Universität Zürich[UZH]

Weisung zur Klassifizierung von Informationen

(vom 21.05.2021)

Die Universitätsleitung, gestützt auf § 56, Abs.4 der Universitätsordnung[1]*, beschliesst:*

1 Klassifizierung von Informationen

Die Universität Zürich ist gemäss § 7 des Gesetzes über die Information und den Datenschutz vom 12. Februar 2007 (IDG, LS 170.4) und § 12 der Verordnung über die Informationsverwaltung und -sicherheit vom 3. September 2019 (IVSV, LS 170.8) verpflichtet, die Sicherheit von Informationen zu gewährleisten. Damit sie die Informationen technisch und organisatorisch angemessen schützen kann, muss deren Schutzbedarf bekannt sein. Dieser ist durch die Klassifizierung von Informationen mit Bezug auf folgende Schutzziele zu ermitteln:

- **Vertraulichkeit:** Informationen dürfen nicht unrechtmässig zur Kenntnis gelangen.
- **Integrität (Unversehrtheit):** Informationen müssen richtig und vollständig sein, Veränderungen von Informationen müssen erkennbar und nachvollziehbar sein.
- **Verfügbarkeit:** Informationen müssen bei Bedarf vorhanden sein.
- **Zurechenbarkeit:** Informationsbearbeitungen müssen einer Person zugrechnet werden können, bei der Übertragung von Informationen bedeutet dies, dass die Informationsquelle ihre Identität bewiesen hat und der Empfang der Nachricht nicht in Abrede gestellt werden kann.

2 Begriffe

Dokumente/Unterlagen	Aufzeichnungen, die bei der Erfüllung von Aufgaben der Universität Zürich und ihrer Organisationseinheiten entstehen. Die Qualifikation als Unterlage oder Dokument ist unabhängig von der Darstellungsform und dem Informationsträger (Papier, elektronisch). Es kann sich dabei um Schriftgut, Bilder, Fotos, Pläne, Tondokumente etc. handeln.
Fachanwendung (Fachapplikation)	Software, die der Universität Zürich und ihren Organisationseinheiten zur Verwaltung geschäftsrelevanter Daten dient (beispielsweise Stammdatenverwaltung) und über fachspezifische Funktionen verfügt.
Geschäftsverwaltungssystem (Records Management System)	Software, die neben den Funktionalitäten einer Geschäftskontrolle auch die digitale Dokumenten- bzw. Dossierverwaltung ermöglicht. Die elektronische Geschäftsverwaltung umfasst somit drei Elemente: dossierbezogene Aktenführung, Ablaufsteuerung und Geschäftskontrolle.
Informationen	Einzelne Aufzeichnungen (Unterlagen, Dokumente).

[1] LS 415.111

Informationsbestände	Sammlung gleichförmiger Aufzeichnungen bzw. Informationen.
Informationsverwaltung	Gesteuertes und geordnetes Erstellen, Bearbeiten, Ablegen, Archivieren, Vernichten, Suchen und Finden von geschäftsrelevanten Informationen.
Registraturplan (Ordnungssystem, Aktenplan)	Systematische Einteilung der anfallenden Unterlagen nach Aufgaben und Prozessen einer Organisationseinheit. Der Registraturplan steuert die Ablage der einzelnen Dossiers und kann für die Festlegung von Verantwortlichkeiten, Zugriffsrechten, Aufbewahrungsfristen, Standorten usw. verwendet werden.

3 Klassifzierungsstufen pro Schutzziel

3.1 Vertraulichkeit

Für das Schutzziel «Vertraulichkeit» müssen alle Informationen einer Organisationseinheit einer der folgenden vier Klassifzierungsstufen zugeordnet werden:

