# IT-Sicherheitsordnung

Präambel

Funktionierende und sichere IT-Prozesse sind eine zentrale Grundlage für die Leistungsfähigkeit einer Hochschule in den Bereichen Lehre, Forschung und Verwaltung.

Durch die zunehmende Abhängigkeit von der IT bestehen Gefahren für die Geschäftsprozesse der Hochschulen. Die Hochschulleitungen des Internationalen Hochschulinstituts Zittau und der Hochschule Zittau/Görlitz (im Folgenden Hochschulen) sind davon überzeugt, dass dieses Gefahrenpotential durch die konsequente Umsetzung eines IT-Sicherheitskonzeptes erheblich gemindert werden kann.
Das IT-Sicherheitskonzept verfolgt notwendigerweise folgende Ziele:

- Gewährleistung der Verfügbarkeit, Integrität, Vertraulichkeit und Verbindlichkeit von IT-Systemen und -Anwendungen, insbesondere den Schutz von Netzwerken, Rechnersystemen und Informationen (Hardware und Software) gegen Missbrauch von innen und außen, um den guten Ruf der Hochschule in der Öffentlichkeit und die gesetzliche Regelung sicherzustellen
- Sicherstellung eines reibungslosen Lehr-, Forschungs- und Verwaltungsbetriebes.

Die Hochschulleitungen übernehmen zur Erreichung dieser Ziele die Gesamtverantwortung und etablieren hierfür einen Sicherheitsprozess, der die beständige Aufrechterhaltung und Verbesserung der Informationssicherheit bewirkt. Hierzu werden die Hochschulleitungen geeignete und angemessene Maßnahmen in organisatorischer, technischer und personeller Hinsicht ergreifen.

Zur Erreichung dieser Ziele werden von den Hochschulleitungen unter Einbeziehung des IT-Sicherheitsmanagementteams Sicherheitsrichtlinien festgelegt und fortgeschrieben. Im Geiste des kooperativen und respektvollen Miteinanders der Mitglieder der beiden Hochschulen werden in den Sicherheitsrichtlinien Nutzungseinschränkungen der IT-Systeme und Dienstleistungen nur in dem Maße festgelegt, das zur Erreichung der Sicherheitsziele unabdingbar notwendig ist. Alle Sicherheitsrichtlinien werden in geeigneter Form bekannt gemacht.

Die Entwicklung und Fortschreibung der Richtlinien zur IT-Sicherheit muss sich einerseits an den gesetzlich festgelegten Aufgaben der Hochschulen sowie an ihrem Mandat zur Wahrung der akademischen Freiheit orientieren, andererseits ist sie nur über einen kontinuierlichen IT-Sicherheitsprozess innerhalb geregelter Verantwortungsstrukturen zu erzielen.

Diese Ordnung regelt die Zuständigkeiten und die Verantwortung sowie die Zusammenarbeit im hochschulübergreifenden IT-Sicherheitsprozess. Neben den genannten Zielen soll die IT-Sicherheitsordnung die Hochschulen vor Imageverlusten und finanziellen Schäden bewahren.

Die IT-Sicherheitsordnung orientiert sich an den Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

## § 1
## Gegenstand der Ordnung

Gegenstand dieser Ordnung ist die Festlegung der zur Realisierung eines hochschulübergreifenden IT-Sicherheitsprozesses erforderlichen Verantwortungsstrukturen, eine Aufgabenzuordnung sowie die Festlegung der Zusammenarbeit der Beteiligten. Diese Ordnung wird ergänzt durch weitere Ordnungen für die Benutzung der IT-Infrastrukturen und zur Regelung des Umgangs mit Informationen.

## § 2
## Geltungsbereich

Der Geltungsbereich dieser Ordnung erstreckt sich auf alle Struktureinheiten der Hochschule Zittau/Görlitz (Fakultäten, wissenschaftliche/zentrale Einrichtungen, Hochschulverwaltung) und das Internationale Hochschulinstitut Zittau sowie auf die gesamte IT-Infrastruktur der Hochschulen und deren Benutzergesamtheit.

## § 3
## Verantwortung für den IT-Sicherheitsprozess

Die Hauptverantwortung für den IT-Sicherheitsprozess liegt bei den Hochschulleitungen. Sie setzen gemeinsam folgende Gremien und Funktionsträger ein:

⇒ den Zentralen IT-Sicherheitsbeauftragten und

⇒ das IT-Sicherheitsmanagementteam (SMT)

## § 4
## IT-Sicherheitsbeauftragte

(1) Die Hochschulleitungen berufen den zentralen IT-Sicherheitsbeauftragten.

(2) Jede Struktureinheit der Hochschule Zittau/Görlitz und das IHI Zittau benennt einen dezentralen Sicherheitsbeauftragten. Mehrere Struktureinheiten können sich eines gemeinsamen dezentralen IT-Sicherheitsbeauftragten bedienen. Durch diese Benennungen müssen alle IT-Systeme im Geltungsbereich sowie die vor Ort für deren Betrieb verantwortlichen Personen einem IT-Sicherheitsbeauftragten zugeordnet sein.

