HAW BW
Hochschulen
für Angewandte Wissenschaften
Baden-Württemberg

Digitale Souveränität und Cyber-Resilienz der baden-württembergischen Hochschulen bis 2030

Positionspapier der Hochschulen für Angewandte Wissenschaften (HAW)

Ziele der HAW bis 2030

- **Souveräne europäische IT-Infrastruktur:** Modernisierte, überwiegend europäisch ausgerichtete IT-Infrastrukturen mit Zero-Trust-Campus-Netzen und souveräne Cloud/Datenräume unter EU-Rechtsrahmen.
- **Etablierte Cyber-Resilienzstrukturen:** Professionelle Incident-Response-Teams, CERT-Services und belastbares Business-Continuity-Management für alle HAW in enger Verzahnung mit bwInfoSec/CSBW.
- **Sicherer, unabhängiger KI-Einsatz:** Europäische KI-Dienste für sensible Prozesse, souveräne HPC/GPU-Infrastrukturen sowie systematische Kompetenzentwicklung und klare Regeln für den Einsatz von KI in Lehre, Prüfung und Forschung.
- **Durchgehend digitale, sichere Verwaltungsprozesse:** OZG-konforme, medienbruchfreie Abläufe mit föderiertem Identity- und Access-Management, starker Authentifizierung und Ende-zu-Ende-Verschlüsselung.
- **Klare Governance und Verantwortlichkeiten:** In einem Umfeld hybrider Bedrohungen agieren HAW als verlässliche Partner für Staat, Wirtschaft und Gesellschaft innerhalb einer Landes-Digitalstrategie mit definierten Sicherheitsniveaus, Betreiberrollen und abgestimmten Notfallprozessen.

HAW in Baden-Württemberg sind Schlüssel für Innovation, Fachkräftesicherung und Technologietransfer. Digitalisierung ist dafür Grundvoraussetzung – so elementar wie Gebäude und Labore.

Wir befinden uns in einem dauerhaften Zustand hybrider Auseinandersetzungen. Hochschulen werden Ziel von Spionage, Sabotage und Desinformation.[1] Die USA sind aufgrund geopolitischer Interessen und Rechtslage (Cloud Act, extraterritoriale Zugriffe) auf Dauer kein verlässlicher Anker digitaler Souveränität. Die Europäische Union muss handlungsfähig werden und verlässliche digitale Infrastrukturen, Dienste und Regelwerke bereitstellen.

HAW verantworten den Betrieb kritischer Lehr-, Prüfungs- und Verwaltungssysteme und den Schutz sensibler Forschungs- und Personendaten in einer per se offenen und leicht zugänglichen Umgebung. IT-Sicherheit ist damit strategische Führungsaufgabe und Teil öffentlicher Daseinsvorsorge. Mit ihren Kompetenzen können die HAW dann die Sicherheits- und Resilienzpolitik des Landes aktiv vorantreiben und in der Fläche zu ebendiesem notwendigen

[1] Dieses Papier fokussiert den digitalen Raum. Zum Umgang mit weiteren Bedrohungen und der Resilienz im physischen Raum, siehe das *Positionspapier der HAW in Baden-Württemberg zu Sicherheit und Resilienz* vom 27. Februar 2026.

Anker digitaler Souveränität werden (s. hierzu das *Positionspapier der HAW in Baden-Württemberg zu Sicherheit und Resilienz*).

Mit bwInfoSec wurden wichtige Grundlagen gelegt. Für die nächsten fünf Jahre sind jedoch ein Umbau zu modernen Sicherheitsarchitekturen, professionelle Incident-Response-Strukturen sowie ein systematisches Business Continuity Management (BCM) erforderlich. Die Landesstrukturen bwInfoSec und CSBW müssen gestärkt, Zuständigkeiten (insbesondere nach CSG § 2 Abs. 2) klar geregelt und mit Forensik-, CERT- und Krisenkompetenzen hinterlegt werden.

1. Infrastruktur und Systeme: Sicherheit und Souveränität

Ausgangslage

Die Abhängigkeiten von US-Hyperscalern sind Sicherheits-, Rechts- und Innovationsrisiko. Veraltete Systeme und Insellösungen erhöhen die Angriffsfläche. HAW benötigen leistungsfähige, sichere und überwiegend europäisch betriebene IT-Infrastrukturen.

