Amtliche Bekanntmachungen
der Pädagogischen Hochschule Freiburg

2026, Nr. 5 21. Januar 2026

Leitlinie zur Informationssicherheit

20. Januar 2026

Inhalt

1. Stellenwert der Informationssicherheit

Laut Verwaltungsvorschrift des Innenministeriums zur Informationssicherheit (VwV Informationssicherheit) vom 7. April 2017 - Az.: 5-0275.0/25 sind alle Dienststellen und Einrichtungen der unmittelbaren und mittelbaren Landesverwaltung Baden-Württemberg – also auch Hochschulen – verpflichtet, die Informationssicherheit[1] (IS) gemäß IT-Grundschutz (IT = Informationstechnik; BSI-Standards 200-1 bis 200-3) des Bundesamts für Sicherheit in der Informationstechnik (BSI) umzusetzen. Daneben weist das IT-Grundschutz-Profil für Hochschulen (Version 2022.0.0) darauf hin, dass die IS im Rahmen der aktuellen Bedrohungslage auch im Hochschulumfeld eine immer größer werdende Relevanz erhält. Der Forschungsstandort Deutschland ist attraktiv, damit werden auch Hochschulen zunehmend zu Zielen für Angriffe im IT-Bereich. Aufgrund ihrer offenen Struktur sehen sich Hochschulen hier einer besonderen Herausforderung gegenüber. Die Pädagogische Hochschule Freiburg räumt der IS infolgedessen höchste Priorität ein.

2. Sicherheitsziele

Die Pädagogische Hochschule Freiburg setzt sich die folgenden Sicherheitsziele:

2.1 Bewusstsein für Informationssicherheit

Um die IS sicherzustellen, bedarf es eines Sicherheitskonzepts. Dieses Konzept ist nur dann effektiv, wenn alle Mitglieder und Angehörigen die Gefährdungen für die IS kennen und unter Beachtung ihrer Sorgfaltspflichten so handeln, dass Risiken auf ein vertretbares Maß reduziert werden. Dementsprechend soll das Bewusstsein aller Mitglieder und Angehörigen für die IS aufrechterhalten und erhöht werden.

[1] Im Folgenden wird die weitreichendere Bezeichnung „Informationssicherheit“ anstelle des in der Literatur oft synonym verwendeten Begriffs „IT-Sicherheit“ verwendet. Gemäß der Empfehlung des BSI-Standards 200-1 wird IS in einem umfassenden und ganzheitlichen Sinne verstanden. Dies schließt die Bereiche „Informations- und Kommunikationstechnik“ sowie „Informations- und Telekommunikationstechnik“ ein und bezieht sich auf den Schutz von Informationen jeglicher Art und Herkunft. Dies gilt unabhängig davon, ob diese in technischen Systemen, auf Papier oder in Köpfen gespeichert sind.

2.2 Einhaltung von Rahmenbedingungen

Relevante Rahmenbedingungen sollen eingehalten werden, darunter die folgenden:

- Bundesdatenschutzgesetz (BDSG)
- Datenschutz-Grundverordnung (DSGVO)
- Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD)
- Landesdatenschutzgesetz (LDSG)
- Landeshaushaltsordnung für Baden-Württemberg (LHO)
- Landeshochschulgesetz (LHG)
- Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG)
- Verwaltungsvorschrift des Innenministeriums zur Informationssicherheit (VwV Informationssicherheit)

2.3 Sicherstellung der Informationssicherheit

Da nicht zuletzt auch die Aufgabenerfüllung der Pädagogischen Hochschule Freiburg in hohem Maße von der Vertraulichkeit, Integrität und Verfügbarkeit der Informationen und Prozesse im Informationsverbund abhängt, sollen zumindest diese Schutzziele sichergestellt werden. Sofern möglich sollen auch alle erweiterten Schutzziele (Authentizität, Verbindlichkeit und Zurechenbarkeit) sichergestellt werden. Grundsätzlich soll ein umfassender Schutz aller Informationen und Prozesse im Informationsverbund im Sinne der vom BSI empfohlenen Standard-Absicherung sichergestellt werden (eine Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz wird angestrebt).

2.4 Vermeidung oder Reduktion von Schäden

Materielle Schäden (z. B. Investitionsverluste) und immaterielle Schäden (z. B. Reputationsverluste) sollen vermieden werden. Tritt trotz aller Bemühungen ein Schadensfall ein, sollen die Schäden reduziert werden.

