Alice Salomon Hochschule Berlin
University of Applied Sciences

AMTLICHES MITTEILUNGSBLATT

04/2026 **12.02.2026**

Informationssicherheitsleitlinie*

der Alice-Salomon-Hochschule Berlin

*) Von der Hochschulleitung auf der Sitzung am 12.02.2026 beschlossen.

HERAUSGEBERIN: Präsidentin der Alice-Salomon-Hochschule Berlin
ANSCHRIFT: Alice-Salomon-Platz 5, 12627 Berlin, Tel.: (030) 992 45-0

Informationssicherheitsleitlinie

1. Stellenwert der Informationsverarbeitung

Der mit Hilfe geeigneter Informations- und Kommunikationstechnik durchgeführten Verarbeitung von Informationen kommt an Hochschulen eine Schlüsselrolle bei der Erfüllung der Aufgaben in Studium und Lehre, Forschung und Transfer sowie in der Administration zu. Alle Bereiche der Alice-Salomon-Hochschule Berlin verarbeiten in ihren Prozessen, Verfahren oder Abläufen Informationen.
Die Hochschulleitung erkennt an, dass sich die Risiken und die zu erwartenden Auswirkungen bei der Informationsverarbeitung verändern und im schlimmsten Fall für die Hochschule eine existenzielle Bedrohung darstellen können.
Mit Veröffentlichung dieser Informationssicherheitsleitlinie mit den Informationssicherheitszielen der Hochschule unterstreicht die Hochschulleitung die Bedeutung der Informationssicherheit für die Hochschule und bestätigt die Übernahme der Gesamtverantwortung für den Informationssicherheitsprozess.
Die vorliegende Leitlinie beschreibt die allgemeinen Grundsätze, Ziele und Sicherheitsmaßnahmen, die für die Initiierung, Etablierung und Aufrechterhaltung eines ganzheitlichen Informationssicherheitsprozesses an der ASH Berlin erforderlich sind.
IT-Sicherheit ist von herausragender Bedeutung für die Kernprozesse der Hochschule in den Bereichen "Studium und Lehre" sowie "Forschung". Besonders wichtig ist sie darüber hinaus im Hinblick auf personenbezogene Daten, die dort bzw. in zugehörigen Unterstützungsprozessen verarbeitet werden.

2. Grundsätze der Informationssicherheit

Informationssicherheit bezeichnet den Schutz aller Informationen – unabhängig davon, ob sie elektronisch, schriftlich oder mündlich vorliegen – vor unbefugtem Zugriff, Verlust, Manipulation oder Zerstörung. Sie umfasst organisatorische, technische und personelle Maßnahmen und dient dazu, Risiken für Informationen und informationsverarbeitende Prozesse auf ein vertretbares Maß zu reduzieren.
Ziel der Informationssicherheit ist es, die Risiken, die auf die folgenden drei Grundwerte einwirken, auf ein vertretbares Maß zu reduzieren. Die Informationssicherheit umfasst neben der Sicherheit der IT-Systeme und der darin gespeicherten Daten auch die Sicherheit von nicht elektronisch verarbeiteten Informationen. Die Grundwerte der Informationssicherheit lauten:

Vertraulichkeit: Informationen dürfen nur dem berechtigten Personenkreis zur Verfügung stehen resp. zur Verfügung gestellt werden.

Integrität: Die Unversehrtheit von Informationen ist sicherzustellen.

Verfügbarkeit: Die Nutzung von Informationen muss dem berechtigten Personenkreis im benötigten Zeitraum mit der erforderlichen Güte möglich sein.

3. Informationssicherheitsziele

Die Hochschulleitung initiiert den Aufbau eines Informationssicherheitsmanagementsystems (ISMS), das sich an den Vorgaben der Standards des BSI (200-1 zu Managementsystemen und 200-2 zur IT-Grundschutzmethodik sowie 200-3 zum Risikomanagement und 200-4 zum Notfallmanagement) orientiert.
In diesen Aufbauprozess des ISMS, also dem Einführen, Umsetzen und Verankern der Standards, sollen schrittweise alle Organisationseinheiten der ASH Berlin einbezogen werden, damit das Primärziel sicher zu realisieren ist. Das ISMS-Team führt regelmäßige Prüfungen der Organisationseinheiten der ASH Berlin durch, um zu bewerten, inwieweit sie besonders sensible Informationen verarbeiten und welchen Bedrohungen diese ausgesetzt sein könnten. Im Rahmen einer anschließenden Risikoanalyse wird dann bewertet, wie die

