Technische Universität Braunschweig

Inhalt

Informationssicherheitsordnung der TU Braunschweig

Präambel

Diese Ordnung regelt die Zuständigkeiten und die Verantwortung sowie die Zusammenarbeit im hochschulweiten Informationssicherheitsprozess[1]. Ziel der Informationssicherheitsordnung ist es, nicht nur die existierenden gesetzlichen Auflagen zu erfüllen, sondern auch die TU Braunschweig soweit möglich vor Schäden zu bewahren. Die Entwicklung und Fortschreibung der Informationssicherheits-ordnung müssen sich an den gesetzlich festgelegten Aufgaben der Hochschule sowie an ihrem Mandat zur Wahrung der akademischen Freiheit orientieren. Dies kann jedoch nur über einen kontinuierlichen Informationssicherheitsprozess innerhalb geregelter Verantwortungsstrukturen erreicht werden.
Diese Ordnung orientiert sich bei Etablierung und Weiterentwicklung des Informationssicherheits-prozesses an allgemeinen Anforderungen an einen ordnungsgemäßen IT-Betrieb, welche zusammengefasst in den „Mindestanforderungen der Rechnungshöfe des Bundes und der Länder zum Einsatz der Informationstechnik“[2] dargestellt sind. Diese Mindestanforderungen an den IT-Betrieb beziehen sich auf allgemein anerkannte rechtliche und technische Normen. Im Bereich der technischen Umsetzung von Informationssicherheit sind dies beispielsweise das „Grundschutz-Kompendium“[3] des Bundesamts für Sicherheit in der Informationstechnik (BSI), welches auf den weitgehend gleichwertigen Normen der ISO 2700x-Reihe fußt, dem vom Verein der Hochschul-rechenzentren Deutschlands („Zentren für Kommunikation und Informationsverarbeitung e.V.“ (ZKI)) erarbeiteten „Grundschutzprofil für Hochschulen“[4] und weitere etablierte Quellen, die in ihrer jeweils aktuellen Fassung den aktuellen Stand widerspiegeln. Rechtliche Grundlagen dieser Ordnung sind:

- Die Verpflichtung entsprechend der „Leitlinie zur Gewährung der Informationssicherheit“ (ISLL) des Landes Niedersachsens entsprechende Mindeststandards zu schaffen
- § 37 Absatz 1 in Verbindung mit § 3 NHG.

Über diese Ordnung werden mithilfe vorstehend genannter Normen die an der TU Braunschweig geltenden Richtlinien zur Informationssicherheit und IT-Sicherheit abgeleitet.

---

[1] Diese Ordnung fokussiert sich auf die informationstechnischen Aspekte der Informationssicherheit. Weitere Aspekte wie z.B. physische Sicherheit und organisatorische Sicherheit müssen darüber hinaus auch in anderen Bereichen der Universität entwickelt und beachtet werden (z.B. Gebäudemanagement, Prozessentwicklung, Arbeitsprozesse in den Organisationseinheiten).
[2] https://www.bundesrechnungshof.de/de/veroeffentlichungen/produkte/weitere/mindestanforderungen-der-rechnungshoefe-des-bundes-und-der-laender-zum-einsatz-der-informationstechnik/mindestanforderungen-der-rechnungshoefe-des-bundes-und-der-laender-zum-einsatz-der-informations-und-kommunikationstechnik/@@download/file [letzter Abruf 24.06.2021]
[3] BSI Grundschutz-Kompendium
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html [letzter Abruf 08.07.2021]
[4] ZKI Grundschutzprofil für Hochschulen: Leitdokument und Bausteinkommentierungen
https://www.zki.de/fileadmin/user_upload/Downloads/IT-Grundschutz-Profil_fuer_Hochschulen_V1_0.pdf und
https://www.zki.de/fileadmin/user_upload/Downloads/IT-Grundschutz-Profil_fuer_Hochschulen_Bausteinkommentierungen_V1_0.pdf [letzter Abruf 08.07.2021]

§ 1 Gegenstand der Ordnung

Gegenstand dieser Ordnung ist die Festlegung der zur Realisierung eines hochschulübergreifenden Informationssicherheitsprozesses[5] erforderlichen Verantwortungsstrukturen, eine Aufgabenzuordnung sowie die Festlegung der Zusammenarbeit der Beteiligten. Diese Ordnung wird auf technischem Gebiet ergänzt durch die folgenden Ordnungen:

(1) Nutzungsordnung zur Informationstechnologie der Technischen Universität Braunschweig,
(2) Informationsdienste-Ordnung der Technischen Universität Braunschweig sowie
(3) Richtlinien zur Informationssicherheit und IT-Sicherheit zu einzelnen Themen.
(4) Bestehende und zukünftige Dienstvereinbarungen zur Informationssicherheit und zur Nutzung technischer Geräte.

