Leitlinie zur Informationssicherheit der Pädagogischen Hochschule Schwäbisch Gmünd

vom 01.08.2025

Inhaltsverzeichnis

Präambel

Für die Aufgabenerfüllung der Pädagogischen Hochschule Schwäbisch Gmünd sind Dienstleistungen der Informationstechnik von zunehmender Bedeutung. Dies führt dazu, dass auch die Abhängigkeit der PH Schwäbisch Gmünd von der Funktionstüchtigkeit der Informationstechnik stetig zunimmt.
Aufgrund dessen ist es unerlässlich, dass die PH Schwäbisch Gmünd umfassende Schutzmaßnahmen ergreift. Um die Anforderungen des Datenschutzes und der Informationssicherheit gleichzeitig zu erfüllen und das Entstehen von parallelen Strukturen zu vermeiden, wird versucht, durch diese Leitlinie ein gemeinsames Vorgehen zu erreichen.

I. Gegenstand der Leitlinie

Die Leitlinie definiert die Informationssicherheitspolitik der PH Schwäbisch Gmünd. Dabei dient sie als Basis für ein Informationssicherheitskonzept und den daraus folgenden Maßnahmen für eine schrittweise Verbesserung und dauerhafte Aufrechterhaltung der Sicherheit im Bereich der Informationstechnik.

Mit ihr werden die Ziele, Grundsätze, Organisationsstrukturen sowie Maßnahmen festgelegt, die für die Etablierung eines ganzheitlichen Informationssicherheitsprozesses der PH Schwäbisch Gmünd erforderlich sind.
Die Informationssicherheitsrichtlinie der PH Schwäbisch Gmünd orientiert sich an der Verwaltungsvorschrift des Innenministeriums von Baden-Württemberg zur Informationssicherheit (VwV Informationssicherheit) in der Fassung vom 10. April 2025 sowie an den allgemeinen Datenschutzbestimmungen des BDSG-neu/EU-Datenschutzgrundverordnung. Sie folgt dem Grundsatz, dass der Aufwand für die Informationssicherheitsmaßnahmen stets in Relation zu dem erzielten Sicherheitsgewinn

und dem Wert der zu schützenden Güter - insbesondere der immateriellen Werte und dem Ruf der Hochschule - zu setzen ist.

Die PH Schwäbisch Gmünd ist als bildungswissenschaftliche Hochschule universitären Profils sowohl Dienststelle des Landes Baden-Württemberg als auch Forschungseinrichtung.

Die Hochschulen des Landes Baden-Württemberg haben sich zur Föderation bwInfoSec zusammengeschlossen, um gemeinsam die Informationssicherheit an den Hochschulen sowie den Kunst- und Kultureinrichtungen des Landes zu verbessern.
Die Föderation hat zum Ziel, Hochschulen bei der Verbesserung der Informationssicherheit zu unterstützen. Dazu werden Informationen geteilt, zentrale Dienste etabliert, gemeinsame Projekte bearbeitet und Hilfestellungen bei Problemen geleistet.

Die PH Schwäbisch Gmünd arbeitet aktiv in der Föderation mit.

Die nachfolgenden Ausführungen stecken den Rahmen der Informationssicherheitspolitik der PH Schwäbisch Gmünd ab.

Die Informationssicherheitspolitik ist die Basis für das Informationssicherheitskonzept, welches Detailmaßnahmen beschreibt. Bei dauernd wechselnden Gefährdungen ist die Aufrechterhaltung der Informationssicherheit eine permanente Aufgabe. Diese erfordert personelle und finanzielle Mittel und die Mitwirkung jedes und jeder Einzelnen.

Anstelle des in der Literatur oft synonym verwendeten Begriffs „IT-Sicherheit“ wird hier die weitergehende Formulierung „Informationssicherheit“ verwendet. Entsprechend der Empfehlung im BSI Standard 200-1 wird Informationssicherheit umfassend und ganzheitlich verstanden, sie umfasst auch die Begriffe „Informations- und Kommunikationstechnik“ und „Informations- und Telekommunikationstechnik“ und bezieht sich auf den Schutz von Informationen jeglicher Art und Herkunft, unabhängig davon, ob diese in technischen Systemen, auf Papier oder in Köpfen gespeichert sind.

