

Erläuterungen der Ordnung zur Informationssicherheit

Diese Handreichung ist eine Hilfestellung zur Umsetzung der Ordnung zur Informationssicherheit der Leibniz Universität Hannover.

Bindend sind die Regelungen der Ordnung.

Informationssicherheitsstab

bearbeitet von:
IT-Sicherheitsteam des LUIS
Tel. +49 511 762 4663
E-Mail: security@uni-hannover.de

16.05.2019

Dezentrale Informationssicherheitsbeauftragte

Um die elektronische Daten- und Informationsverarbeitung der Leibniz Universität Hannover (LUH) zu schützen, hat die LUH bereits 2002 mit dem Erlassen einer IT-Sicherheitsordnung angefangen, nicht nur einen IT-Sicherheitsprozess zu initiieren, sondern auch ein Informationssicherheitsmanagement aufzubauen. Dabei wurden auf zentraler und dezentraler Ebene die Rolle von IT-Sicherheitsbeauftragten eingeführt. Mit der Überarbeitung der Ordnung 2018/2019 wurden deren Rollen mit ihren Aufgaben und Befugnissen anhand der Erfahrungen der letzten Jahre und in Bezug auf die neue Ordnung zur IT-Organisationsstruktur 2019 angepasst.

Auf Ebene der Fakultäten, der Zentralen Universitätsverwaltung und der Zentralen Einrichtungen sind Dezentrale Informationssicherheitsbeauftragte vorgesehen. Sie stellen ein Bindeglied zwischen den Einrichtungen und dem Informationssicherheitsstab sowie der oder dem Zentralen Informationssicherheitsbeauftragten dar. Die Benennung muss nach §4, Abs. 2, inklusiv der Benennung einer Vertretung durch die Einrichtungen erfolgen.

Aufgaben

Die dezentralen Informationssicherheitsbeauftragten veranlassen die Umsetzung des Informationssicherheitsprozesses¹ in ihrem Zuständigkeitsbereich und überwachen diesen. Sie sind zentrale Ansprechpersonen für Belange der Informationssicherheit in Ihrem Zuständigkeitsbereich. Die Gesamtverantwortung für die Informationssicherheit verbleibt nach §6, Abs. 6, jedoch bei der Leitung der jeweiligen Einrichtung. Die Informationssicherheitsbeauftragten berichten der jeweiligen Einrichtungsleitung anlassbezogen sowie regelmäßig über den Stand der Informationssicherheit in ihrem Zuständigkeitsbereich und schlagen Maßnahmen zur Optimierung der Informationssicherheit vor.

Die Dezentralen Informationssicherheitsbeauftragten kommunizieren zentrale Vorgaben der Informationssicherheit in die Einrichtungen und veranlassen deren Umsetzung. Sie nehmen sicherheitsrelevante Informationen im Rahmen Ihrer Tätigkeit jederzeit entgegen und veranlassen notwendige Maßnahmen. Sie informieren die Einrichtungsleitung und das Informationssicherheitsteam des LUIS über kritische Informationssicherheitsvorfälle in ihrem Zuständigkeitsbereich.

Im Rahmen ihrer Tätigkeit arbeiten die Dezentralen Informationssicherheitsbeauftragten eng mit dem Informationssicherheitsteam des LUIS, den Ansprechpersonen für Datenschutz, den IT-Beauftragten und den FIOs zusammen und etablieren geeignete Kommunikationswege innerhalb der eigenen Einrichtung. Insbesondere koordinieren sie

Dienstgebäude:
Welfengarten 1
30167 Hannover

Zentrale:
Tel. +49 511 762 0
Fax +49 511 762 3456
www.uni-hannover.de

¹ Ein Informationssicherheitsprozess besteht aus den zyklischen Phasen akute und mögliche Bedrohungen analysieren, mögliche Schäden für die LUH bewerten, Maßnahmen für ein effizientes Risikomanagement entwickeln und umsetzen sowie den Erfolg der Maßnahmen kontrollieren.

dabei die Kommunikation und Umsetzung von Vorgaben und informationssicherheitsrelevanten Maßnahmen zwischen den zentralen Strukturen für Informationssicherheit und den dezentralen Einrichtungen.

Unterstützung

Dezentrale Informationssicherheitsbeauftragte sind bei allen für die Informationssicherheit relevanten Planungen und Entscheidungen in ihrem Zuständigkeitsbereich zu beteiligen. Die konkreten Konzepte und Umsetzungen sind durch die IT-Verantwortlichen und Administratoren zu erstellen, die so neben den Dezentralen Informationssicherheitsbeauftragten wesentlich bei der Umsetzung des Sicherheitsprozesses mitwirken.

