RUHR-UNIVERSITÄT BOCHUM

RUB

NR. 872 | 06. MAI 2011

AMTLICHE BEKANNTMACHUNG

Leitlinie zur Informationssicherheit

vom 05.05.2011

Leitlinie zur Informationssicherheit

vom 5. Mai 2011

Inhaltsverzeichnis

PRÄAMBEL

Für die Ruhr-Universität Bochum (RUB) als leistungsstarke europäische Hochschule ist eine zuverlässig funktionierende Informations- und Kommunikationstechnik (IT) für Forschung, Lehre, Studium und Verwaltung unerlässlich. Viele Prozesse wie etwa administrative Aufgaben, Vorlesungs- und Prüfungsplanung, Finanzmanagement, Personal- und Studierendenverwaltung sind zunehmend von IT-Verfahren abhängig. Lern-, Klausur- und Kollaborationsplattformen stehen Lehrenden und Lernenden rund um die Uhr zur Verfügung, Forschungsaktivitäten werden international vernetzt. Der Einsatz von IT-Systemen führt dabei zu einer Effizienzsteigerung von Arbeitsabläufen bei gleichzeitig deutlich verbessertem Dienstleistungsangebot. Aus dem umfangreichen Einsatz von IT in Forschung, Lehre, Studium und Verwaltung erwächst ein hoher Anspruch an die Verfügbarkeit, die Vertraulichkeit und die Integrität der verarbeiteten Informationen, IT-Verfahren und IT-Systeme an der Ruhr-Universität Bochum. Die vorliegende Leitlinie zur Informationssicherheit und das ergänzende Rahmenkonzept zur Informationssicherheit, das Regeln zur Sicherung der Informationsverarbeitung beschreibt, dienen diesem Anspruch. Sie wahren den Geist des kooperativen und respektvollen Miteinanders der universitären Gemeinschaft. Einschränkungen der Nutzung und des Betriebs von IT-Systemen, IT-Verfahren und Dienstleistungen erfolgen nur in dem Maße, das zur Erreichung der Sicherheitsziele unabdingbar notwendig ist.

Das Rektorat hat die vorliegende Leitlinie zur Informationssicherheit beschlossen und unterstützt die Maßnahmen zur Informationssicherheit. Damit trägt es zur sicheren IT-Nutzung und zum sicheren IT-Betrieb an der RUB bei. Ziel ist es, Forschung und Lehre kontinuierlich auf höchstem Niveau betreiben zu können sowie Studium und Verwaltung optimal zu unterstützen.

ZIELE UND ADRESSATENKREIS

Die Realisierung von angemessener Verfügbarkeit, Vertraulichkeit und Integrität sowie die Gewährleistung des Datenschutzes sind grundlegende Ziele der Informationssicherheit. Dabei bezeichnet

- Verfügbarkeit die Gewährleistung, dass Informationen, Anwendungen und IT-Systeme für Berechtigte im vorgesehenen Umfang und in angemessener Zeit nutzbar sind.
- Vertraulichkeit die Gewährleistung, dass Informationen ausschließlich Berechtigten zugänglich sind.
- Integrität, dass Unverfälschtheit und Vollständigkeit von Informationen, Anwendungen und IT-Systemen überprüfbar sind.

Die vorliegende Leitlinie bestimmt die Prinzipien zur Ausgestaltung der Informationssicherheit an der RUB. Sie ist an alle Organisationseinheiten, Mitglieder und Angehörige der RUB sowie an Dritte gerichtet, die IT-Systeme (z.B. Arbeitsstationen, Notebooks, Smartphones, Server oder Netzwerkkomponenten) und IT-Verfahren (Zusammenwirken von Anwendungen und IT-Systemen) der RUB benutzen oder betreiben.

LEITSÄTZE

Die nachfolgenden Leitsätze bestimmen die Gestaltung der Informationssicherheit an der RUB.