Informationen vor diesen Bedrohungen geschützt werden und welche zusätzlichen Schutzmaßnahmen noch erforderlich sind. Dabei wird das ISMS-Team von den jeweiligen Organisationseinheiten unterstützt.
Auf Basis dieser Risikoanalyse nimmt die Hochschulleitung eine Priorisierung der Organisationseinheiten bei der Einbeziehung in den Informationssicherheitsprozess vor. Im Sinne einer iterativen Vorgehensweise wird der Sicherheitsprozess in den Organisationseinheiten schrittweise etabliert.

Resultierend aus diesem primären Ziel der ISMS-Einführung ergeben sich folgende Informationssicherheitsziele, die dessen Umsetzung konkret unterstützen:

- **Gewährleistung eines einheitlichen Standards für die Informationssicherheit:** Ziel ist es, durch verbindliche schriftliche Regeln und Verfahren ein konsistentes und unternehmensweites Sicherheitsniveau sicherzustellen. Die Informationssicherheitsleitlinie sowie ergänzende Handbücher zum ISMS sollen hierbei als zentrale Orientierung dienen.
- **Sicherstellung, dass alle Bereiche und Nutzer_innengruppen von IT-Sicherheitsbedrohungen geschützt sind:** Alle Bereiche und Nutzer_innengruppen werden durch geeignete Maßnahmen vor IT-Sicherheitsbedrohungen geschützt, um Sicherheitslücken und Angriffsflächen systemweit zu minimieren.
- **Einhaltung von Gesetzen, Vorschriften, Leitlinien und Persönlichkeitsrechten:** Verstöße gegen Gesetze und Vorschriften können zu Strafen und Sanktionen führen, daher wird auf die Berücksichtigung und Einhaltung von Gesetzen und Vorschriften besonders geachtet.
- **Sicherstellung der funktionalen Aufgabenerfüllung:** Ausfälle und Fehler in IT-Systemen und Anwendungen können die Erfüllung von Aufgaben und Tätigkeiten erheblich beeinträchtigen und sind daher zu vermeiden.
- **Schutz von sensiblen und vertraulichen Daten:** Sensible Daten, insbesondere auch personenbezogene Daten sowie Dienst- und Amtsgeheimnisse, sind gemäß Art. 9 DSGVO ein wichtiges Gut und dürfen nicht in unbefugte Hände gelangen.
- **Sicherung der unwiederbringlichen Werte der verarbeitenden Information:** Ziel ist der Schutz verarbeiteter Informationen mit hohem Schutzbedarf, deren Verlust oder unautorisierte Veränderung nicht wiederherstellbare Schäden verursachen würde.
- **Sensibilisierung aller Angehörigen der Hochschule:** Informationssicherheit kann an der Hochschule nur etabliert werden, wenn alle Angehörigen der Hochschule aktiv mitwirken. Ein erklärtes weiteres Ziel ist es, alle Angehörigen der Hochschule im erforderlichen Umfang zu sensibilisieren und zu qualifizieren, um notwendige Kompetenzen bezüglich der Informationssicherheit aufzubauen bzw. zu vertiefen.

Die umzusetzenden Sicherheitsmaßnahmen müssen in einem wirtschaftlich vertretbaren Verhältnis zum Schaden stehen, der durch einen Sicherheitsvorfall erwartet wird. Zu bewerten sind dabei die Auswirkungen des Sicherheitsvorfalls auf die **körperliche und seelische Unversehrtheit von Menschen**, das **Recht auf informationelle Selbstbestimmung**, **finanzielle Schäden, Beeinträchtigungen des Ansehens der Hochschule** sowie die **Folgen von Gesetzesverstößen** und **Beeinträchtigungen der Aufgabenerfüllung**.
Die genaue Bewertung und Gegenüberstellung dieser Kriterien wird in der Richtlinie zum Risikomanagement festgelegt.