§ 2 Geltungsbereich

(1) Der Geltungsbereich dieser Ordnung erstreckt sich auf alle Organisationseinheiten der TU Braunschweig gemäß § 4 der Grundordnung der TU Braunschweig (insbesondere die Organe nach Abschnitt 3 und 4 der Grundordnung), auf die gesamte von der TU Braunschweig zu verantwortenden IT-Infrastruktur, einschließlich aller zentral und dezentral betriebenen IT-Systeme, sowie einschließlich aller extern betriebener und beauftragter Systeme, unter Berücksichtigung der Prozesse, denen diese Systeme dienen.
(2) Die Festlegungen dieser Ordnung und der hieraus entstehenden Richtlinien sind bei Vereinbarungen und Verträgen mit An-Instituten und außeruniversitären Einrichtungen, die direkt an das Hochschulnetz angeschlossen sind oder über dieses Mitnutzer des Deutschen Forschungsnetzes (DFN) sind, zu beachten.

§ 3 Beteiligte am Informationssicherheitsprozess

Die Gesamtverantwortung für den Informationssicherheitsprozess liegt bei der Hochschulleitung[6]. Sie benennt folgende Gremien und Funktionstragende als Beteiligte am Informationssicherheitsprozess:

(1) Das CIO-Board (CIOB),
(2) Der:die Chief Information Security Officer (CISO) als von der Hochschulleitung beauftragte verantwortliche Person für Informationssicherheit[7],
(3) IT-Security Board (IT-SB),
(4) Ein operatives Informationssicherheitsmanagement-Team (ISMT) (Leitung: CISO),
(5) dezentrale Informationssicherheitsbeauftragte (DISB) der dezentralen Organisationseinheiten,
(6) das Gauß-IT-Zentrum (GITZ),
(7) Die Universitätsbibliothek (UB)
(8) die Leitungen der Organisationseinheiten der Universität. Diesen wird für ihren Bereich die Verantwortung für die Einhaltung der Standards übertragen.

---

[5] Immer bezogen auf elektronisch gestützte Informationsverarbeitungsprozesse.
[6] § 37 Abs 1 Niedersächsisches Hochschulgesetz (NHG)
[7] Die Bezeichnungen „zentrale:r Informationssicherheitsbeauftragte:r (ISB)“ bzw. „Informationssicherheits-beauftragte Person (ISB)“, „Chief Information Security Officer (CISO)“, „Person in der Rolle CISO“ sowie „beauftragte Person zur Informationssicherheit“ sind gleichwertig, werden synonym verwendet und in der Abkürzung CISO mit maskulinem Artikel geschlechtsneutral verwendet, da die Rolle eines „Officers“ weltweit in verschiedenen Kontexten auch von nicht-männlichen Personen ausgefüllt wird.

Die benannten Beteiligten wirken arbeitsteilig zusammen, um die Informationssicherheitsstandards an der TU Braunschweig einzuhalten.
Als beteiligtes Leitungsgremium der Hochschule wird zum Zeitpunkt des Inkrafttretens dieser Ordnung das CIO-Board (CIOB) der TU Braunschweig bestimmt.