- **Öffentlich:** Als öffentlich gelten alle Informationen, die von der zuständigen Stelle (z.B. durch die Universitätsleitung, die Abteilung Kommunikation oder eine Fakultät) zur Veröffentlichung frei gegeben bzw. von ihr bereits publiziert sind (z.B. Erlasse, öffentliche Statistiken, Geschäftsbericht oder andere Informationen, die auf dem Internet frei verfügbar sind). Bis zur Publikation sind alle Informationen zumindest als intern zu klassifizieren.
- **Intern:** Interne Informationen sind für Angehörige der UZH bestimmt und innerhalb der UZH bzw. innerhalb einer Organisationseinheit frei zugänglich, nicht aber für die Öffentlichkeit. Interne Informationen sind z.B. Inhalte auf Lehr- bzw. Lernplattformen (sofern keine Leistungs- und Verhaltensdaten erkennbar sind), interne Weisungen und Regelungen, Informationen zu Gebäuden und Infrastruktur oder nicht vertrauliche Finanzdaten sowie weitere Daten bzw. Informationen, die der internen Organisation oder Administration dienen (z.B. Inventarlisten etc.).
- **Vertraulich:** Als vertraulich gelten Informationen, die nur einem begrenzten, explizit festgelegten Kreis von Personen innerhalb der UZH zugänglich sind. Beispiele für vertrauliche Unterlagen sind etwa Personaldossiers oder andere Informationen im Zusammenhang mit der Personaladministration, die in der Regel Personendaten oder besonders schützenswerte Personendaten enthalten (Bewerberdaten, Mitarbeiterbeurteilungen, Informationen zu Lohn, Gesundheit oder Religion von Mitarbeitenden), ausserdem Daten von Studierenden (z.B. akademische Arbeiten, Prüfungen und deren Bewertungen), personenbezogene oder aus anderen Gründen vertraulich zu haltende Forschungsdaten oder vertrauliche Informationen zur Strategie, Finanzen und Infrastruktur, ebenso wie dem Fernmeldegeheimnis unterstehende Informationen (z.B. Logdaten). Ebenfalls als vertraulich zu klassifizieren sind Informationen zu Kernaufgaben, Schwerpunktthemen, Projekten und Vorhaben einzelner Organisationseinheiten, Informationen zur internen Organisation und Administration oder zu Sitzungsgefässen und Gremien, die nur einem eingeschränkten Empfängerkreis zugänglich sein dürfen.

- **Geheim:** Als geheim klassifiziert werden Informationen, die dem Berufsgeheimnis gemäss Art. 321 StGB resp. Art. 321bis StGB oder anderen Geheimhaltungsverpflichtungen unterstehen (z.B. Patientendaten und Krankengeschichten des Zentrums für Zahnmedizin ZZM, Autopsie-/ Laborberichte sowie Gutachten des Instituts für Rechtsmedizin IRM, Laborberichte des Instituts für Medizinische Mikrobiologie IMM sowie andere personenbezogene Forschungsdaten der Humanmedizin und Psychologie, Geheimhaltungsverpflichtungen in Verträgen betr. Lizenzen / Immaterialgüterrechte). Ebenso als geheim gelten Informationen, die aus sonstigen Gründen streng vertraulich behandelt werden müssen und deshalb nur einem sehr engen Kreis von Personen zugänglich sind (z.B. Informationen/Unterlagen zu laufenden Gerichts- oder Vertragsverhandlungen oder Daten, deren Bekanntwerden den Meinungsbildungsprozess in den Organen der UZH beeinträchtigen könnten).

Mindestens für alle Informationen die als «geheim» klassifiziert werden, müssen auch die Klassifizierungsstufen der Schutzziele Integrität (Unversehrtheit), Verfügbarkeit und Zurechenbarkeit ermittelt werden.

3.2 Integrität (Unversehrtheit)

- **Normal:** Mögliche Auswirkungen unbefugter oder unbeabsichtigter Veränderungen der Informationen sind akzeptabel. Ein sorgfältiger Umgang mit Informationen im Tagesgeschäft, sowie die Anwendung von Basisschutzmassnahmen (wie Audit-Trail, Zugriffsschutz und Backup) werden als ausreichende Sicherheitsmassnahmen betrachtet. Gilt als Standardwert für alle Informationen, die bezüglich Integrität (Unversehrtheit) nicht als «hoch» eingestuft sind.
- **Hoch:** Unbefugte oder unbeabsichtigte Veränderungen der Informationen sind nicht akzeptabel. Sie müssen verhindert oder mindestens erkannt werden.

3.3 Verfügbarkeit

- **Tief:** Verfügbarkeit > 96.0%, resp. Ausfalldauer max. 350 Stunden / Jahr
- **Normal:** Verfügbarkeit > 98.5%, resp. Ausfalldauer max. 131 Stunden / Jahr
- **Hoch:** Verfügbarkeit > 99.5%, resp. Ausfalldauer max. 44 Stunden / Jahr
- **Sehr hoch:** Verfügbarkeit > 99.9%, resp. Ausfalldauer max. 9 Stunden / Jahr

Die Stundenberechnung basiert auf 365 Tagen à 24 Stunden und beinhaltet alle Unterbrüche inklusive geplanter Wartungsarbeiten.

3.4 Zurechenbarkeit

- **Normal:** Die Informationsbearbeitung muss einer Person zugerechnet werden können. Für die Informationsübertragung sind keine Massnahmen zum Identitätsnachweis erforderlich.
- **Hoch:** Die Zuordnung zu einer identifizierten Person bei der Bearbeitung ist Voraussetzung, ebenfalls der Identitätsnachweis bei der Informationsübertragung.