II. Geltungsbereich

Die Leitlinie zur Informationssicherheit der PH Schwäbisch Gmünd ist gültig für sämtliche Personen, die Informationen der Hochschule nutzen.

Der sachliche Geltungsbereich erstreckt sich dabei auf sämtliche Anwendungen und Prozesse, die an der PH Schwäbisch Gmünd zum Einsatz kommen, wozu insbesondere der Betrieb von Anlagen, die Durchführung von Versuchen und Experimenten, wissenschaftliche Anwendungen und Simulationen, die Arbeit der Verwaltung und der zentralen Dienste sowie die Kommunikation mit externen Partnern und Auftraggebern gehört.

Die Bedeutung der Informationstechnik für die verschiedenen Anwendungsgebiete ist unterschiedlich hoch. Dementsprechend sind die Auswirkungen von Störungen oder Ausfällen in den einzelnen Anwendungsgebieten von unterschiedlicher Tragweite.

Vor diesem Hintergrund hat für jedes Gebiet eine getrennte Betrachtung und Analyse der Informationssicherheit zu erfolgen.

Die Leitlinie gilt auch für kooperierende Einrichtungen, insofern sich deren Benutzung auf die Informationssicherheit der Hochschule auswirkt.

III. Sicherheitsgrundsätze

Die PH Schwäbisch Gmünd hat die Umsetzung der Informationssicherheit gemäß IT-Grundschutz nach BSI Standards zum Ziel (BSI Standard 200-2 „IT-Grundschutz-Vorgehensweise“).

Die PH Schwäbisch Gmünd wird aufgrund von Partnerschaften mit Industrie und Hochschulen in anderen Ländern, welche den nationalen Standard nicht kennen, eine Umsetzung von ISO 27001 auf Basis des BSI Grundschutze anstreben, um beide Normen gleichzeitig zu erfüllen.

Um der Verwaltungsvorschrift der Landesregierung zur Informationssicherheit (VwV Informationssicherheit) des Landes Baden-Württemberg zu entsprechen, werden die Sicherheitsgrundsätze dieser Vorschrift wie folgt übernommen:

- Alle Dienststellen und Einrichtungen der Landesverwaltung Baden-Württemberg bekennen sich zur Informationssicherheit und zur Umsetzung in Anlehnung an den IT-Grundschutz (BSI Standard 200-2 „IT-Grundschutz-Vorgehensweise“).
- Für die Landesverwaltung Baden-Württemberg wird ein Informationssicherheitsmanagementsystem (ISMS) in Anlehnung an die internationalen Standards (ISO = International Organization for Standardization) unter Berücksichtigung des nationalen BSI Standards 200-1 „Managementsysteme für Informationssicherheit“ eingeführt (ISO 27001 in der Ausprägung BSI IT-Grundschutz). Dieses ISMS umfasst Ressourcen, Prozesse und Konzepte für die Informationssicherheit in der Landesverwaltung Baden-Württemberg. Deshalb wird auch die PH Schwäbisch Gmünd ein internes ISMS aufbauen und dieses mit dem Landeskonzept abstimmen.
- Die Ebenen-übergreifende Zusammenarbeit zwischen Bund, Ländern und Kommunen wird berücksichtigt.
- Die Notfallvorsorge orientiert sich am BSI Standard 200-4 („Business Continuity Management“).
- Informationssicherheit erfordert personelle, organisatorische, rechtliche und technische Maßnahmen.
- Informationssicherheit ist als kontinuierlicher Prozess zu gestalten. Der Prozess umfasst insbesondere die mindestens jährlich dokumentierte Überprüfung der Umsetzung und Wirksamkeit von Sicherheitsmaßnahmen und gegebenenfalls erforderliche Anpassungen.
- Der Zugriff auf IT-Systeme, -Anwendungen, Daten und Informationen ist unter Abwägung des Schutzbedarfs und der Wirtschaftlichkeit auf den unbedingt erforderlichen Personenkreis zu beschränken. Jede/jeder Bedienstete sowie Mitglieder und Angehörige der Hochschule erhalten nur auf diejenigen Daten und Informationen die Zugriffsberechtigungen, die zur Erfüllung der jeweiligen Aufgaben erforderlich sind.
- Beim Einsatz von Informationstechnik sind Verfügbarkeit, Vertraulichkeit und Integrität im jeweils erforderlichen Maße zu erreichen. Dazu sind angemessene und dem Stand der Technik entsprechende Sicherheitsmaßnahmen zu ergreifen.
- Notwendige Sicherheitsmaßnahmen sind auch dann anzuwenden, wenn sich daraus Beeinträchtigungen für die Nutzung von IT-Systemen ergeben.

