

IT-Governance an der Hochschule München

Ziele

Die Ziele der IT-Governance an der Hochschule München sind vielfältig und darauf ausgerichtet, eine sichere und effektive Nutzung von Ressourcen zu gewährleisten. IT-Sicherheit hat an der Hochschule München einen sehr hohen Stellenwert und ist aus diesem Grund Teil der IT-Governance. Ziel ist es eine gesamtseinheitliche Betrachtung der IT und der IT-Sicherheit zu erreichen.

1. Gewährleistung der Verfügbarkeit und Kontinuität von IT-Systemen: Ein zentrales Ziel der IT-Governance ist es, sicherzustellen, dass die IT-Systeme und -Dienste an der Hochschule München kontinuierlich verfügbar sind. Dazu werden robuste Infrastrukturen und Technologien eingesetzt, um Ausfallzeiten zu minimieren und einen reibungslosen Ablauf von Lehrveranstaltungen, Forschungsprojekten und Verwaltungsaufgaben zu gewährleisten. Durch geeignete Maßnahmen wie Redundanz, Notfallwiederherstellungspläne und regelmäßige Wartung werden die Verfügbarkeit und Kontinuität der IT-Systeme sichergestellt.

2. Sicherstellung der Datensicherheit und Datenschutz: Die IT-Sicherheit hat das Ziel, die Vertraulichkeit, Integrität und Verfügbarkeit sensibler Daten an der Hochschule München zu schützen. Es werden geeignete Sicherheitsmaßnahmen ergriffen, wie beispielsweise Zugriffskontrollen, Verschlüsselungstechnologien und Sicherheitsrichtlinien, um unbefugten Zugriff, Datenverlust oder -manipulation zu verhindern. Darüber hinaus wird die Einhaltung der geltenden Datenschutzgesetze und -bestimmungen sichergestellt, um den Schutz personenbezogener Daten zu gewährleisten.

3. Risikomanagement: Die IT-Governance an der Hochschule München zielt darauf ab, Risiken im Zusammenhang mit IT-Systemen und -Prozessen zu identifizieren, zu bewerten und angemessene Maßnahmen zu deren Minderung zu ergreifen. Dies beinhaltet die Durchführung regelmäßiger Sicherheitsaudits, die Bewertung von Schwachstellen und die Implementierung geeigneter Sicherheitsmaßnahmen, um mögliche Bedrohungen zu erkennen und zu reduzieren. Das Risikomanagement ermöglicht es, potenzielle Risiken frühzeitig zu erkennen und entsprechende Maßnahmen zur Risikominderung zu ergreifen.

4. Einhaltung von Vorschriften und Standards: Die IT-Governance an der Hochschule München sichert die Einhaltung geltender Vorschriften, gesetzlicher Bestimmungen und Industriestandards. Dazu gehören beispielsweise Datenschutzgesetze, rechtliche Anforderungen im Bildungsbereich sowie Standards wie ISO 27001 für Informationssicherheitsmanagement. Durch die Erfüllung dieser Vorschriften und Standards wird sichergestellt, dass die IT-Systeme der Hochschule den aktuellen Best Practices entsprechen und ein angemessenes Sicherheitsniveau bieten.

5. Förderung einer Kultur der IT-Sicherheit: Ein weiteres wichtiges Ziel ist die Schaffung einer Bewusstseinskultur für IT-Sicherheit an der Hochschule München. Dies beinhaltet die Sensibilisierung aller Studierenden, Mitarbeiterinnen und Mitarbeiter sowie Dozentinnen und Dozenten für die Bedeutung von IT-Sicherheit. Schulungen, Trainings und Informationsveranstaltungen werden durchgeführt, um das Bewusstsein für Sicherheitsrisiken und bewährte Sicherheitspraktiken zu schärfen. Indem die Hochschulangehörigen in Bezug auf IT-Sicherheit geschult werden, werden sie befähigt, potenzielle Bedrohungen zu erkennen und entsprechende Maßnahmen zu ergreifen, um Sicherheitsverletzungen zu verhindern. Eine Kultur der IT-Sicherheit trägt dazu bei, das Risikobewusstsein zu stärken und die IT-Sicherheit an der Hochschule München kontinuierlich zu verbessern.