4 Schutzbedarf

Aus der ermittelten Klassifizierungsstufe pro Schutzziel ergibt sich der Schutzbedarf der Informationen und es sind die erforderlichen organisatorischen und technischen Schutzmassnahmen abzuleiten.

4.1 Normaler Schutzbedarf

Der normale Schutzbedarf beinhaltet organisatorische und technische Massnahmen zum Schutz der Informationen. Das sind etwa die Zugriffserteilung via Benutzendenverwaltung nach dem need-to-know-Prinzip oder der Zutrittsschutz mittels Zutritts- oder Schliesskonzept sowie das Erstellen regelmässiger Backups und die Auswahl geeigneter Anwendungen zur Informationsverwaltung.

4.2 Erhöhter Schutzbedarf

Informationen mit erhöhtem Schutzbedarf müssen mit weiteren technischen oder organisatorischen Massnahmen geschützt werden. Das sind etwa:

- für das Schutzziel **Vertraulichkeit:** die Definition und Vergabe restriktiver Berechtigungen, die Verschlüsselung sowie die Anonymisierung bei der Übermittlung,
- für das Schutzziel **Integrität (Unversehrtheit):** die Zuweisung und Steuerung der Zugriffsrechte oder deren Protokollierung und Überwachung sowie Änderungen, sowie eine bedarfsgerechte Datensicherung
- für das Schutzziel **Verfügbarkeit:** der Aufbau von Redundanzen sowie die Umsetzung von Vorsorgemassnahmen für Ausfälle und Notfälle,
- für das Schutzziel **Zurechenbarkeit:** die Verwendung digitaler Zertifikate und Signaturen oder von Logfiles

Die Massnahmen für den erhöhten Schutzbedarf werden in Zusammenarbeit mit der Zentralen Informatik bzw. den dezentralen IT-Verantwortlichen in den Organisationseinheiten definiert und implementiert.

5 Vorgehen bei der Klassifizierung der Informationen

5.1 Grundsatz

Aspekte der Verhältnismässigkeit, der Wirtschaftlichkeit und der Risikobeurteilung werden sowohl bei der Klassifizierung wie auch bei der Definition von Massnahmen zum Schutz von Informationen angemessen berücksichtigt.

5.2 Schutzziel Vertraulichkeit

5.2.1 Klassifizierung von Informationsbeständen

Die Klassifizierung kann ganze Informationsbestände umfassen: z.B. Personaldossiers, Forschungsprojekte zu einem Fachgebiet, Anfragen an den Rechtsdienst, Auswertungen und Statistiken zu einer Dienstleistung oder Sitzungsunterlagen aus einem Gremium der Universität Zürich. In diesem Fall gilt die ermittelte Klassifzierungsstufe für alle zum Informationsbestand gehörenden Aufzeichnungen.

Anwendungsbeispiel 1:
Ein Informationsbestand wird als «vertraulich» klassifiziert. Diese Klassifzierungsstufe gilt für alle zu diesem Informationsbestand gehörenden Elemente (z.B. Fälle, Projekte, einzelne Dokumente) und für alle darin enthaltenen Aufzeichnungen.

Anwendungsbeispiel 2:
Ein Informationsbestand wird als «vertraulich» klassifiziert. Diese Klassifzierungsstufe gilt für alle zu diesem Informationsbestand gehörenden Elemente (z.B. Fälle, Projekte, einzelne Dokumente) und für darin enthaltenen Aufzeichnungen.
Werden in einem einzelnen Element aus diesem Informationsbestand Aufzeichnungen als «geheim» klassifiziert, werden sie gemäss Ziffer 5.2.2 gekennzeichnet. Das einzelne Element (nicht aber der Informationsbestand) gilt als «geheim» und wird unter Berücksichtigung der Verhältnismässigkeit auf die übrigen Schutzziele überprüft.

Anwendungsbeispiel 3:
Ein Informationsbestand wird als «geheim» klassifiziert. Diese Klassifzierungsstufe gilt für alle zu diesem Informationsbestand zugehörigen Elemente (z.B. Fälle, Projekte, einzelne Dokumente) und für alle Aufzeichnungen, die dazu bearbeitet werden. Für den Informationsbestand müssen die weiteren Schutzziele überprüft werden.

