Richtlinie für die Informationssicherheit an der Universität Duisburg-Essen

Vom 21. Dezember 2017

(Verkündungsblatt Jg. 15, 2017 S. 1055 / Nr. 200)

1 Gegenstand und Geltungsbereich

(1) Die Richtlinie legt die Zuständigkeiten, Verantwortungsstrukturen, Aufgabenzuordnung und Zusammenarbeit der Beteiligten im hochschulweiten IT-Sicherheitsprozess fest.

(2) Unter Berücksichtigung von Risiken und Eintrittswahrscheinlichkeiten setzt die Universität Duisburg-Essen (UDE) geeignete organisatorische, technische und finanzielle Mittel zur Umsetzung der vorliegenden Richtlinie ein.

(3) Die Regelungen dieser Richtlinie gelten für Mitglieder, Angehörige, Gäste und Dienstleister der UDE. Sie richtet sich an alle, die IT-Systeme und IT-Verfahren in der UDE benutzen oder betreiben.

(4) Die Regelungen gelten für Netze und IT-Systeme der UDE und die Nutzung von externen IT-Ressourcen.

2 Begriffsbestimmungen

(1) Einrichtungen sind insbesondere die Fakultäten, die wissenschaftlichen Einrichtungen sowie die Zentralverwaltung und die Zentralen Einrichtungen der Universität, darüber hinaus die studentischen Vertretungen und ihre Gremien im Zuständigkeitsbereich der UDE.

(2) IT-Systeme sind Datenverarbeitungsanlagen, Kommunikationssysteme und sonstige Einrichtungen zur elektronischen Informationsverarbeitung.

(3) IT-Verfahren beschreiben das Zusammenwirken von Anwendungen bzw. IT-Diensten und IT-Systemen.

(4) Verantwortlichkeit liegt immer dann vor, wenn eine Person über den Einsatz von IT-Systemen und IT-Verfahren sowie die damit verbundenen Zwecke und Mittel entscheidet.

(5) Beratung liegt immer dann vor, wenn eine Person durch Empfehlungen die Verantwortlichen über notwendige Maßnahmen informiert und entsprechende Entscheidungen vorschlägt.

(6) Mobile Geräte im Sinne dieser Richtlinie sind tragbare IT-Systeme, die ortsungebunden zur Sprach- und Datenkommunikation eingesetzt werden können und mit dem Netzwerk der Universität Duisburg-Essen verbunden sind.

(7) Der Begriff der Netze in dieser Richtlinie umfasst sowohl kabelgebundene als auch kabellose Netze mit statischer oder dynamischer Zuordnung von IP-Adressen. Weiterhin gehören dazu auch alle Netze in den Einrichtungen mit einer Verbindung zum UDE-Netz.

(8) Nutzerinnen und Nutzer sind Personen gemäß der IT-Benutzungsordnung der Universität Duisburg-Essen, die IT-Systeme im Rahmen des Geltungsbereichs dieser Richtlinie verwenden.
(9) Administratorinnen oder Administratoren sind Nutzerinnen und Nutzer, die IT-Dienste oder IT- Systeme verwalten, z. B. das selbstgenutzte IT-System oder die von anderen genutzten IT-Systeme.
(10) Die bzw. der Informationssicherheitsbeauftragte (ISB/CISO) wird von der Rektorin bzw. dem Rektor bestellt. Sie/Er nimmt die zentralen Informations- und IT-Sicherheitsaufgaben für die UDE wahr.
(11) Die dezentralen Informationssicherheitsbeauftragten (dISB/ISO) können in den Einrichtungen bestellt werden und nehmen die dezentralen Informations- und IT-Sicherheitsaufgaben wahr.
(12) Das „Computer Emergency Response Team“ (ZIM-CERT) ist eine Arbeitsgruppe innerhalb des Zentrums für Informations- und Mediendienste (ZIM) und dient als zentrale Anlaufstelle bei sicherheits- und verfügbarkeitsrelevanten Vorfällen in IT-Systemen der UDE.
(13) Schützenswerte Daten sind personenbezogene Daten im Sinne des Datenschutzrechts sowie solche Informationen, bei denen der Verlust der Vertraulichkeit, Integrität oder Verfügbarkeit der Universität oder Dritten Schaden zufügen könnte.