Zusammenfassend ist es das Ziele der IT-Governance an der Hochschule München, eine sichere und effektive Nutzung von IT-Ressourcen sicherzustellen. Dies umfasst die Gewährleistung der Verfügbarkeit und Kontinuität von IT-Diensten, den Schutz sensibler Daten, das Risikomanagement, die Einhaltung von Vorschriften und Standards sowie die Förderung einer Kultur der IT-Sicherheit. Durch die Umsetzung dieser Ziele wird die Hochschule München in der Lage sein, ihre IT-Systeme und -Infrastrukturen effizient zu betreiben und ein hohes Maß an Sicherheit für alle Nutzerinnen und Nutzer zu gewährleisten.

Rollen

Chief Information Officer (CIO)

Der CIO (Chief Information Officer) an der Hochschule München spielt eine zentrale Rolle in Bezug auf die IT-Governance und -Strategie. Seine Verantwortlichkeiten umfassen die Entwicklung und Umsetzung der IT-Strategie, die Gewährleistung der IT-Sicherheit, die Auswahl und Implementierung von Technologien sowie die enge Zusammenarbeit mit den verschiedenen Fakultäten, Verwaltungseinheiten und der Hochschulleitung. Der CIO trägt dazu bei, dass die IT-Ressourcen effizient genutzt werden und einen Mehrwert für die Hochschule bieten. Die folgenden Verantwortungen obliegen ihm/ihr:

1. IT-Strategie und -Planung
2. IT-Richtlinien
3. IT-Management der gesamten Hochschule
4. Stakeholder-Management

Die Rolle des CIOs ist organisatorisch beim Kanzler als Stabstelle eingerichtet. Der Kanzler und CIO berichten regelmäßig zum Thema IT und IT-Sicherheit an die Hochschulleitung. Mitarbeiter und Mitarbeiterinnen des CIOs sind organisatorisch in der IT aufgehängt und der CIO ist diesen fachlich weisungsbefugt. Die Budgets des CIOs sind in der IT organisiert.

Leiter IT

Der Leiter der IT an der Hochschule München hat eine maßgebliche Rolle bei der Organisation und Steuerung der IT-Abteilung auf Grundlage der IT-Strategie. Er ist dem Kanzler unterstellt. Seine Hauptaufgabe besteht darin, die effektive Bereitstellung von IT-Services und -Infrastrukturen sicherzustellen, um den reibungslosen Betrieb der Hochschule zu unterstützen. Folgende Verantwortungen obliegen ihm/ihr:

1. IT-Management für hochschulweite Dienste
2. Budgetierung und Ressourcenallokation
3. Technologische Entwicklung und Innovation

Informationssicherheitsbeauftragter / CISO

Der Informationssicherheitsbeauftragte an der Hochschule München spielt eine wichtige Rolle bei der Gewährleistung der Informationssicherheit und des Datenschutzes. In dieser Rolle berichtet er direkt an den Kanzler. Seine Hauptaufgabe besteht darin, Maßnahmen zu entwickeln, zu implementieren und zu überwachen, um die Vertraulichkeit, Integrität und Verfügbarkeit der Informationen und IT-Systeme an der Hochschule zu gewährleisten. Eine enge Zusammenarbeit mit dem Datenschutzbeauftragten ist notwendig, damit das gemeinsame Ziel, der Schutz von Daten, erzielt werden kann. Im Folgenden sind einige spezifische Aufgaben und Verantwortlichkeiten des Informationssicherheitsbeauftragten an der Hochschule München:

1. Entwicklung von Richtlinien und Standards im Bereich IT-Sicherheit
2. Sicherheitsrisikobewertung und -management
3. Schulungen und Sensibilisierung
4. Vorfallsbehandlung und Untersuchungen
5. Compliance und Audits in Bezug auf IT-Sicherheit

Gremien

CIO-Board

Das CIO-Board an der Hochschule München besteht aus einer Gruppe von Führungskräften, die die IT-Governance und die strategische Ausrichtung der Informationstechnologie an der Hochschule steuern. Es dient als zentrales Gremium für die Entscheidungsfindung und die Förderung der Zusammenarbeit zwischen der IT-Abteilung und den Fakultäten sowie Verwaltungseinheiten.