- Die vorrangigen Kriterien für geeignete Sicherheitsmaßnahmen sind deren Wirksamkeit in Verbindung mit einem tragbaren Restrisiko. Dabei werden insbesondere die wirtschaftliche Angemessenheit, die Ergonomie sowie die größtmögliche Handlungsfreiheit für Lehre und Forschung berücksichtigt.
- Gesetzliche und vertragliche Anforderungen sowie Selbstverpflichtungen, wie die zur guten wissenschaftlichen Praxis, werden erfüllt.
- Die Verfügbarkeit der IT, die für die ordnungsgemäße Durchführung insbesondere der Lehre, Forschung und der IT-gestützten Verwaltungsprozesse erforderlich ist, wird gewährleistet.
- Jeglicher Umgang mit Daten und Informationen entspricht von der Erhebung bis zur Löschung den Anforderungen der Informationssicherheit. Sämtliche IT-Systeme werden in angemessen sicherer Weise und Umgebung betrieben.
- Es gibt eine geordnete Vorgehensweise für die Inbetriebnahme und die Änderung von IT-Verfahren. In diesem werden die Belange der Informationssicherheit in angemessenem Umfang berücksichtigt.
- Anwenderinnen und Anwender haben ein Grundverständnis für die Belange der Informationssicherheit. IT-Systeme werden durch Personal betreut, welches über die erforderliche Fachkunde verfügt.
- Das Angebot regelmäßiger und anlassbezogener Schulungen gehört zum Selbstverständnis eines geordneten Informationssicherheitsprozesses.
- Die Wirksamkeit und Angemessenheit der Sicherheitsmaßnahmen wird regelmäßig überprüft und dokumentiert. Dies schließt die vorliegende Leitlinie zur Informationssicherheit ein.
- Verletzungen der Informationssicherheit werden kommuniziert und dokumentiert, so dass schnell, angemessen und nachhaltig auf sie reagiert werden kann.

Zentrale Angebote unterstützen die Umsetzung der Leitsätze.

ORGANISATIONSSTRUKTUR

Zur Gestaltung des Informationssicherheitsprozesses an der RUB wird eine Informationssicherheits-Organisation eingerichtet. Diese setzt sich zusammen aus der oder dem Beauftragten für Informationssicherheit (ISB) der RUB, der oder dem behördlichen Datenschutzbeauftragten (bDSB), den dezentralen Beauftragten für Informationssicherheit und dem Koordinierungsausschuss für Informationssicherheit.

Aufgaben der Beauftragten für Informationssicherheit

Die Beauftragten für Informationssicherheit initiieren, koordinieren und dokumentieren die Entwicklung, Umsetzung, Kontrolle und Fortschreibung des Regelwerks zur Informationssicherheit. Sie sind bei der Einführung neuer und Änderung bestehender Verfahren frühzeitig zu beteiligen. Sie beraten und sensibilisieren zu Fragen der Informationssicherheit.

Die Beauftragten für Informationssicherheit unterstützen die/den behördliche/n Datenschutzbeauftragte/n bei der Aufgabenerfüllung.

Die/Der zentrale Beauftragte für Informationssicherheit der RUB

Die/Der zentrale Beauftragte für Informationssicherheit hat die Leitung der Stabsstelle für Informationssicherheit des Rektorats inne. Sie/Er nimmt die Aufgabenerfüllung einrichtungsübergreifend für die RUB wahr und steht dem Rektorat, den dezentralen Beauftragten für Informationssicherheit und den Leitungen der Einrichtungen beratend zur Verfügung. Die/Der zentrale Beauftragte für Informationssicherheit ist bei der Einführung oder Änderung aller Verfahren mit einrichtungsübergreifender Auswirkung sowie bei sonstigen Verfahren auf Verlangen zu beteiligen.

Die/der zentrale IT-Sicherheitsbeauftragte der RUB nimmt die Funktion der/des zentralen Beauftragten für Informationssicherheit wahr.

Die dezentralen Beauftragten für Informationssicherheit

Die dezentralen Beauftragten für Informationssicherheit nehmen ihre Aufgaben innerhalb einer oder mehrerer Einrichtungen der

RUB, wie z.B. innerhalb einer Fakultät, eines Lehrstuhls, eines Instituts oder der Universitätsverwaltung wahr. Bei einrichtungsübergreifenden Fragestellungen und in Zweifelsfällen beteiligen die dezentralen Beauftragten für Informationssicherheit die/den zentrale/n Beauftragte/n für Informationssicherheit.

Sie unterstützen die/den zentrale/n Beauftragte/n für Informationssicherheit bei der Aufgabenerfüllung.

Die Einsetzung von Beauftragten für Informationssicherheit wird allen Organisationseinheiten der RUB empfohlen, andernfalls nimmt die Leitung der Einrichtung diese Funktion wahr.

Die Benennung der dezentralen Beauftragten für Informationssicherheit ist zu dokumentieren und der Stabsstelle für Informationssicherheit des Rektorats anzuzeigen.

