (e.g. copyright).
• This applies especially to decentralised offerings where there is no central technical access.
• In the event of a change of personnel, the data provided must be updated promptly.

5. **Institutions and projects at CAU use uni-kiel.de domains.** The purchase and use as forwarding of external domains is possible after consultation with the Press Office and University Computing Centre. Purchases are always made via the DFN-Verein in cooperation with the University Computing Centre.

   • The aim is to avoid internal university institutions concealing their affiliation with CAU; the affiliation should therefore also be evident from the web address.
   • If own domains are used for certain projects or cooperations, it should be avoided that arbitrary domain vendors are used and that the type of integration is not done according to the specifications of CAU (e.g. no use of CAU name servers).

6. **Web presences are to be designed bilingually (German and English).**

7. **Web presences and web applications must be developed in such a way that they can also be used on mobile devices.**

8. **The University Computing Centre reserves the right to completely or partially deactivate websites (web applications as well as web presences) in risk situations or in the case of clear and serious violations of these guidelines, or to enforce global security settings.**

   • Enforceable security measures could include forcing encrypted connections, access to login pages only via VPN/On Campus, restricting third-party content or automated attack prevention.
   • In the case of websites that are located outside the hardware of the University Computing Centre but within the CAU intranet, the University Computing Centre reserves the right to isolate vulnerable and endangering systems.

At the end of September 2022, the University Board decided to adopt a web governance and, in connection with this, to communicate and ensure the implementation of these guidelines by the Press Office and the University Computing Centre.