§ 4 Einsetzung der Beteiligten

(1) Die Hochschulleitung setzt für die Konzeption, Umsetzung und Überwachung des Informationssicherheitsprozesses eine:n CISO als von der Hochschulleitung beauftragte verantwortliche Person für diesen Prozess ein. Als Vertretung wird der:die für den Bereich Informationssicherheit ressortierte Vizepräsident:in[8] bestimmt, bei Abwesenheit sowohl von CISO als auch der:der ressortierten Vizepräsident:in übernimmt der:die Vizepräsident:in für Personal, Finanzen und Hochschulbau (HVP) die Vertretung.
(2) Die Hochschulleitung setzt das IT-SB ein und bestimmt den:die CISO als leitende Person.
(3) Das IT-SB setzt das ISMT ein. Das ISMT ist eine operative Gruppe und wird vom:von der CISO geleitet.
(4) Alle Organisationseinheiten, welche Informationstechnik nutzen, setzen eine Person als DISB[9] ein und eine weitere Person als Stellvertretung. Mehrere Organisationseinheiten können einen gemeinsamen DISB gemeinsam einsetzen.
(5) Alle informationsverarbeitenden Systeme und alle Benutzenden sind je einer:einem DISB zuzuordnen. Diese Zuordnung ist zu dokumentieren. Die Hochschulleitung kann bei fehlender Selbstzuweisung auch entsprechende Zuordnungen beschließen. („Auffanglösung“)
(6) In den Fakultäten werden DISB und Stellvertretende so eingesetzt, dass alle dort betriebenen informationsverarbeitenden Systeme und alle IT-Nutzenden entsprechend zugeordnet sind. Die Fakultäten setzen eine:n DISB sowie eine Stellvertretung auf Fakultätsebene ein. Sofern dann auf Institutsebene weitere DISB eingesetzt werden, arbeiten diese dem:der auf Fakultätsebene eingesetzten DISB zu.
(7) Der:die für das GITZ eingesetzte DISB ist auch für die Informationssicherheits-Belange der zentralen Verwaltung zuständig.
(8) Die Studierendenschaft wird über eine vom Studierendenparlament zu entsendende Person als beratendes Mitglied im IT-SB am Informationssicherheitsprozess beteiligt.
(9) Bei der Einsetzung von DISB und ISMT ist auf personelle Kontinuität zu achten. Die Beteiligten sollen nach Möglichkeit zum hauptberuflichen Personal der TU Braunschweig gehören.
(10) Die operative Gruppe des ISMT besteht aus ganz oder teilweise der:m CISO zugeordneten Mitarbeitenden sowie den in §5 aufgeführten Personen. Weitere Personen aus anderen Organisationseinheiten können dem ISMT zugeordnet werden. Das ISMT arbeitet der:m CISO zu.

[8] Zum Stand des Beschlusses der Ordnung: Vizepräsident:in für Digitalisierung und Technologietransfer (VP-DT)
[9] nachfolgend wird das Akronym DISB mehrheitlich ohne geschlechtsspezifischen Artikel auch als Ersatz für eine Person bzw. Personen verwendet, welche die Rolle eines dezentralen Informationssicherheitsbeauftragten für eine (dezentrale) Organisationseinheit übernommen hat.

§ 5 Zusammensetzung des IT-Sicherheits-Boards (IT-SB) / Bestellung der Informationssicherheitsbeauftragten Personen

(1) Die Mitglieder des IT-SB werden vom Präsidium bestimmt (siehe Anhang). Die Leitung des IT-SB erfolgt durch die:den CISO.

(2) Das IT-SB setzt das Informationssicherheitsmanagement-Team, (ISMT) als operative Gruppe ein, welches die Person der:s CISO im operativen Geschäft unterstützt). Ständige Mitglieder sind:
- CISO als vorsitzender Person,
- die DISB der Fakultäten,
- eine von der Leitung des Gauß-IT-Zentrum bestimmte Person,
- eine von der Leitung der Universitätsbibliothek bestimmte Person,
- die der:m CISO zugeordneten Mitarbeitenden (Informationssicherheitsmanagement, Stabsstelle CISO).

(3) IT-SB und ISMT sollen bei Bedarf den Rat von internen und externen Fachleuten einholen (z. B. für Teilbereiche der Informationssicherheit oder des IT-Betriebs).

§ 6 Aufgaben der am Informations-Sicherheitsprozess beteiligten Personen

(1) Die Wahrung der Informationssicherheit ist Aufgabe der Leitung in deren Zuständigkeit die jeweiligen Informationen verarbeitet werden, einschließlich der technischen Systeme die dafür genutzt werden sowie die Gestaltung der informationsverarbeitenden Prozesse. Sie umfasst die Sicherung der technischen Systeme, die Gestaltung der informationsverarbeitenden Prozesse und die Unterrichtung und Schulung der diese Prozesse durchführenden Personen. Die Aufgabe kann in diesem Umfang auf eine:n (dezentralen) Informationssicherheitsbeauftragte:n übertragen werden. Dies entbindet weder die Leitung der Universität insgesamt noch die Leitung der jeweiligen Organisationseinheit von ihrer Gesamtverantwortung für die Informationssicherheit im jeweiligen Zuständigkeitsbereich.