4. Informationssicherheitsrollen und -verantwortlichkeiten

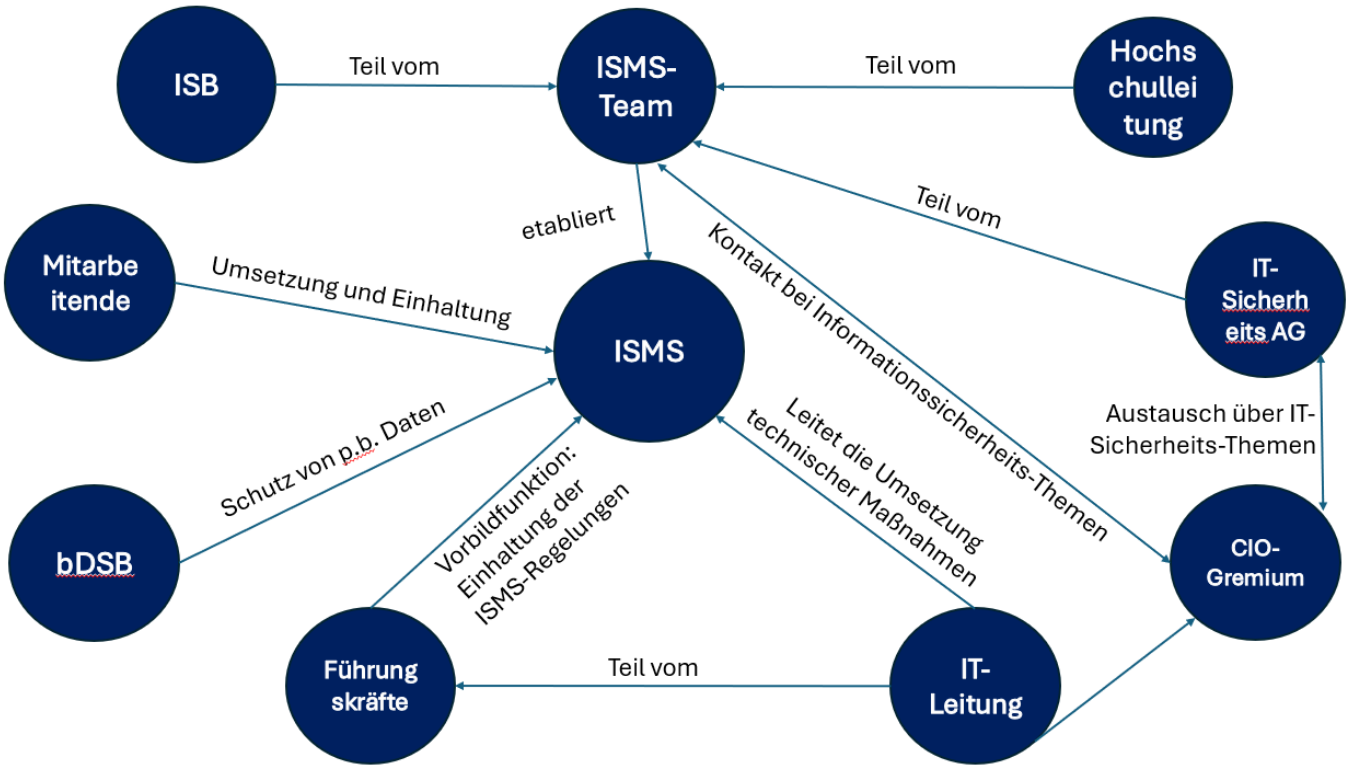

Diagramm: Kommunikation im ISMS

ISMS-Team

Das ISMS-Team ist für die Umsetzung der Informationssicherheit verantwortlich. Es kümmert sich um den Betrieb, Umsetzung, Verbesserung und Weiterentwicklung des ISMS.
Das Team setzt sich aus den folgenden wesentlichen Rollen des ISMS zusammen:

- der_dem ISB;
- der Hochschulleitung;
- den Mitgliedern der IT-Sicherheits-AG;
- der IT-Leitung;
- ausgewählten Führungskräften

Die Aufgaben müssen dabei nicht immer vom gesamten ISMS-Team ausgeübt werden, sondern können auf die Mitglieder aufgeteilt werden. Für die Sicherstellung, dass alle Aufgaben vom ISMS-Team wahrgenommen werden, ist der_die Informationssicherheitsbeauftragte/-r (ISB) verantwortlich.