3 Schutzziele

(1) Für die produktive und störungsfreie Wahrnehmung der Aufgaben in Forschung, Lehre und Verwaltung an der Universität Duisburg-Essen ist eine sichere Verarbeitung von elektronischen Daten wesentliche Voraussetzung.
(2) Risiken beim Einsatz von elektronischen Informationssystemen sind durch geeignete Maßnahmen zu minimieren. Die Verfügbarkeit von Systemen, Daten und Diensten muss gewährleistet, ihre Vertraulichkeit geschützt und ihre Integrität gesichert werden.
(3) Einschlägige Gesetze, Verordnungen, Richtlinien und Erlasse (zum Beispiel zum Datenschutz und zur Informationssicherheit) sind zu beachten.
(4) Die Sicherheitsmaßnahmen orientieren sich am Stand der Technik und müssen in einem wirtschaftlich vertretbaren Verhältnis zum Wert der schützenswerten IT-Systeme, sowie dem Risiko und Schutzbedarf der schützenswerten Informationen angemessenen Verhältnis stehen.
(5) Schadensfälle, die das Ansehen der Universität Duisburg-Essen beinträchtigen, natürliche Personen betreffen oder solche mit hohen finanziellen Auswirkungen, müssen vermieden werden.

4 Verantwortungsstrukturen

(1) Die Gesamtverantwortung für die Informationssicherheit liegt bei der Rektorin bzw. dem Rektor der Universität Duisburg-Essen.
(2) Die Verantwortung für die Informationssicherheit in den Einrichtungen liegt bei deren Leiterinnen bzw. Leitern. Diese berücksichtigen die Informationssicherheit in jedem Geschäftsprozess. Ihnen obliegt die organisatorische Verantwortung zur Umsetzung notwendiger Maßnahmen zur IT- und Datensicherheit.

(3) Der bzw. die Informationssicherheitsbeauftragte berät Rektor, CIO, IKM-Vorstand, dezentrale Informationssicherheitsbeauftragte und die Leitungen der Einrichtungen. Die Aufgaben der bzw. des Informationssicherheitsbeauftragten sind in Anhang 1 definiert.

(4) In den Einrichtungen sind dezentrale Informationssicherheitsbeauftragte (dISB) zu benennen, welche ebenfalls als Ansprechpartnerinnen und Ansprechpartner für den Datenschutz fungieren. Diese sind der oder dem zentralen Informationssicherheitsbeauftragten, sowie der oder dem behördlichen Datenschutzbeauftragten (bDSB) zu melden. Die dezentralen Informationssicherheitsbeauftragten arbeiten mit dem Informationssicherheitsbeauftragten und dem behördlichen Datenschutzbeauftragten zusammen und beraten und sensibilisieren die Anwenderinnen und Anwender in den Einrichtungen und Fakultäten zu Fragen der Informationssicherheit und des Datenschutzes.

(5) Die Leiterinnen und Leiter der Einrichtungen sind verpflichtet, die Verantwortlichkeiten für den Betrieb der dezentralen IT-Systeme festzulegen.

(6) Die Verantwortlichen in den Einrichtungen sind verpflichtet, für vernetzte IT-Systeme, die IT-Verfahren bereitstellen, die dienstlichen Kontaktdaten des verantwortlichen Administrators zu erfassen.

(7) Diese dezentral betriebenen IT-Dienste und die zuständigen Administratoren (Name und Kontaktdaten) werden von den Einrichtungen und Fakultäten erfasst und dem ZIM gemeldet.

(8) Bei Systemen, an denen nur vordefinierte Dienste genutzt werden können (z. B. vordefinierte IT-Dienste mit anonymen Nutzerkennungen oder Messgeräte mit Netzwerkschnittstellen), tragen die Administratorinnen und Administratoren der Systeme die Verantwortung im Sinne dieser Richtlinie.

(9) Die Verwaltung und Zuordnung von IP-Adressen aus dem öffentlichen IP-Adressraum der UDE obliegt dem ZIM.

(10) Durch den IKM-Vorstand wird eine Arbeitsgruppe „IT-Sicherheit“ unter der Leitung der/des ISB/CISO eingesetzt. Mitglieder der Arbeitsgruppe sind der behördliche Datenschutzbeauftrage (bDSB), der dezentrale Informationssicherheitsbeauftragte des ZIM und weitere, vom IKM-Vorstand berufene Personen. Diese Arbeitsgruppe erarbeitet Maßnahmen zur IT-Sicherheit an der UDE.