(2) Das CIOB beschließt als höchstes Beratungs- und Kontrollorgan in Sachen Informationssicherheit die Handlungsempfehlungen und schlägt die strategische Informationssicherheitsleitlinie für die TU Braunschweig vor. Das Präsidium beschließt die vom CIOB unter Berücksichtigung der Empfehlungen aus dem IT-SB erarbeiteten und mit den Gremien abgestimmten strategischen Informationssicherheitsleitlinie und dieser Ordnung und anderen Handlungsempfehlungen. Das CIOB erarbeitet mit Zuarbeit durch das IT-SB aus der Leitlinie und dieser Ordnung die zugehörigen technischen Richtlinien und setzt diese in Kraft. Das CIOB legt den vom IT-SB jährlich zu erstellenden Informationssicherheitsbericht dem Präsidium vor. Das CIOB befasst sich mindestens einmal pro Quartal oder nach Anforderung der:s CISO mit den Belangen der Informationssicherheit.

(3) Das IT-SB bildet für die Universität das zentrale Beratungs- und Kontrollorgan in Sachen Informationssicherheit für die Zeit zwischen den Sitzungen des CIOB. Es erstellt die zentralen technischen Rahmenrichtlinien der Informationssicherheit der Hochschule. Das IT-SB berät das CIOB und das Präsidium zu allen Fragen der Informationssicherheit und der Risikoeinschätzung. Das IT-SB tagt regelmäßig sechs Mal im Jahr oder auf Anforderung der:s CISO.

(4) Die:der CISO
   a. ist für die Kontrolle der Umsetzung der Informationssicherheitsordnung und der Richtlinien der Informationssicherheit an der Hochschule zuständig und wird darin vom IT-SB unterstützt; dies entbindet die Leitung der Universität nicht von ihrer Verantwortung zur Sicherstellung einer angemessenen Informationssicherheit,
   b. baut ein Informationssicherheitsmanagement (ISMS) auf, betreibt es und entwickelt es gemäß den sich ändernden Anforderungen weiter,
   c. ist in allen informationssicherheitsrelevanten Fragen die anzusprechende Person nach innen und außen,
   d. koordiniert die Untersuchung und Dokumentation informationssicherheitsrelevanter Vorfälle und entwickelt einen Schulungs- und Weiterbildungsplan zur Informationssicherheit,
   e. wird gemäß den Richtlinien des BSI[10]-Grundschutzes[11] berufen,
   f. berichtet direkt dem zuständigen Leitungsgremium (CIOB) und hat bei Bedarf direkten Zugang zu Leitung der Universität; eine Personalunion zwischen CISO und DSB oder IT-Leitungen (z.B. zuständiger:m Vizepräsident:in, Leitung Gauß-IT-Zentrum) ist nicht zulässig,
   g. ist in allen für die Informationssicherheit relevanten Themen in allen Organisationseinheiten unaufgefordert zu informieren,
   h. hat in allen Fragen der Informationssicherheit das Recht, mündliche und schriftliche (bzw. Textform) Stellungnahmen gegenüber der Universitätsleitung abzugeben,
   i. hat – ggf. nach Vorabsprache mit der:dem DSB – auf alle betroffenen IT-Systeme TU Braunschweig Zugriff, um Kontroll- und Beratungsaufgaben wahrzunehmen,
   j. hat Zutrittsrecht zu allen Räumen in denen Informationstechnik eingesetzt wird,
   k. wird von der Leitungsebene bei der Wahrnehmung der sich aus dieser Verfügung ergebenden Aufgaben durch Verfügbarmachung angemessener finanzieller, personeller und sonstiger Ressourcen unterstützt und gewährleistet seine angemessene Aus- und Fortbildung,
   l. ist zur Vermeidung von Interessenskonflikten in ihrer:seiner fachlichen Funktion als CISO nicht weisungsgebunden seitens der Hochschulleitung.

(5) Das ISMT ist die operative Basis, um den Informationssicherheitsprozess hochschulweit praktisch umzusetzen und Erfahrungen auszutauschen.

(6) Das ISMT unterstützt die:den CISO und die DISB bei ihrer praktischen Arbeit. Diese operative Gruppe trifft sich nach Bedarf und legt ihren Sitzungsrhythmus selbst fest. Das ISMT wird von der:m CISO geleitet.

(7) Die DISB führen den Informationssicherheitsprozess und die Schulung der Mitarbeitenden in ihren Organisationseinheiten in Bezug auf Informationssicherheit durch. Die Leitungen sind für den dezentralen IT-Betrieb verantwortlich und unterstützen die DISB bei der Implementierung und Durchführung des Informationssicherheitsprozesses.