Die Hauptrolle des CIO-Boards besteht darin, die IT-Strategie und -richtlinien der Hochschule München zu beschließen und zu überwachen. Es setzt die strategischen Ziele für die IT fest und stellt sicher, dass diese mit den gesamten Hochschulzielen übereinstimmen. Das CIO-Board überprüft und genehmigt auch große IT-Projekte, Investitionen und Budgets, um sicherzustellen, dass sie den strategischen Prioritäten entsprechen.

Ein weiteres wichtiges Anliegen des CIO-Boards ist die Förderung der Zusammenarbeit und des Austauschs zwischen der IT-Abteilung und Fakultäten sowie

Verwaltungseinheiten. Es bietet eine Plattform für den Dialog und die Abstimmung von IT-Anforderungen und -Initiativen mit den Bedürfnissen und Zielen der Hochschule insgesamt. Das CIO-Board unterstützt die Integration der IT in die Kernprozesse und -aktivitäten der Hochschule und fördert eine effektive Nutzung von IT-Ressourcen zur Verbesserung der Lehr-, Lern- und Verwaltungsprozesse.

Darüber hinaus kann das CIO-Board auch eine Rolle bei der Überwachung und dem Management von IT-Risiken und -Sicherheitsfragen spielen. Es unterstützt die Entwicklung und Umsetzung von IT-Sicherheitsrichtlinien und -verfahren und stellt sicher, dass angemessene Maßnahmen zum Schutz der IT-Infrastruktur und der Daten der Hochschule ergriffen werden.

Das CIO-Board setzt sich aus dem Kanzler, dem CIO, dem IT-Leiter und einem Vertreter der Dekan:Innen (jeweils eine Stimme) zusammen. Dem CIO-Board steht der CIO vor und wird vom CIO organisiert. Das CIO-Board tagt einmal im Semester und zusätzlich bei Bedarf.

IT-Community oder IT-Anwenderkreis

Der IT-Anwenderkreis an der Hochschule München ist ein Gremium, das aus Vertretern der verschiedenen Nutzergruppen aus Fakultäten/Verwaltungseinheiten besteht. Die Zusammensetzung und der Turnus der gemeinsamen Sitzungen ist abhängig vom jeweiligen Bedarf bzw. spezifischen Themen/Projekten. Es hat die Aufgabe, die Bedürfnisse und Anforderungen der Endbenutzer in Bezug auf IT-Services und -Lösungen zu erfassen und diese in die IT-Strategie und -Planung einzubinden. Der IT-Anwenderkreis fungiert als Sprachrohr und Interessenvertretung der Nutzer gegenüber der IT-Abteilung.

Die Hauptrolle des IT-Anwenderkreises besteht darin, eine enge Zusammenarbeit zwischen den Nutzern und der IT-Abteilung sicherzustellen. Durch regelmäßige Treffen und Kommunikation werden aktuelle Anliegen, Herausforderungen und Wünsche der Nutzer besprochen. Der IT-Anwenderkreis trägt dazu bei, dass die IT-Services an den tatsächlichen Bedarf der Hochschule angepasst werden und eine hohe Benutzerzufriedenheit gewährleistet ist.

Der IT-Anwenderkreis spielt eine wichtige Rolle bei der Identifizierung von Verbesserungspotenzialen und neuen Anforderungen. Er bringt Anregungen, Vorschläge und Feedback aus den Fakultäten sowie Verwaltungseinheiten ein und unterstützt die IT-Abteilung bei der Priorisierung von Projekten und Initiativen. Der IT-Anwenderkreis kann auch bei der Evaluierung und Auswahl von Softwarelösungen oder bei der Definition von Standards und Richtlinien mitwirken.