Informationssicherheitsbeauftragte/-r (ISB)

Die Hochschulleitung benennt eine_n Informationssicherheitsbeauftragte_n, der_die über eine geeignete Fachkompetenz zur Informationssicherheit verfügt. Er_Sie ist für alle operativen Belange und Fragen der Informationssicherheit der Hochschule zuständig und stellt die fortlaufende Berücksichtigung der drei Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit sicher. Der_Die ISB berichtet in seiner_ihrer Funktion direkt an die Hochschulleitung. Der_Die ISB kann extern beauftragt werden.

Hochschulleitung

Die Hochschulleitung ist aufgrund ihrer Gesamtverantwortung für die Risikovorsorge an der Hochschule und somit auch für die Informationssicherheit verantwortlich. Die Hochschulleitung erlässt verbindliche Regeln zur Informationssicherheit für die ASH Berlin und gibt sie den Mitarbeitenden und Studierenden bekannt. Diese Regeln werden auf der Webseite unter dem Punkt „Informationssicherheit“ in Form von Informationsmaterialien und Anleitungen abgelegt.

Die Hochschulleitung stellt jederzeit eine Möglichkeit zur Kenntnisnahme der aktuellen Regeln sicher. Zudem werden von der Hochschulleitung benötigte Ressourcen für die Informationssicherheit bereitgestellt.
Die Hochschulleitung hat die Verantwortung, eine IT-Sicherheits-AG einzurichten.

IT-Sicherheits-AG

Die Mitglieder der IT-Sicherheits-AG unterstützen den_die ISB bei strategischen Entscheidungen wie beispielsweise der Bestimmung der Sicherheitsziele, der Sicherheitsstrategie und der Erstellung und Anpassung des Sicherheitskonzeptes. Die Mitglieder der IT-Sicherheits-AG werden durch die Hochschulleitung benannt. Es finden monatliche Treffen statt, bei denen die operativen Maßnahmen in Form einer Maßnahmenliste besprochen werden. Im Kontext der Informationssicherheit finden sie sich quartalsweise zusammen.

CIO-Gremium

Das CIO-Gremium ist ein operativ arbeitendes Expert_innengremium, das von dem_der Kanzler_in geleitet wird. Die dort zu treffenden Maßnahmen leiten sich von strategischen Entscheidungen der Hochschulleitung ab. Der_die Kanzler_in berichtet der Hochschulleitung über die Umsetzung der Maßnahmen. Die Orientierung an einer digitalen Agenda soll das digitale Arbeiten auf allen Ebenen und in allen Bereichen der Hochschule durch den Einsatz einer zukunftsfähigen digitalen Infrastruktur und dazugehöriger Services gewährleisten. Das CIO-Gremium wirkt als Treiber und Berater bei der Weiterentwicklung des Informationssicherheitsprozesses und erarbeitet Entscheidungsvorlagen über die Priorisierung von Projekten sowie die Wirtschaftlichkeit und Effizienz von eingesetzten Maßnahmen für die Hochschulleitung.

Rolle Führungskräfte in Technik, Service, Verwaltung, Lehre und Forschung

Führungskräfte nehmen eine Vorbildfunktion ein und sind für die Einhaltung der ISMS-Regelungen sowie die Umsetzung von Sicherheitsmaßnahmen in ihren Bereichen / Abteilungen verantwortlich. Zudem tragen sie Verantwortung dafür, dass die Regeln den Beschäftigten zur Verfügung gestellt werden, sie regelmäßig, z.B. in Team-Meetings, sensibilisiert werden und dass die Beschäftigten geschult sind.

Rolle IT-Leitung

Die IT-Leitung ist für die zentrale Umsetzung der technischen Maßnahmen aus der Informationssicherheit verantwortlich. Sie ist für die Koordinierung der IT-Abteilung zuständig. Die IT-Leitung ist gleichzeitig eine Führungskraft.