- Die angemessene Sicherheit der in der Landesverwaltung Baden-Württemberg eingesetzten IT-Verfahren ist neben der Leistungsfähigkeit und Funktionalität zu gewährleisten. Bleiben im Einzelfall trotz der Sicherheitsvorkehrungen Risiken untragbar, ist an dieser Stelle auf den IT-Einsatz zu verzichten.
- Lösungen zur Erreichung von Sicherheitszielen sollen das Restrisiko verkleinern. Sie müssen angemessen und wirtschaftlich vertretbar sein.

IV. Sicherheitsstrategie

Mit der Sicherheitsstrategie der PH Schwäbisch Gmünd soll das notwenige Sicherheitsniveau mit wirtschaftlichem Ressourceneinsatz erreicht sowie gehalten werden. Hierzu wird durch die Einführung eines ISMS ein kontinuierlicher Prozess etabliert, der sicherstellt, dass das Sicherheitsniveau den jeweiligen Anforderungen jederzeit bedarfsgerecht angepasst und fortgeschrieben wird. Wesentliche Elemente dieses ISMS sind Planung, Umsetzung, Überprüfung und Aufrechterhaltung des Prozesses.

Dabei kann anstelle der Umsetzung aller Maßnahmen des IT-Grundschutzes auch ein risikobasierter Ansatz gewählt werden. Dabei werden die Risiken klassifiziert und bewertet und in der Folge genau diejenigen Maßnahmen ergriffen, die notwendig sind, um das Risiko auf ein tragbares Maß zu reduzieren.

V. Informationssicherheitsziele

In Anlehnung an die Landesrichtlinie zur Informationssicherheit und den Datenschutz ist auf den IT-Einsatz zu verzichten, wenn trotz Sicherheitsvorkehrungen Risiken untragbar sind.
Ein sinnvoller Einsatz von Ressourcen ist daher nur möglich, wenn von Anfang sowohl die Informationssicherheit als auch der Datenschutz gewährleistet sind.

1. Investitionsschutz

Die Umsetzung dieser Richtlinie stellt auch einen Investitionsschutz dar, das heißt, die Erhaltung der in Technik, Informationen, Arbeitsprozesse und Wissen investierten Werte wird gewährleistet.
Forschung und die Entwicklung von Konzepten für Bildungseinrichtungen setzen voraus, dass diese Konzepte auch den gesetzlichen Vorgaben und damit einem entsprechenden Datenschutzniveau und der Informationssicherheit entsprechen. Andernfalls sind die Ergebnisse nicht für den Einsatz in Bildungseinrichtungen geeignet.
Um den Investitionsschutz in der Forschung und Entwicklung von Konzepten zu gewährleisten, müssen die Informationssicherheit und der Datenschutz „by Design“ erfolgen. Die Informationssicherheit stellt somit einen maßgeblichen Faktor für die Entwicklungen in der Forschung dar.

2. Verfügbarkeit der Informationstechnik

Technische Systeme (Hardware, Software und Daten) besitzen eine begrenzte Verfügbarkeit. Dabei ist organisatorisch festzulegen, welche Ausfallzeiten akzeptabel und unter dem Gesichtspunkt der Wirtschaftlichkeit vertretbar sind. In Abhängigkeit dieser Forderungen sind geeignete Maßnahmen zu ergreifen, die in den akzeptierten zeitlichen Grenzen einen Wiederanlauf ermöglichen. Daten sind in mehrstufigen Verfahren so zu sichern, dass nach menschlichem Ermessen ein grundsätzlicher Verlust ausgeschlossen werden kann.

Um den Betrieb und die Aufrechterhaltung der Sicherheit gewährleisten zu können ist neben den technischen Systemen eine ausreichende personale Ausstattung erforderlich. Die Maßnahmen haben sich daher an dem zur Verfügung stehenden Personal zu orientieren.