5.2.2 Klassifizierung von einzelnen Dokumenten

Kann nicht ein gesamter Informationsbestand klassifiziert werden, oder gilt innerhalb eines Informationsbestandes für einzelne Dokumente eine abweichende (in der Regel höhere) Klassifizierungsstufe, wird die Klassifizierung auf Stufe Dokument vorgenommen und vermerkt. Zur Kennzeichnung der betreffenden Dokumente gibt es verschiedene Möglichkeiten:

- Nutzung von Standardvorlagen der jeweiligen Organisationseinheit, in denen die Klassifizierung markiert werden kann
- Kennzeichnung an geeigneter Stelle im Dokument (z.B. im Titel, als Wasserzeichen oder in der Kopf- oder Fusszeile des Dokuments)
- Kennzeichnung bzw. Labelling von Dokumenten und Datensätzen, die in Fachanwendungen geführt werden
- Kennzeichnung über den Registraturplan (nach dem Vererbungsprinzip), z.B. in einem Geschäftsverwaltungssystem

Auf die Kennzeichnung einzelner Dokumente mit den Klassifizierungen ‘öffentlich’ oder ‘intern’ kann verzichtet werden, wenn sich die Klassifizierung selbsterklärend aus dem Dokument oder der Anwendung ergibt (z.B. öffentliche Medienmitteilung sind selbsterklärend ‘öffentlich’, interne Kommunikation/Anträge etc. sind selbst selbsterklärend ‘intern’ solange nicht anders klassifiziert) sofern praktische Gründe und Wirtschaftlichkeit gegen die Kennzeichnung sprechen.

Nicht gekennzeichnete Dokumente sind mindestens gemäss Schutzziel ‘intern’ zu handhaben, ausser die Informationseigner haben sie bereits veröffentlicht.

5.3 Prüfung der Schutzziele Integrität (Unversehrtheit), Verfügbarkeit und Zurechenbarkeit

Die Klassifizierung mit Bezug auf das Schutzziel Vertraulichkeit (öffentlich, intern, vertraulich, geheim) wird auf einzelne Informationen und Informationsbestände angewendet. Bei der Klassifizierung mit Bezug auf die Schutzziele Integrität, Verfügbarkeit und Zurechenbarkeit erfolgt die Klassifizierung ggf. auf Stufe der Anwendung. Das Vorgehen hängt von der betroffenen Information bzw. dem betroffenen Informationsbestand ab.

5.4 Dokumentation der Klassifizierung

Die Ergebnisse der Klassifizierung sowie allfällige Massnahmen zum Schutz der Informationen müssen angemessen dokumentiert werden.

6 Geltungsbereich

Die Weisung ist für alle Organisationseinheiten der Universität Zürich verbindlich. Organisationseinheiten der Universität Zürich sind die Organe und Gremien der Universität, der Fakultäten und Institute und alle ihnen unterstellten Organisationseinheiten.

7 Verantwortlichkeiten

Die Leitungen der Fakultäten, Institute, der Zentralen Dienste (ZDU) und weiterer Organisationseinheiten der Universität Zürich sorgen dafür, dass die Grundsätze dieser Weisung in ihrer Organisationseinheit angewendet werden. Sie bestimmen die Informationseigner innerhalb ihrer Organisationseinheit.

Die Informationseigner sind verantwortlich für die Informationen und Informationsbestände in ihrem Zuständigkeitsbereich und für deren Klassifizierung. Sie setzen insbesondere auch die im Kapitel Controlling beschriebenen Massnahmen zur Pflege der Dokumentation um. Sie können Aufgaben delegieren.

Der Chief Information Security Officer (CISO), resp. die Zentrale Informatik bzw. die dezentralen IT-Verantwortlichen in den Organisationseinheiten unterstützen die Informationseigner bei Fragestellungen zur Informationssicherheit, resp. technologischen Themen und beraten sie in Bezug auf erforderliche Massnahmen.

Die Mitarbeitenden der Universität Zürich wenden die Grundsätze dieser Weisung an.

8 Controlling und Pflege

Die Informationseigner führen mindestens alle zwei Jahre eine Überprüfung der Klassifizierung ihrer Informationen und Informationsbestände und der Schutzmassnahmen durch. Sie berücksichtigen dabei ausdrücklich auch neu dazugekommene Informationen und Informationsbestände.

9 Umsetzung, Frist

Die Weisung zur Klassifizierung von Informationen tritt per 01.09.2023 in Kraft.
Die Klassifizierung von Informationen und Informationsbeständen gemäss dieser Weisung erfolgt erstmals im Rahmen des Projekts «Erhebung Informationsbestände gemäss IDG» und soll bis Ende 2025 abgeschlossen sein. Sobald eine Organisationseinheit die Initialklassifizierung durchgeführt hat, sind Ziff. 7 und Ziff.8 anwendbar.