



IT-Architektur

Die Universität Zürich will ein gemeinsames Verständnis für IT-Architektur entwickeln und fördern. Die Architektur-Prinzipien unterstützen darin, gemeinsame Lösungen und Standards voranzutreiben und gleichzeitig lokale Innovationen zu ermöglichen. Dies hilft, die IT-Komplexität und -Kosten in der gesamten Universität zu reduzieren und Freiräume für Neues zu schaffen.

Allgemeine Grundsätze

Reuse before Reinvent

Bevor Neues entwickelt wird, sollen - sofern sinnvoll - bestehende Services und zentrale Dienste genutzt werden.

Erläuterung:

- Die Verwendung bestehender Services spart Zeit und Kosten (keine Ressourcen für Neuentwicklung).
- Der Aufwand für Wartung und Support wird reduziert: bestehende Systeme sind bereits getestet und etabliert.
- Durch Vermeidung von Redundanzen wird die IT-Landschaft weniger komplex; die Nachhaltigkeit wird gefördert.

Produktneutralität

Vorgaben und Architekturentscheidungen sind grundsätzlich produktneutral.

Erläuterung: Produktneutralität minimiert die Abhängigkeiten von einem spezifischen Hersteller und trägt so zu einem fairen und offenen Wettbewerb bei.

Offene Standards

Offene Standards sind gegenüber proprietären Lösungen zu bevorzugen.

Erläuterung:

- Die Nutzung offener Standards ermöglicht herstellerunabhängige Interoperabilität und Flexibilität.
- Nutzende sind nicht an einen einzelnen Anbieter gebunden.
- Verschiedene Systeme können einfacher miteinander kombiniert werden.

Transparenz und Nachvollziehbarkeit

Architektur-Dokumentation und -entscheide sind transparent, nachvollziehbar und wo sinnvoll zugänglich.

Erläuterung:

- Transparenz und Nachvollziehbarkeit ermöglichen den Austausch und eine gute Zusammenarbeit.
- Die Governance wird verbessert, Audits erleichtert.

Lifecycle-Management

Lifecycle-Management wird für Komponenten jeden Layers umgesetzt.

Erläuterung:

- Dank Lifecycle-Management werden Informatikmittel/Daten über ihren gesamten Lebenszyklus effizient, sicher und kosteneffektiv genutzt sowie regelmässig gewartet und bei Bedarf ersetzt.
- Dadurch erhöht sich die Betriebssicherheit; Risiken werden minimiert.
- Die IT passt sich so nachhaltig an sich ändernde Geschäftsanforderungen an.

Modularität

Komponenten werden modular aufgebaut, d.h. in unabhängige, klar abgegrenzte Module unterteilt. Jedes Modul übernimmt eine spezifische Aufgabe.

Erläuterung: Modulare Komponenten ermöglichen eine einfache Integration, fördern die Wiederverwendbarkeit und vereinfachen Anpassungen, Testing oder auch den Austausch einzelner Komponenten.

Security

Integrale Sicherheit

Sicherheit wird über die gesamte Lebensdauer eines Systems bewertet und umgesetzt. Das System wird als Ganzes betrachtet (nicht nur bestimmte Layers).

Erläuterung: Die Sicherheitsaspekte eines Systems werden umfassend und abgestimmt betrachtet bzw. gesteuert. Sicherheitsbereiche werden verknüpft und so koordiniert, dass sie optimal zusammenwirken und sich gegenseitig ergänzen. Damit wird ein höheres Sicherheitsniveau erreicht als durch isolierte Einzelmassnahmen.

Wirksame Sicherheit

Das kontinuierliche Managen von Risiken ermöglicht es, sinnvolle, wirksame und standardisierte Sicherheitsmassnahmen umzusetzen.

Erläuterung: Wirksame Sicherheit entsteht durch das Zusammenwirken folgender Aspekte:

- geeignete Schutzmassnahmen
- regelmässige Überprüfungen
- eine Kultur, in der alle Beteiligten Verantwortung für die Sicherheit übernehmen.

So werden unvermeidbare Risiken zuverlässig abgewehrt oder auf ein akzeptables Mass reduziert.

Security by Default

Informatikmittel werden so entwickelt, konfiguriert und betrieben, dass sie dem «Security by Default»-Prinzip Rechnung tragen. Dies gilt auch für Testsysteme.