Rolle betrieblicher Datenschutz-Beauftragter

Der_Die betriebliche Datenschutz-Beauftragte (bDSB) berät die oberste Leitung zu allen Angelegenheiten des Datenschutzes. Im Rahmen des ISMS wirkt der_die bDSB bei der Einhaltung zur Absicherung von personenbezogenen Daten mit. Der_die bDSB kann extern beauftragt werden.
Der bDSB wird bei Bedarf in den ISMS-Prozess eingebunden. Datenschutzrelevante Fragen und Probleme werden in der Regel bereits außerhalb der ISMS-Treffen behandelt, weshalb der bDSB nicht regelmäßig an diesen Sitzungen teilnimmt, es sei denn, es werden Themen besprochen, die ihn betreffen.

Rolle Mitarbeiter_innen in Technik, Service, Verwaltung, Lehre und Forschung

Die Mitarbeiter_innen sind für die Umsetzung und Einhaltung der Regelungen für die Informationssicherheit und des ISMS im Rahmen ihrer täglichen Arbeit verantwortlich.
Die Aufgaben und Pflichten für diese Rolle werden für die Mitarbeiter_innen im ISMS-Handbuch-Endbenutzer im Abschnitt Organisation und Ansprechpartner im ISMS näher beschrieben und kommuniziert.

Risikoeigentümer_innen

Die Risikoeigentümer_innen sind Personen oder Organisationseinheiten, die Verantwortung und Rechenschaftspflicht für einen bestimmten Prozess oder Risiko tragen und für dessen Überwachung, Bewertung und Minderung zuständig sind. Zudem ist diese Rolle eine Schlüsselfigur, um sicherzustellen, dass Informationssicherheitsrisiken erkannt, bewertet und durch gezielte Maßnahmen wirksam behandelt werden, um Vertraulichkeit, Integrität und Verfügbarkeit von Informationen zu gewährleisten. Die Risikoeigentümer_innen besitzen eine ausreichende Budgetverantwortung und haben die Befugnis, die Umsetzung von Maßnahmen zu genehmigen und Rest-Risiken für die Organisation zu akzeptieren.

5. Sicherheitsmaßnahmen

Verteilen von Verantwortlichkeiten

Für alle Prozesse, Verfahren, Informationen, IT-Anwendungen und IT-Systeme wird eine verantwortliche Person entsprechend der Organisationsstruktur benannt, die den jeweiligen Schutzbedarf bestimmt und Zugriffsberechtigungen festlegt und regelmäßig überprüft. Dies dient der eindeutigen Nachverfolgbarkeit bei der Vergabe von Zugriffsberechtigungen. Für alle verantwortlichen Funktionen sind Vertretungen zu benennen. Es muss durch Unterweisung und angemessene Dokumentation sichergestellt sein, dass Vertretungen ihre Aufgaben erfüllen können.

Zutrittskontrollen

Gebäude und Räumlichkeiten werden durch angemessene Zutrittskontrollen geschützt. Der Zugang zu IT-Systemen wird durch angemessene Zugangskontrollen und der Zugriff auf die Informationen durch ein Berechtigungskonzept geschützt. Auf allen IT-Systemen wird, soweit technisch möglich, ein geeigneter Schutz vor Schadsoftware eingesetzt. Alle Internetzugänge werden durch eine geeignete Firewall gesichert. Alle Schutzprogramme werden so konfiguriert und administriert, dass sie einen effektiven Schutz darstellen und Manipulationen verhindert werden.

Schulung und Sensibilisierung

Die Angehörigen der Hochschule informieren sich durch bereitgestellte Dokumentationen, wie diese Informationssicherheitsleitlinie oder die ISMS Handbücher, und nehmen regelmäßig an Schulungen zur korrekten Nutzung der IT-Dienste und den hiermit verbundenen Sicherheitsmaßnahmen teil. Die Informationen zu den Maßnahmen finden sich auf der Webseite im Bereich der Informationssicherheit wieder. Die Hochschulleitung unterstützt dabei die bedarfsgerechte Fort- und Weiterbildung.