(3) Bei der Benennung der dezentralen IT-Sicherheitsbeauftragten sollen der strategische Aspekt und die dafür erforderliche personelle Kontinuität berücksichtigt werden. Die IT-Sicherheitsbeauftragten sollen deshalb möglichst zum hauptamtlichen Personal gehören. Sie sollen in IT-Sicherheitsfragen besonders geschult werden.

## § 5
## IT-Sicherheitsmanagementteam (SMT)

(1) Ständige Mitglieder des IT-Sicherheitsmanagementteam sind:

- ⇒ der zentrale IT-Sicherheitsbeauftragte (Vorsitz),
- ⇒ ein Vertreter der Verwaltung,
- ⇒ ein Vertreter des Hochschulrechenzentrums,
- ⇒ die Datenschutzbeauftragten der Hochschulen
- ⇒ die Vertreter der dezentralen Sicherheitsbeauftragten (je Hochschulstandort)

(2) Die Personalräte können je ein beratendes Mitglied benennen.

(3) Aus der Mitte der ständigen Mitglieder des SMT wird ein Stellvertreter für den zentralen IT-Sicherheitsbeauftragten benannt.

(4) Weitere IT-sachverständige Mitglieder können von den Hochschulleitungen benannt werden. Die Anzahl der Mitglieder des SMT soll zehn nicht überschreiten.

## § 6
## Aufgaben

(1) Der zentrale IT-Sicherheitsbeauftragte ist für die Konzeption, Umsetzung und Überwachung des IT-Sicherheitsprozesses verantwortlich.
Die Aufgaben des zentralen IT- Sicherheitsbeauftragten sind insbesondere:

- ⇒ den IT-Sicherheitsprozess zu steuern und zu koordinieren,
- ⇒ die Rektorate bei der Erstellung der Leitlinie zur Informationssicherheit zu unterstützen,
- ⇒ die Erstellung des Sicherheits-, Notfallvorsorge- und anderer Teilkonzepte und System-Sicherheitsrichtlinien zu koordinieren sowie weitere Richtlinien und Regelungen zur Informationssicherheit zu erlassen,
- ⇒ den Realisierungsplan für die Sicherheitsmaßnahmen zu erstellen und deren Realisierung zu initiieren und zu überprüfen,
- ⇒ die Rektorate und das IT-Sicherheitsmanagementteam über den Status Quo der Informationssicherheit zu berichten,
- ⇒ sicherheitsrelevante Projekte zu koordinieren und den Informationsfluss zwischen Bereichs-IT-, Projekt- sowie IT-System-Sicherheitsbeauftragten sicherzustellen,
- ⇒ sicherheitsrelevante Zwischenfälle zu untersuchen sowie
- ⇒ Sensibilisierungs- und Schutzmaßnahmen zur Informationssicherheit zu initiieren und zu steuern.

(2) Das Hochschulrechenzentrum ist in Zusammenarbeit mit dem SMT verantwortlich für die system-, netz- und betriebstechnischen Aspekte der IT-Sicherheit und gibt in diesem Rahmen Empfehlungen zu technischen Standards zur IT-Sicherheit vor.

(3) Das Sicherheitsmanagementteam unterstützt den zentralen IT-Sicherheitsbeauftragten, indem es Pläne, Leitlinien und Vorgaben für sämtliche übergreifenden Belange der IT-Sicherheit erarbeitet, Maßnahmen koordiniert, Informationen zusammenträgt und Kontrollaufgaben durchführt. Zur Aufgabenerfüllung kann das SMT externe Berater hinzuziehen.

(4) Die dezentralen IT-Sicherheitsbeauftragten sind für die Umsetzung aller Sicherheitsbelange der IT-Systeme und -Anwendungen in den Bereichen, die ihnen jeweils zugeordnet sind, verantwortlich. Dabei haben sie die Vorgaben des Sicherheitsmanagementteams zu beachten.

(5) Die Einsetzung von IT-Sicherheitsbeauftragten entbindet die Leiter der Struktureinheiten nicht von ihrer Verantwortung zur Umsetzung der IT-Sicherheit in ihrem Bereich.

(6) Die Struktureinheiten sind verpflichtet, bei allen Planungen, Verfahren und Entscheidungen mit Bezug zur IT-Sicherheit die jeweils zuständigen dezentralen IT-Sicherheitsbeauftragten zu beteiligen. Die dezentralen IT-Sicherheitsbeauftragten können bei Entscheidungen den zentralen IT-Sicherheitsbeauftragten einbezogen werden.

## § 7
## IT-Sicherheitsprozess

(1) Der zentrale IT-Sicherheitsbeauftragte plant, steuert und kontrolliert unter Beteiligung des Sicherheitsmanagementteams den IT-Sicherheitsprozess, der nach festzulegenden Prioritäten Maßnahmen, insbesondere zu schneller Krisenintervention umfassen muss. Der IT-Sicherheitsprozess ist dabei ständig weiterzuentwickeln, auf seine Wirksamkeit zu prüfen und ggf. anzupassen, um die IT-Sicherheit aufrechtzuerhalten und eine kontinuierliche Verbesserung sicherzustellen. Zwecks Gewährleistung einer kontinuierlichen Steuerung des IT-Sicherheitsprozesses soll das Sicherheitsmanagementteam regelmäßig tagen.