Erläuterung:

- Informatikmittel werden mit sicheren Voreinstellungen ausgeliefert und Nutzer so vor gängigen Cyberbedrohungen geschützt.
- Sicherheitslücken durch fehlerhafte Konfigurationen werden minimiert.

Sicherheitsvorgaben einhalten, Ausnahmen kennen

Die Einhaltung gesetzlicher, regulatorischer und interner Sicherheitsrichtlinien ist verbindlich. Sicherheitsausnahmen sind bewertet, bewilligt und terminiert.

Erläuterung:

- Die Einhaltung der Sicherheitsvorgaben sorgt für ein hohes Mass an Sicherheit und Verlässlichkeit im täglichen Arbeiten.
- Ausnahmen werden ermöglicht; dies erlaubt flexibles und angemessenes Handeln in besonderen Situationen.
- So werden Routine und Ausnahmefälle optimal abgedeckt; die Sicherheit ist dauerhaft gewährleistet.

Least Privilege Ansatz

Nutzende, Systeme und Prozesse erhalten grundsätzlich nur die notwendigen Rechte, die zur Ausführung ihrer Aufgaben erforderlich sind. Logins für UZH-Dienste, -Anwendungen und -Computer, die über das Internet zugänglich sind, erfordern eine Multifaktor-Authentifizierung (MFA).

Erläuterung:

- Das Risiko von Datenmissbrauch, unbefugtem Zugriff und der Ausbreitung von Schadsoftware wird deutlich reduziert, da Angreifer/Fehler weniger Möglichkeiten haben, Schaden anzurichten.
- Die Angriffsfläche der Universität Zürich wird so minimiert.

Künstliche Intelligenz (KI)

Künstliche Intelligenz unterstützt – Führung und Kontrolle bleiben beim Menschen

Erläuterung:

- Trotz Automatisierung und intelligenter Analysen bleibt der Mensch als Kontrollinstanz unerlässlich.
- Die Synergie zwischen KI und menschlicher Kompetenz wird gefördert.
- Kritische Entscheidungen werden stets durch einen Menschen überprüft.

Sinnvoller Einsatz künstlicher Intelligenz

Erläuterung: Der durchdachte und gezielte Einsatz künstlicher Intelligenz hat zum Ziel, die Geschäftsprozesse zu optimieren und zu vereinfachen.

Sichere künstliche Intelligenz

KI-Systeme erfüllen die Sicherheitsanforderungen der Universität Zürich, sowie die gesetzlichen und ethischen Vorgaben.

Erläuterung:

- Der Schutz sensibler Daten, die Einhaltung von Datenschutz- und Informationssicherheits-Vorgaben sowie die Sicherstellung von Datensouveränität sind zentrale Prinzipien bei der sicheren Nutzung von künstlicher Intelligenz.
- Der Einsatz von Sicherheitsfiltern verhindert Missbrauch.

Transparenz und Kennzeichnung

Der Einsatz von künstlicher Intelligenz (KI) in Systemen der Universität Zürich ist für die Nutzenden ersichtlich.

Erläuterung:

- Nutzende werden klar und verständlich darüber informiert, wenn und wie künstliche Intelligenz eingesetzt wird.
- Transparente Information über den Einsatz und die Funktionsweise der künstlichen Intelligenz fördert das Vertrauen.

Benutzerzentriertes Design

Human-Centered Design

Systeme werden gemäss den Bedürfnissen und im Kontext mit den Anforderungen der Nutzenden gestaltet. Designentscheidungen basieren auf realen Szenarien der Anwender:innen.

Erläuterung: Die konsequente Ausrichtung an die Anforderungen der Nutzenden erhöht die Akzeptanz, verbessert die Prozessqualität und senkt den Schulungsaufwand.

Barrierefreiheit (Accessibility)

Barrierefreiheit ist ein integraler Bestandteil der Gestaltung und wird frühzeitig berücksichtigt.

Erläuterung:

- Die Barrierefreiheit stellt sicher, dass digitale Angebote für alle Nutzengruppen zugänglich sind.
- Dies fördert die Inklusion und entspricht den gesetzlichen Anforderungen.

Build - Test - Learn

Feedbacksysteme, iterative Tests und kontinuierliche Optimierung sind systematisch im Implementierungsprozess verankert.

Erläuterung: Regelmässige und frühzeitige Rückmeldungen der Nutzenden reduzieren Fehlentwicklungen, erhöhen die Qualität und führen zu optimierten Lösungen.