Datensicherungen zur Wahrung der Verfügbarkeit

Wenn Sicherheitsrisiken auftreten (bekannte oder drohende Angriffe), kann die Verfügbarkeit von Informationen entsprechend dem Bedrohungs- und Schadensrisiko vorübergehend eingeschränkt werden. Im Interesse der Funktionsfähigkeit der gesamten Hochschule ist der Schutz vor Schäden vorrangig. Informationsverluste können nie vollkommen ausgeschlossen werden. Durch eine umfassende Datensicherung und regelmäßige Wiederherstellungsübungen wird daher gewährleistet, dass beeinträchtigte Prozesse oder Arbeitsabläufe kurzfristig wiederaufgenommen werden können, wenn Teile des operativen Datenbestandes verlorengehen oder offensichtlich fehlerhaft sind.

Schutzbedarfsfeststellung

Die Feststellung des Schutzbedarfs erfolgt auf Basis eines standardisierten Verfahrens nach den Vorgaben des IT-Grundschutzes. Für jedes informationsverarbeitende System, jede Anwendung und jedes Verfahren wird ein Schutzbedarf ermittelt, der die Vertraulichkeit, Integrität und Verfügbarkeit der verarbeiteten Informationen berücksichtigt.

Risikomanagement

Ein systematisches Risikomanagement wird eingerichtet, um sicherheitsrelevante Risiken frühzeitig zu identifizieren, zu bewerten und durch geeignete Maßnahmen zu behandeln. Dabei wird ein kontinuierlicher Verbesserungsprozess (KVP) genutzt. Die Verantwortung für die Durchführung liegt bei den jeweiligen Systemverantwortlichen, Anwendungsverantwortlichen und Verfahrensverantwortlichen in Zusammenarbeit mit dem Informationssicherheitsbeauftragten (ISB).

Notfallmanagement

Zur Sicherstellung der Betriebsfähigkeit im Krisen- oder Notfall wird ein Notfallmanagement eingerichtet. Es enthält Regelungen zu Notfallplänen, Wiederanlaufzeiten, Wiederanlaufreihenfolgen und Kommunikationswegen.

6. Fortschreibung des Informationssicherheitsprozesses

Das ISMS-Team prüft das ISMS der ASH Berlin regelmäßig auf seine Aktualität und Wirksamkeit. Daneben untersuchen sie auch die Maßnahmen regelmäßig daraufhin, ob sie den betroffenen Angehörigen der Hochschule bekannt sind und ob sie umsetzbar und in den Hochschulablauf integrierbar sind. Die Hochschulleitung unterstützt die ständige Verbesserung des Sicherheitsniveaus. Alle Angehörigen der Hochschule sind angehalten, mögliche Verbesserungen oder Schwachstellen an das Informationssicherheitsteam oder den ISB weiterzugeben. Durch eine kontinuierliche Revision der Regelungen und deren Einhaltung wird das angestrebte Sicherheitsniveau sichergestellt. Abweichungen werden mit dem Ziel analysiert, die Sicherheitssituation zu verbessern und ständig auf dem aktuellen Stand der Informationssicherheitstechnik zu halten. Dieser Prozess wird durch den Plan-Do-Check-Act (PDCA)-Zyklus unterstützt, der einen kontinuierlichen Verbesserungsprozess beschreibt. Dabei werden Sicherheitsmaßnahmen geplant, umgesetzt, überprüft und bei Bedarf angepasst, um ein wirksames und nachhaltiges ISMS sicherzustellen. Durch diesen systematischen Ansatz wird gewährleistet, dass Risiken fortlaufend bewertet und Maßnahmen entsprechend der aktuellen Bedrohungslage sowie organisatorischer Anforderungen verbessert werden.
Alle Angehörigen der Hochschule setzen die festgelegten Maßnahmen durch eine sicherheitsbewusste Arbeitsweise um und informieren bei Auffälligkeiten die entsprechend festgelegten Stellen.

7. Inkrafttreten

Diese Informationssicherheitsleitlinie für die ASH Berlin tritt am Tag ihrer Veröffentlichung in den Amtlichen Mitteilungen in Kraft. Die vorliegende Informationssicherheitsleitlinie wurde von der Hochschulleitung am 12.02.2026 beschlossen.

Sie ergänzt die Mitteilung zu den Informationssicherheitszielen, Amtliche Mitteilung 08/2025 vom 20.02.2025

Prof. Dr. B. Völter, Präsidentin