3. Integrität von Daten

Unbefugte oder unbemerkte Veränderungen von Daten, sei es durch Personen oder technische Fehler, sollen ausgeschlossen sein. Es wird erwartet, dass Daten weder irrtümlich noch mutwillig manipuliert werden. Je nach Anwendung sind deshalb geeignete technische und organisatorische Maßnahmen zu ergreifen, um die Integrität von Daten zu erhalten.

4. Vertraulichkeit von Daten

Die PH Schwäbisch Gmünd verarbeitet unterschiedlichste vertrauliche Informationen. Um einen möglichst effektiven Zugriffsschutz zu gewährleisten sind geeignete technische, organisatorische und personelle Maßnahmen in den Anwendungen, dem IT-Netz, den Arbeitsplatzcomputern und auf den Übertragungswegen zu treffen.

5. Einhaltung gesetzlicher Auflagen

Die PH Schwäbisch Gmünd hat eine Vielzahl gesetzlicher Auflagen (u.a. Datenschutz, Arbeitssicherheit) zu erfüllen. Um die gesetzlichen Bestimmungen einhalten zu können ist erforderlich, dass die IT-Systeme und die dazu erlassenen organisatorischen Regelungen entsprechend der gesetzlichen Regelung ausgelegt werden.

VI. Verantwortlichkeiten und Organisationsstruktur

1. Gesamtverantwortung

Die Gesamtverantwortung für die Informationssicherheit und den Datenschutz liegt beim Rektorat.

Das Rektorat, die Abteilungsleitungen sowohl von Forschung und Lehre als auch anderer Abteilungen wie auch die Mitglieder und Angehörige der PH Schwäbisch Gmünd insgesamt wirken darauf hin, dass diese Informationssicherheitsleitlinie und der Datenschutz umgesetzt werden.

Das Rektorat weist den Verantwortlichen die jeweilig notwendigen Ressourcen und Befugnisse zu**,** um die Informationssicherheit umzusetzen.

2. Verantwortung der Benutzer

Jeder Benutzer und jede Benutzerin der Informationstechnik ist für die Sicherheit und den Schutz der Daten im eigenen Verantwortungsbereich verantwortlich. Alle Hochschulmitglieder und Angehörigen der PH Schwäbisch Gmünd sind verpflichtet, bei der Erfüllung der Aufgabe „Informationssicherheit“ kooperativ und verantwortungsbewusst mitzuwirken.

3. Verantwortung der Abteilungsleitung

Das Rektorat ist im Rahmen der Organisationsverantwortung für die Informationssicherheit der PH Schwäbisch Gmünd verantwortlich. Die fachliche Verantwortung für Abteilungen und Verfahren delegiert das Rektorat aber an jeweils einen Abteilungsleiter(-in).

Das heißt die Verantwortung für die Informationssicherheit liegt beim jeweiligen Verantwortlichen für das Verfahren bzw. Abteilung.

Die Verantwortlichen werden dabei vom Informationssicherheitsbeauftragten beraten.

4. Verantwortung der Lehrenden an der PH Schwäbisch Gmünd

Die PH Schwäbisch Gmünd ist als Hochschule sowohl eine Dienststelle des Landes Baden-Württemberg als auch eine Forschungseinrichtung. Da es im Forschungsbereich zu einem Konflikt von Grundrechten, insbesondere zwischen den Persönlichkeitsrechten von einzelnen und dem Recht auf Freiheit von Forschung und Lehre kommt, muss die Verantwortung für die Informationssicherheit und den Datenschutz in der Forschung und Lehre beim Professor bzw. bei der Professorin und allen weiteren Personen, die selbstständige Forschung betreiben, liegen. Deshalb ist jeder Professor bzw. jede Professorin und alle weiteren Personen, die selbstständige Forschung betreiben, kraft Amtes für die Informationssicherheit und den Datenschutz in seinem Bereich verantwortlich.

5. Bestellung eines/einer Informationssicherheitsbeauftragen

Das Rektorat bestellt einen oder eine Informationssicherheitsbeauftragte/n.

