Beraten und beschlossen in der Sitzung des Präsidiums der Universität Osnabrück am 17.09.2020

Informationssicherheitsrichtlinie der Universität Osnabrück

(Stand 02.07.2020)

Präambel

Funktionierende und sichere IT-Prozesse sind eine zentrale Grundlage für die Leistungsfähigkeit einer Hochschule. Der Hochschulbetrieb erfordert in zunehmenden Maß die Integration von Verfahren und Abläufen, die sich auf die Möglichkeiten der Informationstechnik (IT) stützen. Dafür ist aber die Sicherstellung der Integrität, Vertraulichkeit und Verfügbarkeit von Daten, Programmen und Diensten zwingend erforderlich.

Unter diesen Bedingungen kommt der „Sicherheit in der Informationstechnik“ („IT-Sicherheit“) und der Informationssicherheit eine grundsätzliche und strategische Bedeutung in der Hochschule zu, die die Entwicklung und Umsetzung einer hochschulweit einheitlichen Rahmenrichtlinie der Informationssicherheit erforderlich macht. Hauptziel der Gestaltung von Informationssicherheit muss es sein, den entsprechenden Rahmen für das Funktionieren von Lehre und Forschung zu bieten.

Dieses kann wegen der komplexen Materie, der sich schnell weiter entwickelnden technischen Möglichkeiten und wegen der begrenzten finanziellen und personellen Möglichkeiten nur in einem kontinuierlichen Informationssicherheitsprozess erfolgen, der den besonderen Bedingungen der Hochschule gerecht wird.

Diese Richtlinie regelt die Zuständigkeiten und die Verantwortung sowie die Zusammenarbeit im hochschulweiten Informationssicherheitsprozess. Ziel der Informationssicherheitsrichtlinie ist es dazu beizutragen, dass die existierenden gesetzlichen Auflagen erfüllt werden. Damit soll die Hochschule u. a. auch vor Imageverlust und finanziellen Schäden bewahrt werden.

Die Entwicklung und Fortschreibung des Informationssicherheitsprozesses sollten sich an den Prinzipien orientieren, die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) im IT-Grundschutzkatalog niedergelegt sind.

§1 Gegenstand der Richtlinie

Gegenstand dieser Richtlinie sind die Festlegung der zur Realisierung eines hochschulweiten Informationssicherheitsprozesses erforderlichen Verantwortungsstrukturen, eine grobe Aufgabenzuordnung sowie die Festlegung der Zusammenarbeit der Beteiligten. Diese Richtlinie wird ergänzt durch die separaten Ordnungen für die Benutzung der IT-Infrastrukturen der Hochschule.

§2 Geltungsbereich

Der Geltungsbereich dieser Richtlinie erstreckt sich auf alle Einrichtungen der Hochschule, auf die gesamte IT-Infrastruktur der Hochschule, einschließlich der daran betriebenen IT-Systeme, sowie die Gesamtheit der Benutzer*innen.

§3 Beteiligte am IT-Sicherheitsprozess

Die Hauptverantwortung für den IT-Sicherheitsprozess liegt bei der Hochschulleitung. Zur Wahrnehmung dieser Verantwortung stützt sich die Hochschulleitung auf folgende Beteiligte:

(1) Informationssicherheitsmanagement-AG

(2) Einführung von dezentralen Informationssicherheitskoordinator*innen

(3) Rechenzentrum und weitere zentrale Einrichtungen der Hochschule, insbesondere die Bibliothek und das virtUOS

§4 Einsetzung der Beteiligten

(1) Die Hochschulleitung setzt eine Informationssicherheitsmanagement-AG (ISM-AG) ein. Die Zusammensetzung der ISM-AG sollte – unter Beschränkung der Anzahl der Mitglieder auf das notwendige Maß – sowohl die unterschiedlichen Aufgabenbereiche der Hochschule widerspiegeln als auch die unterschiedlichen, für die Hochschule relevanten Aspekte der Informationssicherheit berücksichtigen.

Ständige Mitglieder der ISM-AG sind:

- der/die Sprecher*in des CIO-Gremiums

- der/die Datenschutzbeauftragte / Informationssicherheitsbeauftragte

- zwei Vertreter*innen der dezentralen Informationssicherheitskoordinator*innen (siehe Abs. (3))

- ein/e Vertreter*in des Rechenzentrums

- ein/e Vertreter*in des virtUOS

- ein/e Vertreter*in aus der IT der Universitätsbibliothek

- ein Mitglied des Personalrats

- ein Mitglied der Studierendengruppe

Personalunion ist zulässig. Vertretung ist zulässig. Weitere sachverständige Mitglieder werden von der ISM-AG benannt.

(2) Die ISM-AG wird von dem/der der Sprecher*in des CIO-Gremiums koordiniert, die/der als Vorsitzende/r die Sitzungen der ISM-AG leitet. Der Vorsitz ist delegierbar.

(3) Die ISM-AG kann zur Unterstützung ihrer Arbeit im operativen Bereich eine weitere Arbeitsgruppe einsetzen. Bei Bedarf sollte sie den Rat von Expert*innen einholen (z. B. Jurist*innen, Spezialist*innen für Teilbereiche der IT- und Informationssicherheit, etc.).