Darüber hinaus ist der IT-Anwenderkreis eine Plattform für den Erfahrungsaustausch und die Zusammenarbeit zwischen den verschiedenen Nutzergruppen. Es ermöglicht den Nutzern, bewährte Praktiken zu teilen, Herausforderungen zu diskutieren und von den Erfahrungen Fakultäten sowie Verwaltungseinheiten zu lernen.

Das Gremium des IT-Anwenderkreises wird in der Regel von einem Moderator oder einer Moderatorin aus der IT geleitet, der/die die Diskussionen strukturiert und sicherstellt, dass alle Stimmen gehört werden. Die Treffen finden regelmäßig statt und können je nach Bedarf auch Arbeitsgruppen oder Projektteams umfassen, die spezifische Themen oder Projekte bearbeiten.

Verantwortlichkeiten

IT-Betrieb

Der IT-Betrieb an der Hochschule München wird in erster Linie von der zentralen Abteilung IT koordiniert und unterstützt. Diese Abteilung bildet den IT-Kern der Hochschule und ist für die Bereitstellung und Wartung der grundlegenden IT-Infrastruktur und -Basisdienste verantwortlich. Dazu gehören unter anderem:

- 1. Netzwerk- und Server-Infrastruktur:** Die IT-Abteilung verwaltet und betreibt das Hochschulnetzwerk, das die Grundlage für die Kommunikation und den Datenaustausch zwischen den verschiedenen Einheiten der Hochschule bildet. Sie stellt Serverdienste bereit, wie E-Mail, Datenbanken und Websites.
- 2. IT-Sicherheit:** Die Sicherheit der IT-Systeme und Daten ist von entscheidender Bedeutung. Die IT-Abteilung sorgt für Firewall- und Virenschutz, überwacht die Netzwerksicherheit und entwickelt Sicherheitsrichtlinien und -verfahren.
- 3. Softwarelizenzen und -Support:** Die IT-Abteilung verwaltet die Lizenzen für Softwareanwendungen, die von der Hochschule genutzt werden. Sie kann auch technischen Support für diese Anwendungen bieten.
- 4. Rechenzentrum:** In einem zentralen Rechenzentrum werden die zentralen IT-Ressourcen wie Server, Speicher und Backup-Systeme gehostet und gewartet.
- 5. Helpdesk und Support:** Die IT-Abteilung betreibt einen Helpdesk, der den Benutzern bei technischen Problemen und Anfragen unterstützt.
- 6. Softwareentwicklung und -Betrieb:** Die IT-Abteilung entwickelt und betreibt Software für die Hochschule.

Die Verantwortung des Betriebs des IT-Kerns obliegt der zentralen Abteilung IT. Zudem verantwortet die Abteilung IT den Betrieb der Verwaltungs-IT. Fakultäten und andere Einheiten der Hochschule München verantworten Ihre eigene IT selbst und müssen die IT-Richtlinien selbst umsetzen. Dies bedeutet, dass sie eigene IT-Ressourcen und -Experten haben können, um ihren speziellen fakultätsspezifischen Anforderungen gerecht zu werden. Alternativ können sie bestimmte Dienste und Ressourcen nach Abstimmung von der Abteilung IT in Anspruch nehmen, wobei in Zukunft die IT-Basisdienste von der Abteilung IT bereitgestellt werden.

Diese flexible Struktur ermöglicht es den verschiedenen Einheiten der Hochschule, ihren IT-Betrieb an ihre individuellen Bedürfnisse anzupassen, während die IT-Abteilung gleichzeitig eine koordinierende und unterstützende Rolle spielt, um die Gesamteffizienz und Sicherheit des IT-Betriebs der Hochschule sicherzustellen.

IT- und IT-Sicherheitsrichtlinien

Der CIO, der ISB, sowie die Leitung der IT geben die Richtlinien im Bereich der IT und IT-Sicherheit vor. Diese Richtlinien sind für alle Hochschulangehörige bindend und müssen umgesetzt werden. Die Richtlinien werden vom CIO-Board beschlossen und auf der Website des CIOs zur Verfügung gestellt.