Transformationsbedarf bis 2030

Um zukunftsfähige IT-Infrastrukturen zu gewährleisten, sollen die Rechenzentren modernisiert und konsolidiert werden, sodass sie standardisierten Landes- und EU-Lösungen entsprechen. Ebenso ist der Aufbau sicherer Campus- und Fernzugänge erforderlich, die auf Zero-Trust-Ansätzen sowie einem umfassenden Identity- und Access-Management und einer konsequenten Segmentierung basieren. Die Etablierung von souveränen Cloud- und Hybridarchitekturen ermöglicht die eindeutig definierte Speicherung von kritisch schutzbedürftigen Daten innerhalb von EU-Rechtsräumen. Der Aufbau sicherer Datenräume und Datenplattformen ist ebenso notwendig, um die präzise Klassifizierung sowie ein durchdachtes Rollen- und Rechtemanagement zu gewährleisten. Open-Source kann dabei eine wichtige Säule sein, aber nicht aus einem idealistischen Selbstzweck heraus. Eine Open-Source-Transformation soll überall dort umgesetzt werden, wo sie Sicherheit, Interoperabilität und Auditierbarkeit stärkt. Schließlich bietet der Ausbau von HPC- und GPU-Ressourcen in Landes- und EU-Verbundstrukturen leistungsfähige und zukunftsfähige technische Grundlagen für den Forschungskontext.

Um eine politische Priorität für europäische, souveräne Cloud-, Kollaborations- und Prüfungsdienste bei allen Landeslösungen umzusetzen, stehen die HAW als Pilotstandorte bereit zur Beteiligung an europäischen Initiativen (Datenräume, Cloud-Netzwerke, KI-Infrastrukturen). Ein Ausbau von bwInfoSec zu einer aktiv unterstützenden Stelle (Monitoring-Services, Forensik, CERT-Leistungen, Krisenteams) ist dafür insbesondere im BCM unabdinglich.

2. KI in Verwaltung, Lehre und Forschung: sicher und unabhängig

Ausgangslage

KI verändert Verwaltung, Lehre und Forschung tiefgreifend. Souveräner KI-Einsatz ist eine Sicherheitsfrage: Datenabflüsse, Modellmanipulationen und Abhängigkeiten von Anbietern aus problematischen Drittstaaten müssen minimiert werden. Europäische KI-Infrastrukturen und -Lösungen sind prioritär.

Transformationsbedarf bis 2030

Der Einsatz von KI zur Prozessoptimierung (Dokumentenklassifikation, Workflows, Plausibilitätsprüfungen, Auswertungen) in der **Verwaltung** ist in Zukunft eine essenzielle Fähigkeit. Voraussetzung sind vollständig digitalisierte, standardisierte Prozesse und klare rechtliche Leitplanken (Transparenz, Nachvollziehbarkeit und Datenschutz). Im Rahmen des Dialogprozesses „Zukunftslabor: Hochschulen in der Digitalen Welt“ erfolgen notwendige, erste Schritte. Die Nutzung zertifizierter europäischer KI-Dienste für sensible Verwaltungsprozesse muss strategische Selbstverständlichkeit sein, Anbieter aus unsicheren Rechtsräumen sollten nur in klar definierten, niedrigkritischen Bereichen eingesetzt werden.

Die **Lehre** benötigt Zugang zu modernen KI-Modellen auf souveränen Infrastrukturen (Land/EU), nicht nur über globale Plattformen. Neben der Integration von KI-Kompetenzen in alle Studiengänge (Anwendung, kritische Reflexion, Sicherheit, Ethik) sind klare Regeln für Prüfung, wissenschaftliche Redlichkeit und Umgang mit KI-Tools erforderlich.

Innovative **Forschung und Transfer** basieren auf dem Aufbau bzw. der Nutzung leistungsfähiger, souverän betriebener HPC-/GPU-Infrastrukturen und Datenplattformen. Open-Source-Modelle und -Werkzeuge müssen dort zum Einsatz kommen, wo Transparenz und Anpassbarkeit sicherheitsrelevant sind. Zur Ressourcensparsamkeit gehört, dass der Betrieb großer Basismodelle nicht isoliert an Einzelhochschulen, sondern über professionell betriebene Landes-, Bundes- oder EU-Dienste läuft, von denen alle HAW profitieren.