Der Informationssicherheitsbeauftragte bzw. die Informationssicherheitsbeauftragte ist für den gesamten Überblick und die Koordination aller Maßnahmen an der PH Schwäbisch Gmünd verantwortlich. Dazu pflegt er bzw. sie in Kooperation mit anderen das ISMS und erstellt für das Rektorat eine gesamte Planung für die notwendigen Maßnahmen.

Die Verantwortung für die Umsetzung liegt aber in der Linienorganisation bzw. den entsprechenden Stellen. Auf Vorschlag des bzw. der Informationssicherheitsbeauftragten weist das Rektorat den Umsetzenden die notwendigen und für die PH Schwäbisch Gmünd möglichen Ressourcen zu.

Der bzw. die Informationssicherheitsbeauftragte ist dafür zuständig, dass die in der Informationsleitline benannten Ziele an der PH Schwäbisch Gmünd umgesetzt werden. Er bzw. sie sorgt dafür, dass angemessene Informationssicherheitsmaßnahmen realisiert, fortentwickelt und überwacht werden.

Der bzw. Die Informationssicherheitsbeauftragte ist deshalb als Stabsstelle beim Rektorat angesiedelt. Der bzw. die ISB arbeitet fachlich weisungsfrei, koordiniert und steuert das Informationssicherheitsmanagement der Hochschule. In Fragen der Informationssicherheit ist er bzw. sie den Hochschulangehörigen gegenüber, durch/über das Rektorat, weisungsbefugt.

Er bzw. sie sorgt zudem für die Erstellung und Pflege des Informationssicherheitskonzepts und die Umsetzung des Maßnahmenkatalogs.

6. Stellvertretung des/der Informationssicherheitsbeauftragten

Um die vorgeschriebenen Fristen bei Meldungen etc. einhalten zu können, bestimmt das Rektorat einen stellvertretenden Informationssicherheitsbeauftragten bzw. eine stellevertretende Informationssicherheitsbeauftragte. Die Stellvertretungsposition kann als zusätzliche Aufgabenbereich/Rolle einem anderen Mitarbeiter bzw. einer anderen Mitarbeiterin zugewiesen werden.

7. Projekt- oder Systeminformationssicherheitsbeauftragte und Bereichsinformationssicherheitsbeauftragte

Das Rektorat kann zudem Projekt- oder Systeminformationssicherheitsbeauftragte und spezifische Bereichsinformationssicherheitsbeauftragte gemäß BSI Standards benennen. Diese Personen sind für die Informationssicherheit der jeweiligen Anwendungen, Verfahren, Systeme oder spezifischer Informationen zuständig bzw. unterstützen den ISB.

Sie arbeiten dabei eng mit der bzw. dem ISB der PH Schwäbisch Gmünd und den Bereichsverantwortlichen zusammen.

8. Informationssicherheits- und Datenschutzteam

Für die Umsetzung wird der Expertenkreis Digitalisierung um die Funktion eines Informationssicherheitsteams und Datenschutzteams erweitert.
Dieses Gremium berät über alle wichtigen IT Projekte an der PH.

VII. Grundpflichten

1. Alle Mitglieder und Angehörige der PH Schwäbisch Gmünd gewährleisten die Informationssicherheit durch verantwortungsbewusstes Handeln und Halten die für die Informationssicherheit relevanten Gesetze, Vorschriften, Richtlinien, Anweisungen sowie vertraglichen Verpflichtungen ein.

2. Sie haben Sicherheitsvorfälle möglichst zu vermeiden und sicherheitsrelevante Ereignisse, soweit diese für sie erkennbar sind, unverzüglich nach Kenntniserlangung der jeweiligen Abteilungsleitung, dem Informationssicherheitsbeauftragten und Datenschutzbeauftragten zu melden, damit schnellstmöglich Abhilfemaßnahmen eingeleitet werden können.

3. Die jeweils für Verfahren Verantwortlichen sorgen dafür, dass verfahrens- bzw. anwendungsbezogene Sicherheitskonzepte erstellt und regelmäßig bedarfsgerecht fortgeschrieben werden. Soweit für einzelne Verfahren keine Sicherheitskonzepte erforderlich sind, wird dies jeweils aktenkundig begründet.