(8) Die DISB sind bezüglich ihrer Mitteilungspflichten gegenüber der:m CISO unabhängig von Weisungen ihrer Vorgesetzten. Die DISB geben ihre Berichte auch den Leitungen der betreffenden Organisationseinheiten zur Kenntnis.

---

[10] Bundesamt für Sicherheit in der Informationstechnik
[11] BSI Grundschutzkompendium und Umsetzungshinweise: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_2.html und https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/Umsetzungshinweise/umsetzungshinweise_node.html [letzter Abruf: 09.07.2021]

(9) Die Benennung der DISB entbindet die Leitung der Organisationseinheiten nicht von ihrer Verantwortung für die Informationssicherheit in ihrem Bereich.
(10) Die DISB sind verpflichtet, an allen strukturellen Planungen, Verfahren und Entscheidungen mit Bezug zur Informationssicherheit die:den CISO angemessen zu informieren. Dies sind insbesondere Planungen und Entscheidungen, die einen Bezug zur Informationssicherheit von Prozessen haben.
(11) Das Gauß-IT-Zentrum unterstützt die DISB, das ISMT, das IT-SB und die:den CISO in technischen Fragen und bei der praktischen Durchführung von notwendigen Maßnahmen. Dafür sind entsprechende Ressourcen in den jährlichen Budgetverhandlungen des GITZ zu berücksichtigen.
(12) Die Organisationseinheiten der Universität sind verpflichtet, bei allen relevanten Planungen, Verfahren und Entscheidungen mit Bezug zu Informationssicherheit einschließlich Planungen zu neuen Diensten oder informationsverarbeitenden Systemen die jeweils zuständigen DISB sowie die:den CISO bereits im Vorfeld zu beteiligen.
(13) Die am Informationssicherheitsprozess Beteiligten arbeiten in allen Belangen der Informationssicherheit zusammen, stellen die dazu erforderlichen Informationen bereit und regeln die Kommunikations- und Entscheidungswege sowohl untereinander wie auch in Beziehung zu Dritten. Hierbei ist insbesondere der Aspekt der in Krisensituationen gebotenen Eile zu berücksichtigen.

§ 7 Umsetzung des Informationssicherheitsprozesses

(1) Die:Der CISO führt zusammen mit dem IT-SB und unterstützt vom ISMT ein hochschulweites Informations- und Kommunikationssystem ein. Über dieses stehen alle am Informationssicherheitsprozess Beteiligten in Kontakt.
(2) Die DISB sind verpflichtet, sich aktuelle sicherheitsrelevante Informationen für den von Ihnen betreuten Bereich zu beschaffen, sofern diese Informationen nicht zentral beschafft und verteilt werden, und werden darin von der:m CISO und ISMT unterstützt. Die DISB veranlassen in ihrem Bereich die erforderlichen Informationssicherheitsmaßnahmen zur Gefahrenabwehr. Hierzu müssen sie von der Leitung ihrer Organisationseinheit mit den notwendigen Kompetenzen und Anordnungsbefugnissen sowie Sachressourcen ausgestattet werden. Sind zur Gefahrenabwehr über eine Organisationseinheit hinausgehende Maßnahmen notwendig, so ist die:der CISO berechtigt, diese direkt anzuordnen. Wird eine Organisationseinheit nicht in einer der Gefahr angemessenen Zeitspanne tätig, ist die:der CISO berechtigt, entsprechende Maßnahmen zur Gefahrenabwehr direkt anzuordnen, wobei die Organisationseinheit darüber zeitnah zu informieren ist. In jedem Fall von Gefahrenabwehr ist die:der CISO einzubinden.
(3) Die am Informationssicherheitsprozess Beteiligten informieren sich gegenseitig schnellstmöglich, umfassend und vollständig über sicherheitsrelevante Vorfälle. Über jeden Vorfall muss die:der CISO informiert werden.
(4) Die:Der CISO ist berechtigt, alle relevanten Informationen, die bei der Behandlung eines IT-Sicherheitsvorfalls und im Rahmen einer Gefahrenintervention (§8) in den einzelnen Einrichtungen anfallen, einzuholen.
(5) Das IT-SB entwickelt die Rahmenrichtlinien kontinuierlich weiter. Die Beteiligten am Informationssicherheitsprozess können hierzu dem IT-SB Vorschläge unterbreiten

§ 8 Gefahrenintervention

(1) Bei einem erheblichen Verstoß gegen die Informationssicherheitsordnung oder die Richtlinien der Informationssicherheit der Universität sowie bei akuten Bedrohungslagen kann die:der CISO die sofortige, vorübergehende Stilllegung des betroffenen IT-Systems anordnen, die verantwortlichen Benutzenden vorübergehend von der Nutzung der Informationstechnik ausschließen sowie weitere notwendige Maßnahmen ergreifen und anordnen. Der:die CISO muss schnellstmöglich den:die zuständige:n DISB über den Vorgang informieren.