(4) Jeder Fachbereich und jede Organisationseinheit der Hochschule hat einen dezentralen/eine dezentrale Informationssicherheitskoordinator*in und einen/eine Stellvertreter*in zu benennen. Es kann aber auch ein dezentraler/eine dezentrale Informationssicherheitskoordinator*in für mehrere Einrichtungen zuständig sein.

(5) Bei der Bestellung/Benennung der im Informationssicherheitsprozess aktiven Personen soll die erforderliche personelle Kontinuität berücksichtigt werden. Deshalb sollen die Informationssicherheitskoordinator*innen über langfristige Verträge verfügen oder möglichst zum hauptamtlichen Personal der Hochschule gehören.

(6) Die Einsetzung von Informationssicherheitskoordinator*innen entbindet die Leitung einer Organisationseinheit nicht von ihrer Gesamtverantwortung für die Informationssicherheit in ihrem Zuständigkeitsbereich.

§5 Aufgaben der Beteiligten

(1) Die ISM-AG ist für die Richtlinienerstellung, Fortschreibung und Umsetzung des Informationssicherheitsprozesses verantwortlich. Unter anderem ist dabei das Erarbeiten von Notfallplänen zu berücksichtigen.

(2) Die ISM-AG gibt die hochschulinternen technischen Standards zur Informationssicherheit vor. Außerdem veranlasst sie die Schulung und Weiterbildung der dezentralen Informationssicherheitskoordinator*innen und die Unterstützung bei der Richtlinienumsetzung.

(3) Die ISM-AG dokumentiert und berät bei sicherheitsrelevanten Vorfällen.

(4) Der/die Datenschutzbeauftragte berät gemeinsam mit dem/der Vorsitzenden der ISM-AG die Hochschulleitung in relevanten Fragen der Informationssicherheit.

(5) Die dezentralen Informationssicherheitskoordinator*innen informieren die ISM-AG über Sicherheitsbelange bei den IT-Systemen und -Anwendungen sowie über relevante Prozesse in ihren Zuständigkeitsbereichen und machen Vorschläge zu deren Verbesserung.

(6) Das Rechenzentrum ist im Wesentlichen für die system-, netz- und betriebstechnischen Aspekte der technischen IT-Sicherheit verantwortlich. Es arbeitet eng mit der ISM-AG zusammen.

(7) Die Organisationseinheiten der Hochschule sind verpflichtet, bei allen relevanten Planungen, Verfahren und Entscheidungen mit Bezug zur Informationssicherheit die ISM-AG zu informieren.

(8) 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.

§6 Umsetzung des Informationssicherheitsprozesses

(1) Die ISM-AG unterstützt das Präsidium bei der Initiierung, Steuerung und Kontrolle der Umsetzung des Informationssicherheitsprozesses, der nach festzulegenden Prioritäten technische und organisatorische Maßnahmen sowohl präventiver als auch reaktiver Art sowie Maßnahmen zur schnellen Krisenintervention umfassen muss.

(2) Die dezentralen Informationssicherheitskoordinator*innen sind insbesondere für die kontinuierliche Überwachung der Umsetzung des Informationssicherheitsprozesses in ihren Bereichen zuständig. Sie informieren regelmäßig sowohl die Leitung ihrer Organisationseinheit als auch die ISM-AG über den Stand der Umsetzung und aktuelle Problemfälle.

(3) Es sind Notfallpläne zu erarbeiten, die Handlungsanweisungen und Verhaltensregeln für bestimmte Gefahrensituationen und Schadensereignisse beinhalten, mit dem Ziel, die Wahrscheinlichkeit und/oder die Auswirkungen von solchen Ereignissen auf ein akzeptables Niveau zu verringern sowie eine möglichst schnelle Wiederherstellung der Verfügbarkeit der IT-Ressourcen zu erreichen.

(4) Alle Angehörigen und Mitarbeiter*innen der Hochschule sollen sicherheitsrelevante Ereignisse umgehend der Leitung der Organisationseinheit melden.

§7 Krisenintervention

(1) Bei Gefahr im Verzuge informieren die dezentralen Informationssicherheitskoordinator*innen schnellstmöglich die Leitung der Organisationseinheit und den CIO (in Vertretung den Sprecher des CIO-Gremiums), welche ggf. die sofortige vorübergehende Stilllegung betroffener IT-Systeme im betroffenen Bereich veranlassen, wenn zu befürchten ist, dass ein voraussichtlich gravierender Schaden nicht anders abzuwenden ist.

(2) Soweit das Rechenzentrum Gefahr im Verzuge feststellt, kann es Netzanschlüsse und andere Ressourcen (soweit möglich mit vorheriger Benachrichtigung der Betroffenen) vorübergehend

sperren, wenn zu befürchten ist, dass ein voraussichtlich gravierender Schaden für die IT-Infrastruktur und/oder Informationssicherheit der Hochschule nicht anders abzuwenden ist. Der/die zuständige dezentrale Informationssicherheitskoordinator*in sowie die ISM-AG werden unverzüglich, ggf. nachträglich, informiert.

(3) Die Wiederinbetriebnahme erfolgt erst nach der Durchführung hinreichender IT-Sicherheitsmaßnahmen in Abstimmung mit der ISM-AG.

§8 In-Kraft-Treten

Diese Richtlinie tritt nach ihrer Verabschiedung im Senat am Tag nach ihrer Bekanntmachung in Kraft.