(11) Bei Fragen zur Auslegung dieser Richtlinie und Unklarheiten entscheidet das Rektorat in grundsätzlichen Fragen, ansonsten der IKM-Vorstand.

5 Grundsätze

5.1 Organisatorische Grundsätze

(1) Alle Nutzerinnen und Nutzer des Geltungsbereiches sind angehalten, verantwortungsbewusst mit der IT und den in ihr verarbeiteten Daten umzugehen; unter Beachtung von IT-Sicherheits- und Datenschutzvorgaben dieser Richtlinie und ergänzender Richtlinien, Ordnungen und Gesetze.

(2) Für alle IT-Systeme im Geltungsbereich dieser Richtlinie müssen die Informationssicherheitsanforderungen festgelegt werden. Hierzu werden die IT-Systeme in Schutzbedarfsklassen[i] eingeordnet. Diese Aufgabe obliegt der Leiterin/dem Leiter der Einrichtung, in der das System betrieben wird. Die Arbeitsgruppe „IT-Sicherheit“ und das ZIM, sowie der Datenschutzbeauf-

i Leitfaden zur Basis-Absicherung nach IT-Grundschutz https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html

tragte (bDSB) bieten hierzu ihre Unterstützung an. Die Leiterin bzw. der Leiter einer Einrichtung informiert die Mitarbeitenden seines Bereiches.

(3) Die notwendige Sensibilisierung für IT-Sicherheits- und Datenschutzrisiken obliegt der Leiterin/dem Leiter der Einrichtung, in der das System betrieben wird. Bei der Durchführung solcher Maßnahmen unterstützen die oder der Informationssicherheitsbeauftragte, die oder der Datenschutzbeauftragte, die Arbeitsgruppe IT-Sicherheit und das ZIM.

(4) In Abhängigkeit von den Anforderungen an die IT-Sicherheit und den Datenschutz der IT-Systeme werden von den Verantwortlichen technische und organisatorische Maßnahmen ergriffen, um das notwendige Sicherheitsniveau zu erreichen. Die oder der Informationssicherheitsbeauftragte sowie die oder der Datenschutzbeauftragte unterstützen die Verantwortlichen hierbei.

(5) Die Arbeitsgruppe „IT-Sicherheit“ entwickelt in Zusammenarbeit mit der internen Weiterbildung (PEOE) ein Ausbildungs- und Schulungskonzept für Nutzerinnen/Nutzer, die Administratorinnen/en und die Arbeitsgruppe „IT-Sicherheit“.

(6) Die Arbeitsgruppe IT-Sicherheit entwickelt einen Vorschlag zum Aufbau einer Organisationsstruktur, die die Meldungen an die Betroffenen und die Aufsichtsbehörde gemäß den einschlägigen Vorschriften (Meldeverpflichtung) koordiniert.

(7) Die Arbeitsgruppe IT-Sicherheit erarbeitet und empfiehlt Richtlinien und Maßnahmen zur IT-Sicherheit und begleitet die Umsetzung und Dokumentation. Zur Erfüllung ihrer Aufgaben kann sie dezentrale Informationssicherheitsbeauftragte und weitere Vertreter betroffener Einrichtungen einladen.

5.2 Nutzung von IT-Systemen

(1) Werden Sicherheitsverstöße oder gravierende Sicherheitslücken im UDE-Netz vermutet, so sind diese dem/der Informationssicherheitsbeauftragten und dem ZIM-CERT zu melden. Diese treffen geeignete Maßnahmen, um die gemeldeten Vorfälle zu verfolgen und betroffene Nutzerinnen und Nutzer zu informieren.

(2) Vermutete Schwachstellen dürfen nur mit ausdrücklicher Zustimmung der in (2) genannten Instanzen genauer exploriert werden. Nicht autorisierte Sicherheitsüberprüfungen, Portscans oder Versuche zur Überwindung von Sicherheitsmaßnahmen bei IT-Systemen der UDE sind grundsätzlich nicht zulässig.

(3) Nutzerinnen und Nutzer von mobilen Geräten müssen sich vor der Nutzung am Netzwerk authentifizieren.

(4) Die Verantwortung für den Betrieb des UDE-Netzes, insbesondere auch des WLAN-Netzes oder anderer Funk-betriebener Netze, liegt beim ZIM. Das ZIM formuliert Regelungen für das Einbringen von aktiven Netzwerkgeräten wie Router, Switches, o.ä.