3. Sicherheitsstrategie

Um die Sicherheitsziele zu erreichen, etabliert die Pädagogische Hochschule Freiburg ein Informationssicherheitsmanagementsystem (ISMS), das sich am IT-Grundschutz des BSI orientiert. Der Sicherheitsprozess folgt den BSI-Standards 200-1, 200-2 und 200-3 und dem PDCA-Zyklus (Plan – Do – Check – Act), sodass ein Sicherheitskonzept gemäß gewählter Vorgehensweise (Basis-, Kern- oder Standardabsicherung) erstellt, umgesetzt, geprüft oder fortgeschrieben/verbessert werden kann. Kurz-, mittel- und langfristig werden folgende Vorgehensweisen umgesetzt, dabei wird sich falls möglich am IT-Grundschutz-Profil für Hochschulen[2] orientiert:

- Kurzfristig: Weg in die Basis-Absicherung
- Mittelfristig: Basis-Absicherung (ein Testat nach der Basis-Absicherung wird angestrebt) und Kern-Absicherung (eine Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz wird angestrebt)
- Langfristig: Standard-Absicherung (eine Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz wird angestrebt)

Die Maßnahmen, mit denen die Sicherheitsziele und Sicherheitsstrategie verfolgt werden, werden in einem dokumentierten Sicherheitskonzept beschrieben. Falls nötig werden die Maßnahmen mittels Richtlinien, Standards und Verfahren operativ verankert und durch kontinuierliche

[2] Der Arbeitskreis Informationssicherheit des Vereins „Zentren für Kommunikationsverarbeitung in Forschung und Lehre e. V.“ hat unter Leitung des BSI ein IT-Grundschutz-Profil für Hochschulen entwickelt. Es wurden zunächst repräsentative Prozesse an Hochschulen herausgearbeitet. In einem nächsten Schritt wurden die für diese Prozesse charakteristischen Applikationen sowie der Schutzbedarf und die nötigen IT-Systeme sowie Räumlichkeiten ermittelt. Zuletzt wurden IT-Grundschutz-Bausteine identifiziert, deren Anwendbarkeit auf die Hochschullandschaft geprüft und Umsetzungshinweise erarbeitet. Das Profil dient als Vorlage, die an die individuellen Anforderungen der Pädagogischen Hochschule Freiburg angepasst werden kann.

Schulungs- und Sensibilisierungsmaßnahmen gestützt. Sowohl die Umsetzung und der Erfolg der einzelnen Maßnahmen sowie des Sicherheitskonzepts als auch der Zielerreichungsgrad der Ziele, an denen sich die Maßnahmen orientieren, wird zumindest jährlich kontrolliert. Entsprechend werden die Ziele sowie Maßnahmen möglichst mess- und überprüfbar formuliert. Jeder Schritt dient dem Aufbau, der Aufrechterhaltung sowie kontinuierlichen Verbesserung der IS, da sie kein Zustand ist, der einmal erreicht wird und dann fortbesteht, sondern ein fortwährender Prozess, der gesteuert werden muss. Die Umsetzung der IS an der Pädagogischen Hochschule Freiburg erfolgt unter Berücksichtigung besonderer lokaler Anforderungen und immer darauf bedacht, die Ressourcen gemäß LHO § 7 wirtschaftlich einzusetzen.

4. Organisationsstruktur

Die Pädagogische Hochschule Freiburg legt folgende Organisationsstruktur fest:

4.1 Hochschulleitung

Die Hochschulleitung trägt die Gesamtverantwortung für die IS. Die Hochschulleitung kann damit einhergehende Aufgaben delegieren oder sich bei deren Erfüllung unterstützen lassen. Der Hochschulleitung obliegen Initiierungs-, Planungs-, Kontroll- und Steuerungsaufgaben für den Aufbau, die Aufrechterhaltung und die stetige Verbesserung des Sicherheitsprozesses, dazu gehören:

- die Verabschiedung einer übergeordneten Leitlinie zur Informationssicherheit, die u. a. mess- und überprüfbare Sicherheitsziele, eine Sicherheitsstrategie zur Erreichung dieser Ziele und die Organisationsstruktur der IS enthält,
- sich über den Status quo der IS informieren zu lassen, insbesondere über Risiken und Konsequenzen aufgrund fehlender Sicherheitsmaßnahmen,
- die Bereitstellung ausreichender Ressourcen für eine Umsetzung der Sicherheitsstrategie, darunter sowohl finanzielle, personelle, technische als auch zeitliche Ressourcen,
- die Sicherstellung von Schulungs- und Sensibilisierungsmaßnahmen für Mitglieder und Angehörige der Pädagogischen Hochschule Freiburg sowiedie Benennung eines/einer Informationssicherheitsbeauftragten.

4.2 Leiter/in des Zentrums für Informations- und Kommunikationstechnologie

Die zentrale Instanz für die operative IT-Sicherheit ist das Zentrum für Informations- und Kommunikationstechnologie (ZIK). Der/Die ZIK-Leiter/in ist für den sicheren Betrieb der IT und die Umsetzung geeigneter Sicherheitsmaßnahmen verantwortlich. In Zusammenarbeit mit dem/der Informationssicherheitsbeauftragten bringt er/sie die für die IS spezifischen Aspekte und Anliegen ein. Der/Die ZIK-Leiter/in stellt sicher, dass der/die Informationssicherheitsbeauftragte frühzeitig in alle IT-Projekte eingebunden wird.

