

Weisung zur Daten- und Informationsklassifizierung der Universität Basel

vom Rektorat genehmigt am 17. September 2024

Gestützt auf § 4 Abs. 1 lit. b der Informationssicherheitsordnung der Universität vom 31. Januar 2019 und auf § 8 des Gesetzes über die Information und den Datenschutz des Kantons Basel-Stadt vom 9. Juni 2010 erlässt das Rektorat die folgende Weisung:

§ 1 Zweck

¹ Diese Weisung regelt die Zuweisung von Informationen zu einer Schutzklasse mit dem Ziel die Vertraulichkeit der Informationen zu schützen.

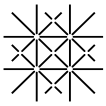
² Die Schutzklasse bestimmt die zum adäquaten Schutz der Informationen erforderlichen Massnahmen.

§ 2 Geltungsbereich

¹ Diese Weisung ist für alle Mitarbeitenden der Universität verbindlich. Sie gilt sinngemäss für Mitarbeitende der universitären Spitäler und Kliniken sowie der Assoziierten Institute im Zusammenhang mit ihrer universitären Tätigkeit. Dritte (inkl. Studierende, die im Rahmen einer Qualifikationsarbeit an universitären Forschungsprojekten arbeiten) sind entsprechend schriftlich zu verpflichten.

§ 3 Definitionen

- **Informationen:** Informationen sind alle Aufzeichnungen (z.B. geschäftsrelevante Unterlagen, Personal- und Studierendendaten, Forschungsdaten, Gebäudepläne, etc.), die bei der Erfüllung von Aufgaben der Universität Basel und ihrer Gliederungseinheiten empfangen oder erstellt werden. Die Qualifikation als Information ist unabhängig von der Darstellungsform und dem Informationsträger (Papier, elektronisch).
- **Personendaten:** Informationen, die sich auf eine bestimmte oder bestimmbare Person beziehen. Unterkategorie der Informationen.
- **Besondere Personendaten:** Personendaten, bei denen wegen ihrer Bedeutung, der Art ihrer Bearbeitung oder der Möglichkeit ihrer Verknüpfung mit anderen Informationen die besondere Gefahr einer schwerwiegenden Persönlichkeitsverletzung besteht.
- **Bearbeitung von Informationen:** Jeder Umgang mit Informationen, unabhängig von den angewandten Mitteln und Verfahren, beispielweise das Erstellen, Kopieren, Zugänglichmachen, Übermitteln, Aufbewahren, und Vernichten.
- **Informationseignerin / Informationseigner:** Die Informationseignerin bzw. der Informationseigner ist jene Person, die aufgrund ihrer Tätigkeit innerhalb der Universität für das Bearbeiten der Informationen verantwortlich ist.
- **IT-Dienste:** Eine Dienstleistung, die von einem IT-Service-Provider (z.B. universitäre IT-Services, sciCORE, Dritte) angeboten wird. Ein Dienst wird durch den Leistungsbeschreibung (u.a. Verfügbarkeit des Dienstes) beschrieben.
- **Schutzbedarf:** Der Schutzbedarf der Daten ergibt sich aus dem Risiko, welches mit der Verletzung der Vertraulichkeit von Informationen einhergeht.



§ 4 Verantwortlichkeiten

¹ Die Universität trägt die Gesamtverantwortung für den rechtlich korrekten, sicheren und vertraulichen Umgang mit Informationen.

² Die Verantwortung für die Umsetzung dieser Weisung tragen die Personen mit Leitungsfunktion für ihren jeweiligen Zuständigkeitsbereich. Sie stellen sicher, dass die Informationseignerinnen bzw. Informationseigner über ihre Pflichten zur Klassifizierung von Informationen und der Anwendung adäquater Schutzmassnahmen informiert sind.

³ Die Universität stellt Informations- und Schulungsunterlagen zum rechtlich korrekten, sicheren und vertraulichen Umgang mit Informationen bereit. Durch den regelmässigen Austausch mit den universitären Organisationseinheiten wird die konforme Umsetzung der Weisung sichergestellt.