Das Informationssicherheitsteam des LUIS informiert betroffene dezentrale Informationssicherheitsbeauftragte (i.d.R. per E-Mail) unverzüglich über relevante akute IT-Sicherheitsvorfälle und akute Bedrohungen. Das Informationssicherheitsteam des LUIS berät die dezentralen Informationssicherheitsbeauftragten und dezentralen IT-Verantwortlichen in operativen und strategischen Fragen der IT-Sicherheit. Zur Unterstützung veröffentlicht das Informationssicherheitsteam Informationen über Bedrohungen, Ursachen von Informationssicherheitsvorfällen und Gegenmaßnahmen im Webauftritt².

Zentrale Vorgaben zur Sicherstellung der Informationssicherheit werden über Rundschreiben im Vademecum unter „IT/IT-Sicherheit & Datenschutz“ veröffentlicht³. Zudem werden Empfehlungen und akute Vorgaben per E-Mail oder LUIS-News⁴ publiziert.

Anforderungsprofil

Informationssicherheitsbeauftragte sollen über IT Know How auch in Bezug auf Sicherheit verfügen. Aufgrund Ihrer Funktion als Bindeglied zwischen den zentralen Verantwortlichen und den dezentralen Einrichtungen (Instituten etc.) und aufgrund der Unterstützung durch das LUIS-Sicherheitsteam sind aber primär organisatorische Fähigkeiten wichtig. Zudem sollen Dezentrale Informationssicherheitsbeauftragte über Kenntnisse der spezifischen Strukturen und organisatorischen Regelungen in ihrem Zuständigkeitsbereich verfügen.

Zur Vermeidung von Interessenskonflikten sollen dezentrale Informationssicherheitsbeauftragte nicht über den operativen oder strategischen IT-Einsatz in der Einrichtung entscheiden. Es empfiehlt sich daher auch nicht, eine oder einen FIO zu benennen. Um die Kontinuität des Informationssicherheitsprozesses sicherzustellen, sollen Informationssicherheitsbeauftragte zum hauptamtlichen Personal gehören.

Dienstrechtliche Stellung

Durch eine Benennung zur oder zum Dezentralen Informationssicherheitsbeauftragten ändert sich nichts am Dienstverhältnis. Sie oder er bleibt der oder dem unmittelbaren Dienstvorgesetzten unterstellt. Zur Erfüllung der Aufgaben und zur Teilnahme an Schulungen ist ausreichend Zeit zur Verfügung zu stellen. Es bestehen keine besonderen Weisungsbefugnisse gegenüber anderen Mitarbeitenden oder Administratoren. Bei

2 https://www.luis.uni-hannover.de/it_sicherheit.html

3 <https://www.intern.uni-hannover.de/de/vademecum/vademecum-category/it/it-sicherheit-datenschutz/>

4 <https://www.luis.uni-hannover.de/aktuelles.html>

auftretenden Problemen kann sich die oder der Dezentrale Informationssicherheitsbeauftragte auf dem Wege des Berichtes an die betreffende Leitung der Einrichtung oder an die oder den Zentralen Informationssicherheitsbeauftragten wenden. Bei einem Bericht an die oder den zentralen Informationssicherheitsbeauftragten sind dezentrale Informationssicherheitsbeauftragte an keine Weisung der zuständigen Leitung der Einrichtung gebunden. Da die Gesamtverantwortung für die Informationssicherheit nach wie vor bei der zuständigen Leitung einer Einrichtung liegt, besteht für Dezentrale Informationssicherheitsbeauftragte kein erhöhtes Haftungsrisiko.

Benennung

Die Benennung erfolgt durch die Fakultäten, die Zentrale Universitätsverwaltung und die Zentralen Einrichtungen, die gemäß §4, Abs. 2 zur Benennung einer oder eines Informationssicherheitsbeauftragten und einer Stellvertretung verpflichtet sind. Es erfolgt keine Benennung unterhalb der genannten Einrichtungsebenen, insbesondere nicht in den einzelnen Instituten. Mehrere Zentrale Einrichtungen können auch eine gemeinsame Person benennen.

Da es eine inhaltliche Nähe in den Aufgaben und Anforderungsprofilen der dezentralen Informationssicherheitsbeauftragten und den dezentralen Ansprechpersonen für den Datenschutz gibt, können diese Funktionen in einer Person gebündelt werden.

Die benannten Dezentralen Informationssicherheitsbeauftragten sind dem Informationssicherheitsteam des LUIS zu melden.