Applikationen & Software as a Service (SaaS)

Always consider Software as a Service (SaaS)

SaaS-Lösungen werden in Erwägung gezogen, wenn sie die funktionalen und nicht-funktionalen Anforderungen sowie die regulatorischen Rahmenbedingungen erfüllen und wirtschaftlich sinnvoll sind.

Erläuterung: Der Einsatz von SaaS-Lösungen reduziert den Entwicklungs- Wartungs- und Bereitstellungsaufwand.

Trennung der Verantwortlichkeiten (Separation of Concerns)

Die Geschäftslogik ist grundsätzlich von der Präsentations- und Datenzugriffsschicht getrennt.

Erläuterung:

- Aufgaben und Verantwortlichkeiten werden in separaten Komponenten oder Schichten organisiert. So bleibt die Geschäftslogik von der Präsentations- und Datenzugriffsschicht getrennt.
- Dies erhöht die Übersichtlichkeit und Flexibilität und vereinfacht die Wartung und Entwicklung.

Versionsverwaltung von Sourcecode

Änderungen am Sourcecode werden durch ein Versionsverwaltungssystem nachvollziehbar dokumentiert und archiviert.

Erläuterung: Der konsequente Einsatz eines Versionsverwaltungssystem ermöglicht die lückenlose Nachverfolgung von Änderungen im Sourcecode, die Wiederherstellung früherer Versionen, eine parallele Entwicklung in Branches sowie eine effektive Zusammenarbeit und Qualitätssicherung im Entwicklungs-Team.

Continuous Integration/Continuous Deployment (CI/CD)

Die Schritte von der Code-Integration über das Unit Testing bis hin zur Bereitstellung in Zielumgebungen sind automatisiert und standardisiert.

Erläuterung:

- Durch automatisierte Integration und automatisiertes Deployment werden manuelle Eingriffe minimiert.
- Fehlerquellen werden reduziert und die Qualität sowie Geschwindigkeit der Softwarebereitstellung nachhaltig gesteigert.
- Kontinuierliche Automatisierung ermöglicht es, Änderungen zuverlässig, reproduzierbar und in kurzen Zyklen auszuliefern. Dies führt zu höherer Produktivität und Kundenzufriedenheit.

Shared Services & Platforms

Platform First

Plattformlösungen sind Einzellösungen vorzuziehen, wenn wiederkehrende Anforderungen adressiert werden.

Erläuterung: Plattformen ermöglichen Synergien, konsistente Umsetzungen und reduzieren Redundanzen über verschiedene Projekte hinweg.

Zentrale und sichere Identity & Access Services

Identitäts- und Zugriffsverwaltung erfolgt zentral, sicher und skalierbar über alle Systeme hinweg.

Erläuterung: Mittels zentraler Zugriffsverwaltung wird eine durchgängige, konsistente Nutzerverwaltung sichergestellt – ein essenzieller Aspekt für Sicherheit, Benutzerkomfort und Governance.

Interoperabilität

Interface-Standardisierung

Die Kommunikation zwischen Systemen, insbesondere der Integrations- und Messaging-Layer folgen klar dokumentierten Schnittstellenstandards.

Erläuterung: Standardisierte Interfaces gewährleisten eine hohe Integrationsfähigkeit, reduzieren den Projektaufwand und beschleunigen die Anbindung neuer Komponenten.

Robuste, entkoppelte Systemkommunikation (Decoupled & Resilient Communication)

Systeme kommunizieren lose gekoppelt über fehlertolerante, asynchrone oder entkoppelte Mechanismen (z. B. Eventing oder Messaging).

Erläuterung: Dies verbessert die Skalierbarkeit, verringert Abhängigkeiten in Echtzeitprozessen und erhöht die Ausfallsicherheit verteilter Systeme.

Daten

Daten haben einen Wert (Data as an Asset)

Daten sind ein strategisches Asset. Sie werden aktiv geschützt und gepflegt. Die Verwendung erfolgt zielgerichtet, um den grösstmöglichen universitären Nutzen zu erzielen.

Erläuterung:

- Daten bilden die Grundlage für fundierte Entscheidungen, Innovationen und universitären Erfolg.
- Daher müssen Daten aktiv geschützt, gepflegt, in hoher Qualität verfügbar gehalten und zielgerichtet genutzt werden, um ihren vollen Nutzen für die Universität zu entfalten.
- Daten unterstehen einem Lifecycle, unnötige Daten generieren Kosten und unnötige Aufwände.

Daten haben einen Verantwortlichen (Ownership)

Daten haben mindestens einen Daten-Owner.