4.3 Informationssicherheitsbeauftragte/r

Der/Die Informationssicherheitsbeauftragte (ISB) ist für alle Belange der IS zuständig. Die Aufgaben des/der ISB sind insbesondere:

- den Sicherheitsprozess zu steuern und zu koordinieren,
- die Hochschulleitung bei der Erstellung der Leitlinie zur IS zu unterstützen,
- die Erstellung des Sicherheitskonzepts, des Notfallvorsorgekonzepts und anderer Teilkonzepte und System-Sicherheitsrichtlinien federführend zu erarbeiten, sowie weitere Richtlinien und Regelungen zur IS zu erlassen,
- den Realisierungsplan für die Sicherheitsmaßnahmen zu erstellen und deren Realisierung zu initiieren und zu überprüfen,
- der Hochschulleitung und dem Informationssicherheitsmanagement-Team über den Status quo der IS zu berichten,
- sicherheitsrelevante Projekte zu koordinieren,
- sicherheitsrelevante Zwischenfälle zu untersuchen sowie
- Sensibilisierungs- und Schulungsmaßnahmen zur IS zu initiieren und zu steuern.

Der/Die ISB ist rechtlich und organisatorisch unabhängig als Stabsstelle im Prorektorat Transfer, Fortbildung und Digitalisierung angesiedelt, arbeitet fachlich weisungsfrei und ist bei Gefahr im

Verzug befugt, allen Mitgliedern der Hochschule fachliche Weisung zu erteilen. Er/Sie hat unmittelbares Vortragsrecht bei der Hochschulleitung. Ihm/Ihr wird ausreichend Zeit für seine/ihre Aufgaben zugebilligt und ihm/ihr steht ein entsprechendes Sachmittelbudget zur Verfügung. Der/Die ISB erhält Gelegenheit, sich im erforderlichen Maße fortzubilden.

4.4 Informationssicherheitsmanagement-Team

Das Informationssicherheitsmanagement-Team (ISMT) unterstützt und berät den/die ISB in Fragen der IS. Das ISMT trifft sich auf Einladung des/der ISB zumindest vierteljährlich und erstattet anschließend einen schriftlichen Statusbericht an das Rektorat. Dem ISMT gehören neben dem/der ISB zumindest folgende Personen an:

- das zuständige Mitglied der Hochschulleitung,
- Datenschutzbeauftragte/r,
- Leiter/in des ZIK sowie
- Technische/r Leiter/in des ZIK.

4.5 Mitglieder und Angehörige

Alle Mitglieder und Angehörigen der Hochschule haben die Aufrechterhaltung der IS in ihrem Verantwortungsbereich zu gewährleisten. Dafür stellen sie sicher, dass sie alle Maßnahmen, Richtlinien, Standards sowie Verfahren, die der IS dienen auf dem jeweils aktuellen Stand, verstehen und einhalten. Sie müssen verdächtige Aktivitäten, ungewöhnliches Verhalten und alle Sicherheitsverstöße unverzüglich melden – Sie sollten stets aufmerksam sein.

5. Geltungsbereich

Der Geltungsbereich dieser Leitlinie ist der Geltungsbereich des ISMS, wie in der Strukturanalyse des Informationsverbundes der Pädagogischen Hochschule Freiburg beschrieben. Zum Informationsverbund gehören alle Prozesse und Verfahren, die für die Abwicklung der Aufgaben gemäß LHG § 2 notwendig sind, darunter Prozesse und Verfahren aus Forschung, Lehre, Studium, Verwaltung und Weiterbildung wie z. B.:

- Bewerbungs- und Zulassungsmanagement,
- Identitätsmanagement,
- Studierendenmanagement,
- IT-Infrastruktur,
- Prüfungs- und Lehrveranstaltungsmanagement sowie
- übergreifende Anwendungen (Basisdienste).

6. Verpflichtungen

Personen innerhalb des Geltungsbereichs sind auf die Leitlinie und das Sicherheitskonzept verpflichtet. Beides muss bei vertraglichen Beziehungen mit Dritten berücksichtigt werden.

7. Folgen von Zuwiderhandlungen

Verstöße gegen die Leitlinie oder das Sicherheitskonzept gefährden die Sicherheitsziele und Sicherheitsstrategie. Verstöße können unbeabsichtigt und unter Beachtung von Sorgfaltspflichten vorkommen und bleiben in der Regel ohne rechtliche Folgen für die Betroffenen, sofern sie unverzüglich gemeldet werden. Vorsätzliche Verstöße oder fahrlässige Handlungen können zu straf- oder zivilrechtlichen Konsequenzen, zu arbeits- oder dienstrechtlichen Sanktionen sowie zu Regressforderungen führen.

8. Inkrafttreten

Die Version 2025.0.0 der Leitlinie zur Informationssicherheit tritt mit ihrer Veröffentlichung in Kraft.

Beschlossen durch das Rektorat in der Sitzung vom 20.01.2026.

Prof. Dr. Hans-Georg Kotthoff, Rektor