§ 5 Schutzklassen auf Basis der Vertraulichkeit

¹ Die Klassifizierung von Informationen an der Universität Basel beruht in erster Linie auf dem Schutzziel der Vertraulichkeit. Vertraulichkeit heisst, nur befugte Personen dürfen Zugang zu den Informationen erhalten.

² Die vier Schutzklassen bezüglich Vertraulichkeit an der Universität sind:

- **Klasse 0** (kein Risiko): Öffentliche bzw. für die Öffentlichkeit bestimmte Informationen, wobei die Kenntnisnahme jeder Person gestattet ist.
- **Klasse I** (tiefes Risiko): Interne Informationen, die innerhalb einer bestimmten Gruppe durch jede Person zur Kenntnis genommen werden können, jedoch nicht für die Öffentlichkeit bestimmt sind. Bei einer allfälligen Veröffentlichung der Information oder der Bekanntgabe der Informationen an Personen ausserhalb der Universität sind keine oder nur geringe negative Auswirkungen auf den Betrieb sowie keine wesentlichen Reputations- oder materiellen Schäden für die Universität oder für Individuen zu erwarten.
- **Klasse II** (moderates Risiko): Vertrauliche Informationen, nur für autorisierte Personen oder Gruppen von autorisierten Personen bestimmt, und Personendaten. Bei einer allfälligen Veröffentlichung der Informationen oder der Bekanntgabe der Informationen an unautorisierte Personen besteht das Risiko von negativen Auswirkungen auf den Betrieb, Reputations- oder materiellen Schäden für die Universität wie für Individuen und Persönlichkeitsverletzungen.
- **Klasse III** (hohes Risiko): Geheime Informationen, aufgrund von gesetzlichen oder vertraglichen Geheimhaltungspflichten nur für autorisierte Personen bestimmt, besondere Personendaten und Datensammlungen von Personendaten, welche grösser sind als 10'000. Bei einer allfälligen Veröffentlichung oder der Bekanntgabe der Informationen an unautorisierte Personen besteht die Gefahr schwerwiegender Einschränkungen der Handlungsfähigkeit der Universität, schwerwiegende Reputations- oder materielle Schäden für die Universität oder für Individuen und schwerwiegende Persönlichkeitsverletzungen.

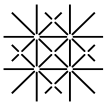
³ Bei zusammenhängenden Informationen mit unterschiedlichem Schutzbedarf ist jene Klasse mit dem höheren Schutz zu wählen.

⁴ Im Einzelfall kann eine Information, unter Beachtung von § 7, mit sachlicher Begründung und nach Abwägung der Risiken, auch einer anderen Klasse zugewiesen werden.

§ 6 Verwendung geeigneter Dienste für die Datenbearbeitung

¹ Die Universität schützt die Informationen und die darauf aufbauenden Geschäftsprozesse mittels infrastrukturellen, organisatorischen, personellen und technischen Massnahmen.

² Grundsätzlich können Informationen bis und mit Klasse II auf der von den IT-Services (ITS) und von sciCORE im internen Netz bereitgestellten universitären Infrastruktur bearbeitet werden. Die Informationseignerin bzw. der Informationseigner ist verantwortlich, im Einzelfall zu prüfen, ob der



gewählte Dienst die Anforderung an die Vertraulichkeit der betreffenden Informationen ausreichend gewährleistet.

³ Die Universität publiziert einen «Service-Katalog», in welchem ersichtlich ist, welche Dienste welche Schutzklassen bieten.

⁴ Für Informationen der Klasse III muss im Einzelfall in Absprache mit den ITS bzw. sciCORE überprüft werden, wie und auf welcher Infrastruktur die Daten bearbeitet werden können.