Diese Anforderung ergibt sich insbesondere aus der EU-Datenschutz-Grundverordnung. Gemäß den Bestimmungen der EU-Datenschutz-Grundverordnung verfolgt die PH Schwäbisch Gmünd mit der Erstellung eines Sicherheitskonzepts das Ziel, dass die Verantwortlichen die jeweils verarbeiteten Daten, deren Schutzbedarf und die mit der Verarbeitung verbundenen Risiken sowie die zugehörigen Rechtsgrundlagen kennen und darüber auskunftsfähig sind.

4. Bei Beeinträchtigungen der Informationssicherheit ergreifen die jeweils Verantwortlichen unverzüglich die zur Aufrechterhaltung bzw. Wiederherstellung des IT-Betriebs und der Informationssicherheit geeigneten und angemessenen Maßnahmen.

5. Notwendige Sicherheitsmaßnahmen sind auch dann anzuwenden, wenn sich daraus Beeinträchtigungen für die Nutzung von IT-Systemen ergeben.

6. Die angemessene Sicherheit der an der PH Schwäbisch Gmünd eingesetzten Verfahren ist neben der Leistungsfähigkeit und Funktionalität zu gewährleisten. Bleiben im Einzelfall trotz der Sicherheitsvorkehrungen Risiken untragbar, ist an dieser Stelle auf den Einsatz zu verzichten.

Sicherheitshinweise und -Handlungsanleitungen des bzw. der Informationssicherheitsbeauftragten sind unverzüglich an alle Betroffenen im eigenen Zuständigkeitsbereich weiterzuleiten.

7. Eine Dokumentationspflicht wird in Zusammenarbeit mit anderen Beauftragten (Arbeitsschutz, Qualitätsmanagement etc.) im Sinne eines integrieren Dokumentationsmanagement festgelegt und vom Rektorat genehmigt. Dies kann sowohl eine allgemeine Mindestversion als auch eine spezifische detaillierte Version für einzelne Bereiche sein.

Bei der Erstellung werden die anderen Beauftragten, der Personalrat und andere Bereiche einbezogen, um die Bedürfnisse von allen zu erfüllen.

Ziel ist es die notwendige Dokumentation zu erhalten, ohne den Geschäftsbetrieb durch verschieden Dokumentationen zu belasten.

8. Sich hieraus ergebende Regeln sind für alle Nutzer der IT-Infrastruktur der PH Schwäbisch Gmünd bzw. der einzelnen Bereiche und insbesondere für die Beschäftigten verbindlich.

VIII. Berichtswege

1. In Abstimmung mit der MIZ-Leitung erhält das Rektorat durch den bzw. die Informationssicherheitsbeauftragte jährlich einen Managementbericht für den Stand der Informationssicherheit an der PH Schwäbisch Gmünd.

2. Auf Aufforderung des MWK erhält auch dieses den Bericht.

3. Eine Vorlage an andere Personen/Einrichtungen erfolgt nur, wenn diese ein berechtigtes Interesse an der Vorlage des Berichts geltend machen können. Die Entscheidung hierbei trifft das Rektorat.

4. Der Informationssicherheitsbeauftragte berichtet außerdem dem Expertenkreis Digitalisierung.

5. Für Sicherheitsvorfälle gilt der allgemeine mit dem Datenschutzbeauftragten abgestimmte Prozess.

6. Das weitere Berichtswesen wird im Sicherheitskonzept dokumentiert und vom Rektorat freigeben.

IX. Umsetzungsplan

Der Umsetzungsplanung wird im Sicherheitskonzept und im ISMS-Tool dokumentiert sowie fortgeführt und muss jederzeit dem Rektorat zur Prüfung zur Verfügung stehen bzw. zur Verfügung gestellt werden.

Der Umsetzungsplan ist mit den ausführenden Abteilungen abzustimmen und mindestens jährlich zusammen mit dem Managementbericht dem Rektorat vorzulegen und von diesem zu genehmigen.

X. Inkrafttreten

Das Rektorat hat mit Beschluss vom 01.07.2025 diese Leitlinie beschlossen.
Die Leitlinie tritt rückwirkend zum 01.07.2025 in Kraft.

Schwäbisch Gmünd, den 01.08.2025

gez. Prof. Dr. Kim-Patrick Sabla-Dimitrov
Rektor