Daten als gemeinsames Gut

Daten werden als gemeinsames Gut betrachtet. Dies fördert die Datenzugänglichkeit und Zusammenarbeit. Daten werden möglichst zentralisiert über standardisierte Schnittstellen bereitgestellt. Berechtigte Nutzende können einfach und sicher darauf zugreifen.

Erläuterung:

- Der Zugriff auf Daten muss so einfach wie möglich und so sicher wie notwendig sein.

- Die zentralisierte Bereitstellung von Daten erhöht die Konsistenz des Datenbestandes, vermeidet widersprüchliche Informationen und erleichtert das Auffinden.

Datenqualität sicherstellen

Die Qualität unserer Daten wird durch klare Verantwortlichkeiten und definierte Massnahmen gesichert.

Erläuterung: Eine definierte Datenqualität gewährleistet, dass die Daten in der benötigten Korrektheit, Vollständigkeit, Konsistenz und Aktualität vorhanden sind.

Betrieb

Automatisierter und standardisierter Betrieb

Betriebsprozesse sind weitgehend automatisiert, standardisiert und werden regelmässig überwacht.

Erläuterung: Ein automatisierter Betrieb steigert die Effizienz, reduziert manuelle Fehler und erhöht die Verfügbarkeit sowie die Reaktionsgeschwindigkeit im Störfall.

Observability by Design

Systeme und Services verfügen über umfassendes, nachvollziehbares Logging und technisches Monitoring.

Erläuterung: Umfassendes Logging/Monitoring ermöglicht, Fehler effizient zu diagnostizieren, die Performance jederzeit zu analysieren und Audits zu bestehen.

Resilienz durch Backup & Recovery

Backup- und Recovery-Strategien sind dokumentiert, getestet und auf aktuelle Risiken abgestimmt.

Erläuterung: Backup- und Recovery-Strategien mit den entsprechenden Massnahmen schützen vor Datenverlust.

Klare Zuständigkeiten im Support

Supportprozesse basieren auf klaren Zuständigkeiten und transparenten Eskalationswegen.

Erläuterung: Klar definierte Zuständigkeiten sichern die Servicequalität und reduzieren Ausfallzeiten.

Infrastruktur & Infrastructure as a Service (IaaS)

Consider Infrastructure as Code (IaaS)

Software definiert die nötige Infrastruktur; diese wird automatisiert und standardisiert bereitgestellt.

Erläuterung: Software-definierte Infrastrukturen sparen Ressourcen.

Skalierbarkeit und Resilienz

Skalierbarkeit, Resilienz, hohe Verfügbarkeit und Redundanz werden von Anfang an berücksichtigt.

Erläuterung: Die frühzeitige Berücksichtigung von Skalierbarkeit, hoher Verfügbarkeit und Redundanz stellt eine hohe Systemstabilität und verlässliche Betriebsbereitschaft auch bei Lastspitzen sicher.

Standardisierte Betriebsbasis durch Container-Technologie

Container-Technologien werden als strategische Basis für moderne Anwendungen bevorzugt.

Erläuterung: Container ermöglichen portable, isolierte Anwendungen und verbessern die Ressourcennutzung deutlich.

Technologie

Technologieauswahl

Die Auswahl von Technologien erfolgt anhand klarer Kriterien: Diese berücksichtigen strategische Ziele, fachliche Anforderungen und technische Qualitätsmerkmale. Technologieentscheidungen werden transparent dokumentiert.

Erläuterung:

- Technologieentscheidungen werden transparent und nachvollziehbar getroffen; dies vermeidet Fehlentscheidungen und schafft Konsens.
- Die Auswahl erfolgt nicht nur nach (kurzfristigen) Projektbedürfnissen, sondern orientiert sich am Optimum für die Universität.
- So wird sichergestellt, dass die Technologieauswahl nicht willkürlich erfolgt, sondern auf einer fundierten, strategisch abgestimmten Basis. Damit werden die nachhaltige Entwicklung der IT-Landschaft unterstützt und Risiken minimiert.

Standardisierung und Interoperabilität

Bei der Auswahl und Nutzung von Technologien werden offene Standards bevorzugt.

Erläuterung:

- Die Nutzung offener Standards ermöglicht einen herstellerunabhängigen Austausch von Daten und Diensten.
- Integrationsaufwände werden reduziert, Innovation gefördert.
- Es werden Abhängigkeiten zu einzelnen Anbietern vermieden (Vendor Lock-in).