(2) Die dezentralen IT-Sicherheitsbeauftragten sind verpflichtet, sicherheitsrelevante Informationen jederzeit entgegenzunehmen und das jeweils Erforderliche zu veranlassen. Soweit notwendig, informieren sich dezentrale IT-Sicherheitsbeauftragte zu Ursachen und Maßnahmen durch Kontaktaufnahme zum zentralen IT-Sicherheitsbeauftragten und/oder zum Hochschulrechenzentrum.

(3) Die dezentralen IT-Sicherheitsbeauftragten sind für die kontinuierliche Überwachung der Umsetzung des IT-Sicherheitsprozesses in ihrem Bereich verantwortlich. Sie informieren sich regelmäßig über die Sicherheit der IT-Systeme in ihrem Bereich und veranlassen unverzüglich die notwendigen Maßnahmen zur Gewährleistung der erforderlichen Sicherheit. Sie informieren die Leiter ihrer Struktureinheiten und den zentralen IT-Sicherheitsbeauftragten regelmäßig über den Sicherheitsstandard und auftretende Probleme und schlagen Lösungsmöglichkeiten vor.

(4) Der zentrale IT-Sicherheitsbeauftragte berichtet den Rektoraten und dem Senat bzw. dem Institutsrat aus gegebenem Anlass darüber und macht Vorschläge für die Weiterentwicklung des IT-Sicherheitsprozesses unter Berücksichtigung der Ausgewogenheit, Durchgängigkeit und Angemessenheit der Maßnahmen. Dabei ist die Höhe des voraussichtlichen finanziellen Aufwandes der einzelnen Maßnahmen anzugeben.

(5) Die dezentralen IT-Sicherheitsbeauftragten sind bezüglich ihrer Mitteilungspflichten gegenüber dem zentralen IT-Sicherheitsbeauftragten, den Rektoraten und dem Senat bzw. Institutsrat unabhängig von Weisungen ihrer Vorgesetzten. Alle Nutzer sind verpflichtet, Vorfälle und andere relevante Informationen unverzüglich an den jeweiligen dezentralen IT-Sicherheitsbeauftragten zu melden.

## § 8
## Gefahrenintervention

(1) Bei Gefahr im Verzug veranlassen die dezentralen IT-Sicherheitsbeauftragten die sofortige vorübergehende Stilllegung betroffener IT-Systeme in ihrem Bereich, wenn zu befürchten ist, dass ein voraussichtlich gravierender Schaden - insbesondere für andere Einrichtungen oder für die Infrastruktur in Teilen oder insgesamt - nicht anders abzuwenden ist.

(2) Soweit das Hochschulrechenzentrum Gefahr in Verzug feststellt, kann es Netzanschlüsse (ggf. auch ohne vorherige Benachrichtigung der Betroffenen) vorübergehend sperren, wenn zu befürchten ist, dass ein voraussichtlich gravierender Schaden für die IT-Infrastruktur in Teilen oder insgesamt nicht anders abzuwenden ist. Die Benachrichtigung des zuständigen dezentralen sowie des zentralen IT-Sicherheitsbeauftragten erfolgt unverzüglich, ggf. nachträglich.

(3) Vor Wiederinbetriebnahme vorübergehend stillgelegter Systeme bzw. gesperrter Netzanschlüsse ist in der Regel die Durchführung hinreichender Sicherheitsmaßnahmen erforderlich. Im Zweifelsfall entscheidet der zentrale IT-Sicherheitsbeauftragte in Abstimmung mit dem Hochschulrechenzentrum über das weitere Vorgehen.

## § 9
## Finanzierung

(1) Die Mittel für spezielle, mit dem zentralen IT-Sicherheitsbeauftragten und dem Hochschulrechenzentrum abgestimmte Sicherheitsmaßnahmen in den Struktureinheiten der Hochschule und im Internationalen Hochschulinstitut Zittau sowie insbesondere Mittel zur Schulung zur IT-Sicherheit sind grundsätzlich von den betreffenden Struktureinheiten bzw. vom Internationalen Hochschulinstitut Zittau aufzubringen. Die Mittel sind für diese Zwecke in ihrer Finanzplanung angemessen zu berücksichtigen.

(2) Soweit Sicherheitsmaßnahmen aus zentralen Mitteln finanziert werden müssen, ordnet der zentrale IT-Sicherheitsbeauftragte in Abstimmung mit dem Sicherheitsmanagementteam diese nach Dringlichkeit in einer Liste. Mit einer Begründung der Prioritäten schlägt er den Rektoraten die Finanzierung vor.

## § 10
## Inkrafttreten

Diese Ordnung tritt am Tag nach ihrer hochschulöffentlichen Bekanntmachung in Kraft.

Zittau, den 28.4.2010

Prof. Dr. phil. Albrecht
Rektor
Hochschule Zittau/Görlitz

Univ.-Prof. Dr. rer. Pol. habil. Löhr
Rektor
Internationales Hochschulinstitut Zittau