Koordinierungsausschuss für Informationssicherheit

Der Koordinierungsausschuss für Informationssicherheit (IS-Koordinierungsausschuss) erarbeitet und empfiehlt in Zusammenarbeit mit den Beauftragten für Informationssicherheit die Leitlinie und das Rahmenkonzept zur Informationssicherheit und begleitet die Umsetzung und Dokumentation. Zum IS-Koordinierungsausschuss zählen die/der zentrale Beauftragte für Informationssicherheit der RUB (Vorsitz), die/der behördliche Datenschutzbeauftragte, vier Vertreterinnen oder Vertreter der Fachbereiche sowie jeweils eine Vertreterin oder ein Vertreter des Rechenzentrums, der Universitätsbibliothek, der Hochschulverwaltung, der Personalräte und der Studierendenschaft. Die Personen aus den Fachbereichen werden vom IT-Beirat der RUB benannt und sollen die Bereiche Geistes-/Gesellschaftswissenschaften, Ingenieurwissenschaften, Medizin und Naturwissenschaften repräsentieren.

Weitere Teilnehmende können vom IS-Koordinierungsausschuss eingeladen werden.

Fachkunde

Die Beauftragten für Informationssicherheit und die Mitglieder des Koordinierungsausschusses für Informationssicherheit verfügen über die erforderliche Fachkunde. Regelmäßige und anlassbezogene Schulungen bilden die Grundlage einer adäquaten Behandlung aller Aspekte der Informationssicherheit.

VERANTWORTLICHKEITEN

Die Leitung der Universität trägt die Gesamtverantwortung für die Informationssicherheit an der RUB.

Die Leitung jeder Einrichtung der RUB trägt die Verantwortung für die Informationssicherheit an ihrer Einrichtung.

Alle Anwenderinnen und Anwender tragen die Verantwortung, bestimmungsgemäß und sachgerecht mit den von ihnen genutzten Informationen umzugehen. Sie sind gehalten, die Regeln zur Informationssicherheit für ihren Arbeitsbereich anzuwenden.

Die Finanzierung der Maßnahmen zur Informationssicherheit wird den Verantwortlichkeiten entsprechend sichergestellt.

ABWEHR VON GEFÄHRDUNGEN

Bei Gefährdung der Informationssicherheit, die von den Beauftragten für Informationssicherheit, der/dem behördlichen Datenschutzbeauftragten oder der Leitung des Rechenzentrums festgestellt wird, veranlassen diese nach Risikoabwägung unverzüglich die notwendigen und angemessenen Maßnahmen. Bei erheblichen Gefährdungen kann dies insbesondere die Sperrung von Zugängen für die Nutzung eines IT-Verfahrens oder die Isolierung der gefährdenden oder gefährdeten IT-Systeme und Netze sein. Die Maßnahmen zur Gefahrenabwehr werden durch das Rechenzentrum oder durch die Betreiber/innen der IT einer Einrichtung umgesetzt. Sie bleiben nur so lange umgesetzt, wie die Gefährdung andauert. Sowohl die Feststellung der Gefahr als auch die Maßnahmen sind mit Angabe von Gründen zu dokumentieren und den zuständigen dezentralen sowie der/dem zentralen Beauftragten für Informationssicherheit unverzüglich mitzuteilen.

RAHMENKONZEPT ZUR INFORMATIONSSICHERHEIT

Das diese Leitlinie ergänzende Rahmenkonzept zur Informationssicherheit beinhaltet die allgemeinen Regeln und Hinweise zur Informationssicherheit für unterschiedliche Anwendergruppen. Es wird durch weiterführende detaillierte Maßnahmenbeschreibungen ergänzt.

Das Rektorat beschließt auf Empfehlung des Koordinierungsausschusses für Informationssicherheit das Rahmenkonzept zur Informationssicherheit und veröffentlicht es.

VERPFLICHTUNGEN

Mitglieder und Angehörige der RUB sowie Dritte, die die IT-Infrastruktur, IT-Systeme oder IT-Verfahren der RUB benutzen oder für die RUB betreiben, werden auf die Einhaltung der vorliegenden Leitlinie und des Rahmenkonzeptes zur Informationssicherheit verpflichtet.

Die Regelungen zur Informationssicherheit werden bei vertraglichen Beziehungen mit Dritten berücksichtigt.