(5) Für Netze, die über ein lokal administriertes Gateway mit den Netzen der UDE verbunden sind und dauerhaft betrieben werden, muss die Administratorin bzw. der Administrator dem ZIM benannt werden. Sie bzw. er muss dem ZIM die verwendeten IP-Adressen mitteilen.

5.3 Betrieb von IT-Systemen

(1) Alle IT-Systeme und zugehörigen Kommunikationsverfahren sind auf dem aktuellen Stand der Sicherheitstechnik zu halten und mit geeigneten Maßnahmen vor unbefugten Zugriffen und Schadprogrammen zu schützen – z. B. durch Virenscanner, lokale Firewalls oder Verschlüsselungsverfahren.

(2) Die Administratorinnen und Administratoren der IT-Systeme müssen regelmäßige Überprüfungen der Schutzmaßnahmen durchführen.
(3) Sicherheitsrelevante Korrekturen müssen unverzüglich umgesetzt werden.

5.4 Fernzugriff auf das interne Netz

Der Zugriff auf IT-Systeme der UDE aus UDE-externen Netzen darf nur über Kommunikationsprotokolle mit Transportverschlüsselung erfolgen. Für den Zugang zum Netzwerk der UDE wird im Regelfall der VPN-Dienst des ZIM genutzt. Ausnahmen zu dieser Regelung sind mit dem ZIM abzusprechen.

5.5 Gefahrenabwehr

(1) Zur Gefahrenabwehr ergreifen die dISB/ISO in Abstimmung mit den Leiterinnen und Leitern der Einrichtung oder bei Gefahr im Verzug selbstständig die erforderlichen Maßnahmen.
(2) Um unmittelbare Gefahren abzuwehren darf das ZIM zusätzliche Maßnahmen ergreifen und z. B. das betreffende System vom Datennetz trennen, vorhandene Zugänge für die Nutzung eines IT-Verfahrens sperren oder andere Maßnahmen zur Gefahrenabwehr einleiten.
(3) Bei Maßnahmen nach (1) oder (2) ist der ISB/CISO unverzüglich zu informieren.
(4) Bei Maßnahmen nach (1) oder (2) und einem Risiko für personenbezogene Daten ist der bDSB einzubeziehen.

Diese Richtlinie für Informationssicherheit tritt am Tag nach ihrer Veröffentlichung im Verkündigungsblatt der Universität Duisburg-Essen in Kraft.

Ausgefertigt aufgrund des Rektoratsbeschlusses vom 13. Dezember.2017.

Duisburg und Essen, den 21. Dezember 2017

Für den Rektor
der Universität Duisburg-Essen
Der Kanzler
Dr. Rainer Ambrosy

Anhang 1: Informationssicherheitsbeauftragter/in (ISB/CISO)

Der bzw. die ISB/CISO wird von der Rektorin bzw. vom Rektor bestellt. Er/Sie nimmt die Aufgabenerfüllung einrichtungsübergreifend für die UDE wahr und steht dem Rektorat, dem CIO, den dezentralen Informationssicherheitsbeauftragten (dISB) und den Leitungen der Einrichtungen beratend zur Verfügung.

Die Aufgabe der bzw. des ISB/CISO ist die Weiterentwicklung der IT-Sicherheit an der UDE und umfasst im Wesentlichen:

- Abstimmung der Informationssicherheitsziele mit den Zielen der UDE,
- Stellungnahmen und Bewertungen zu IT-Sicherheitsfragen der UDE in klarer Abgrenzung zum behördlichen Datenschutzbeauftragten,
- Fortschreibung der Informationssicherheitsrichtlinie der UDE,
- Führung der Arbeitsgruppe „IT-Sicherheit“ der UDE, in der die Fakultäten und andere Einrichtungen vertreten sind,
- Erarbeitung von Maßnahmen zur Informationssicherheit an der UDE in der Arbeitsgruppe „IT-Sicherheit“,
- Bericht in dem IKM-Vorstand sowie Einholung der Zustimmung zu Informationssicherheitsmaßnahmen und -empfehlungen,
- Sammlung der Maßnahmen und Empfehlungen zu IT-Sicherheitsfragen und Veröffentlichung innerhalb der UDE,
- Durchführung von Aufmerksamkeits- und Schulungsmaßnahmen in den Fakultäten und zentralen Einrichtungen zum Thema IT-Sicherheit an der UDE.