§ 7 Klassifizierung

¹ Die Informationseignerin bzw. der Informationseigner hat hinsichtlich der Vertraulichkeit von Informationen folgende Pflichten:

- a) Sie bzw. er soll Informationen der Klassen II und III entsprechend klassifizieren und gemäss §8 deklarieren, sobald sie bzw. er diese weitergibt, versendet, bekanntgibt, etc.. Nicht deklarierte Informationen gelten als der Klasse I (tiefes Risiko) zugewiesen.
- b) Vor der Bearbeitung und insbesondere vor der Weitergabe und Aufbewahrung einer erhaltenen und nicht deklarierten Information soll sie bzw. er im Einzelfall überdenken, ob die Zuteilung zur Klasse I plausibel scheint. Informationen, die eines höheren Schutzes bedürfen, sind der Klasse II oder III zuzuweisen und entsprechend zu deklarieren. Bei fehlender Zuständigkeit (z.B. versehentlichem Mailempfang, Auffinden vergessener Unterlagen auf Drucker, etc.) sind die Informationen an die verantwortliche Informationseignerin bzw. den verantwortlichen Informationseigner zurückzugeben. Falls dies nicht möglich ist, sind die Informationen zu vernichten.
- c) Bei einer bereits klassifizierten Information soll sie bzw. er ausschliesslich dann eine Änderung zu einer tieferen Klasse vornehmen, wenn dies sachlich begründet ist und die bestehende Klassifizierung nicht gesetzlich oder vertraglich vorgeschrieben ist.
- d) Nur Dienste für die Bearbeitung der Informationen zu wählen, die gemäss «Service-Katalog» ausreichende Schutzmassnahmen sicherstellen (siehe § 6 Abs. 4). Bei nicht im «Service-Katalog» enthaltenen Diensten ist der Informationseigner bzw. die Informationseignerin für die Prüfung der ausreichenden Schutzmassnahmen selber verantwortlich.

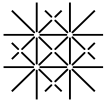
§ 8 Deklaration von Informationen

¹ Die Deklaration von Informationen der Klasse II und III kann auf Ebene von einzelnen Informationen (z.B. Brief, Datei, E-Mail, Intranet-Seite) oder auf Ebene von zusammenhängenden Informationen (z.B. Dokumenten-Ordner, Intranet-Bereich, ADAM-Workspace, Aktenschrank) erfolgen.

² Einzelne Informationen, die nicht / nicht mehr Teil von zusammenhängenden Informationen sind, müssen einen entsprechenden Vermerk in einer geeigneten Form aufweisen. Dabei ist auf eine klare Erkennbarkeit des Vermerks zu achten, um anderen Personen einen der zugeteilten Klasse entsprechenden Umgang zu ermöglichen.

³ Briefe und E-Mails, die Informationen der Klasse II oder III enthalten, müssen im Betreff entsprechend gekennzeichnet werden («Vertraulich» bei Klasse II und «Geheim» bei Klasse III).

⁴ Die Deklaration von einzelnen Informationen sowie von zusammenhängenden Informationen innerhalb von Informationssystemen (z.B. Netz-/Gruppenlaufwerk, Intranet, ADAM, Datenbanken) erfolgt durch Metadaten (z.B. Dateiname, Schlagwort, Ordner-Bezeichnung).



§ 9 Schlussbestimmung

¹ Diese Weisung tritt per 01. Oktober 2024 in Kraft und gilt für alle Personen, die nach dem 01. Oktober 2024 M365 nutzen. Sie gilt spätestens per 01. Oktober 2025 für alle Mitarbeitenden der Universität.

² Vor dem 1. Oktober 2025 generierte Informationen und Informationsbestände, die nicht klassifiziert sind, gelten in Übereinstimmung mit § 7 Abs. 1 lit. a) als der Klasse I zugewiesen. Informationseignerinnen und Informationseigner sind verpflichtet, diese Informationen und Informationsbestände bis spätestens 1. Oktober 2027 zu prüfen und sie der korrekten Klasse zuzuweisen. ¹

¹ § 9 Abs. 2 eingefügt mit Rektoratsbeschluss vom 9. September 2025, in Kraft per 16. September 2025.