(2) Bei einem erheblichen Verstoß gegen die Informationssicherheitsordnung oder die Richtlinien der Informationssicherheit der Universität an einer dezentralen Stelle kann der:die zuständige DISB die sofortige, vorübergehende Stilllegung des betroffenen IT-Systems anordnen, die verantwortlichen Benutzenden vorübergehend von der Nutzung der Informationstechnik ausschließen sowie weitere notwendige Maßnahmen ergreifen und anordnen. Der:die zuständige DISB muss schnellstmöglich den:die CISO sowie das IT-SB über den Vorgang informieren.

(3) Bei Auffälligkeiten und besonders bei Gefahr in Verzug kann das Gauß-IT-Zentrum Netzanschlüsse vorübergehend sperren oder andere Maßnahmen ergreifen, soweit diese geeignet sind, einen absehbaren Schaden von der Hochschule abzuwenden. Das Gauß-IT-Zentrum muss dabei schnellstmöglich die:den CISO, das IT-SB und die betroffenen DISB über den Vorgang informieren.

(4) Die Wiederinbetriebnahme vorübergehend stillgelegter Informationssysteme oder die Rückgängigmachung ergriffener anderer Maßnahmen setzt die eingehende Überprüfung und Freigabe durch den:die DISB und die Zustimmung der/des CISO voraus.

(5) Nach Rücksprache mit dem IT-SB kann der:die CISO den Ausschluss eines vorübergehend von der Nutzung der Informationstechnik ausgeschlossenen Benutzenden wieder aufheben.

(6) Die Reihenfolge in dieser Aufzählung legt keine Reihenfolge für die zu ergreifenden Maßnahmen fest.

(7) Das IT-SB legt die IT-Dienste fest, für die der:die CISO die Erstellung von Notfallplänen koordiniert. Sie enthalten Handlungsanweisungen in Gefahrensituationen und bei Störfällen und unterteilen sich in einen allgemein hochschulöffentlich zugänglichen Benachrichtigungsplan und in ein detailliertes Notfallkonzept für den Dienstgebrauch sowie Maßgaben, in welchen Fällen ein TU-weites Krisenmanagement notwendig ist. Die Einzelheiten über den Erlass und die Umsetzung der Notfallpläne regelt das CIOB auf Vorschlag des IT-SB, die Regelungen werden in geeignetem Format zur Notfallplanung dokumentiert und den jeweils betroffenen Organisationseinheiten zur Verfügung gestellt.

§ 9 Gleichstellungsklausel

Status- und Funktionsbezeichnungen nach dieser Ordnung nehmen keinen Bezug zum Geschlecht der sie ausfüllenden Personen.

§ 10 Inkrafttreten

Die Informationssicherheitsordnung tritt nach ihrer Verabschiedung im Senat am Tag nach ihrer Bekanntmachung in Kraft. Gleichzeitig tritt die Ordnung zur IT-Sicherheit (hochschulöffentliche Bekanntmachung vom 7.7.2003 [TU-Verkündungsblatt Nr.272]), außer Kraft.
Beschlossen im Senat in der Sitzung am 16.03.2022

Anhang

Zusammensetzung des IT-SB gemäß Präsidiumsbeschluss vom 12.05.2021: Einrichtung und Einsetzung eines IT-Security Boards (IT-SB)

Zu § 5:
Dem IT-SB gehören an:

- Chief Information Security Officer (CISO),
- Vizepräsident:in für Digitalisierung und Technologietransfer (VP-DT),
- Vizepräsident:in für Personal, Finanzen und Hochschulbau (HVP),
- Leitung des Gauß-IT-Zentrums.

Die Leitung des IT-SB erfolgt durch den CISO.

Dem IT-SB gehören beratend an:

- Datenschutzbeauftragte:r (DSB),
- Datenschutzmanagementbeauftragte:r,
- Vertretung Personalrat,
- Sprecher:in IT-Multiprojektmanagement-Board (IT-MMB),
- Sprecher:in IT-User Board (IT-UB),
- dezentrale Informationssicherheitsbeauftragte (DISB),
- Leitung des Project Management Office (PMO).