3. OZG – Security-by-Design

Ausgangslage

Medienbrüche zwischen Landesportalen, Kommunen und Hochschulsystemen erschweren die OZG-Umsetzung und erhöhen Risiken. Die schleppende Klärung von Zuständigkeiten und Verantwortlichkeiten in der Registermodernisierung und fehlende einheitliche Identitäts- und Sicherheitskonzepte schwächen zusätzlich die Resilienz.

Transformationsbedarf bis 2030

Durchgängig digitale, medienbruchfreie Prozesse von Landesportalen bis zu Hochschulsystemen mit einem einheitlichen, föderierten Identity- und Access-Management für Studierende, Beschäftigte und (Hochschul-)Partner sorgen für barrierefreie, international nutzbare Angebote.

Dazu zählen der verpflichtende Einsatz starker Zwei-Faktor-Authentifizierung für alle kritischen Dienste (Studien-, Prüfungs-, Personal-, Forschungsverwaltung), eine Ende-zu-Ende-Verschlüsselung für sensible Daten und Kommunikationswege, sowie zentral gemanagte, gehärtete Endgeräte inklusive Mobile-Device-Management. Konsequent ist eine Anbindung an Monitoring-, Logging- und Incident-Response-Strukturen (bwInfoSec, CSBW, CERT).

Erforderlich dafür ist eine ressortübergreifende Digitalisierungsstrategie des Landes mit nationaler Einbindung, in der Hochschulen als eigenständige, aber integrierte Akteure berücksichtigt werden. Verbindliche Schnittstellenstandards zwischen Landesportalen, Kommunen und Hochschulen fördern die Umsetzung ebenso wie klare Verantwortlichkeiten: Wer betreibt was, wer definiert das Sicherheitsniveau, wer unterstützt im Notfall?

Fazit: Souveräne und resiliente HAW bis 2030

Zentrale politische Forderungen: 5-Punkte-Plan

1. Priorisierung und Finanzierung souveräner IT- und Cloud-Lösungen als Grundversorgung: Landesweite Umsetzung europäischer Cloud-, Kollaborations- und Prüfungsdienste sowie Finanzierung von Rechenzentrumsmodernisierung und Datenräumen (Unterstützung von EU-Initiativen, zentrale HPC/GPU-Ressourcen). Verpflichtende Nutzung zertifizierter europäischer KI-Dienste für sensible Verwaltungsprozesse; klare rechtliche Leitplanken (Transparenz, Nachvollziehbarkeit, Datenschutz) durch das Land.

2. Verbindliche technische und organisatorische Sicherheitsstandards: Gesetzlich und finanziell hinterlegte Mindeststandards für Sicherheitsarchitekturen, Endgeräte-Härtung und Schnittstellen (Zero Trust, IAM, 2FA, Verschlüsselung, Monitoring).

3. Belastbare Cyber-Resilienzstrukturen etablieren: bwInfoSec und ein hochschulspezifisches CERT personell und strukturell so ausbauen, dass HAW proaktiv unterstützt und im Notfall wirksam verteidigt und umgehend durch BCM-Maßnahmen flankiert werden.

4. Registermodernisierung in der OZG-Umsetzung mit Hochschulen als integrierte E-Government-Akteure: Verbindliche Schnittstellen- und Sicherheitsstandards zwischen Landesportalen, Kommunen und Hochschulen sowie Förderung eines föderierten Identity- und Access Managements für alle Nutzergruppen. Konsequente Umsetzung der Registermodernisierung mit entsprechender Ausstattung für die Hochschulen. Grundlage dafür ist eine ressortübergreifende Digitalstrategie des Landes, in den Hochschulen als eigenständige, integrierte Akteure mit klaren Zuständigkeiten, Betreiberrollen und verlässlicher Finanzierung berücksichtigt werden.

5. Hybriden Bedrohungen der Gesellschaft wirkungsvoll entgegentreten: HAW als kritische Knotenpunkte gesellschaftlicher Resilienz anerkennen und entsprechend priorisieren – in Gesetzgebung, Finanzplanung und europäischen Initiativen.