Universität Bielefeld	**IT-Sicherheitsrichtlinie für Datacenter**
Art: IT-Sicherheitsrichtlinie	Version: 1.1
Verfassende: Michael Sundermeyer	Freigabedatum: 11.07.2008
Zielgruppe: IT-Personal	Letzte Änderung: 11.07.2008

1. Einführung

Die Universität Bielefeld ist in hohem Maß auf die Integrität, Verfügbarkeit und Vertraulichkeit der Systeme und gespeicherten Informationen in ihren Datacentern angewiesen. Es gilt diese Werte zu jedem Zeitpunkt angemessen zu schützen.

Die Datacenter des Hochschulrechenzentrums (HRZ) der Universität Bielefeld befinden sich in den Bereichen V0 („Maschinensaal“) und S01 („Lampertzzelle“) und stellen eine sichere Umgebung für den Betrieb und die Administration der eingestellten Systeme zur Verfügung.

Alle Bereiche, ihre Beschäftigten und Auftragnehmer, die Systeme in den Datacentern des Rechenzentrums betreiben oder betreuen, stimmen den Regelungen dieser Richtlinie zu und beachten diese bei ihrer Arbeit.

Fragen zu diesem Dokument können an die HRZ Anwenderberatung, Durchwahl 2398 oder die Verfassenden gerichtet werden.

2. Zutrittsregelungen

2.1 Allgemeines

Die Verantwortung für die Sicherheit in den Datacentern liegt bei allen Einrichtungen der Universität die diese nutzen. Die Datacenter sind zugangsbeschränkte Bereiche, die ein höheres Maß an Kontrolle benötigen als andere nichtöffentliche Bereiche der Universität.
Nur Personen die autorisiert wurden, ist der Zutritt gestattet. Zutrittsberechtigungen erhalten nur Personen, die diese für ihre Arbeit in den Datacentern benötigen.

2.2 Zutrittskontrollsystem

Das Zutrittskontrollsystem des HRZ wird durch eine/n Beschäftigte/n des HRZ verwaltet. Der oder die „Verwalter/in des Zutrittskontrollsystems“ vergibt über elektronische Schlüssel (Sicherheitstokens) Berechtigungen, welche Zutritt zu den Datacentern gewähren.

Bei der Handhabung und Vergabe von Zutrittsberechtigungen über das Zutrittskontrollsystem ist die aktuell gültige Dienstvereinbarung zu beachten.

Das Anlegen und die Änderungen der Zutrittsberechtigungen für die Datacenter werden nachvollziehbar im Zutrittskontrollsystem protokolliert.

Personengebundene Tokens und Funktionstokens werden auf die notwendigen Aufenthalts-, Arbeitsbereiche und Arbeitszeiten beschränkt.

Die Herausgabe von Sicherheitstokens, die Zutritt zu den Datacentern gewähren und nicht an eine Person gebunden sind (sogenannte „Funktionstokens“), wird nachvollziehbar dokumentiert.

2.3 Zutrittsberechtigungen

Für die Beantragung der Zutrittsberechtigung sowie die Ausgabe und Nutzung des Sicherheitstokens sind insbesondere die § 2 bis § 5 „Dienstvereinbarung zur Einführung eines elektronischen Schließ- und Zutrittskontrollsystems im Hochschulrechenzentrum der Universität Bielefeld“ maßgeblich.

Zutrittsberechtige sind Personen, die auf Basis Ihres Tätigkeitsprofils Zutritt zu definierten Bereichen der Datacenter benötigen und einen persönlichen Sicherheitstoken erhalten haben. Zutrittberechtigungen zu den Datacentern bzw. zu den Zellen des Maschinensaals werden auf Antrag durch den oder die Verwalter/in des Zutrittskontrollsystems des HRZ erteilt. Die Zutrittsberechtigen erhalten einen elektronischen Sicherheitstoken und die entsprechende Dienstvereinbarung.
Zutrittsberechtigungen für den Housing-Bereich der Datacenter werden maximal für ein Jahr vergeben, und laufen spätestens zum 31.01. des Vergabezeitraumes ab. Eine Verlängerung der Zutrittsberechtigungen wird durch den oder die Verwalter/in des Zutrittskontrollsystems im HRZ erteilt.
Ist die Notwendigkeit für eine Zutrittsberechtigung z.B. durch die Änderung oder den Wegfall einer Tätigkeit entfallen, sind die Berechtigten verpflichtet, dies umgehend dem HRZ mitzuteilen und den ausgehändigten Sicherheitstoken zurückzugeben.
Ein Verlust des Sicherheitstokens ist dem HRZ unverzüglich zu melden, damit dieser gesperrt werden kann.

Es werden folgende Zutrittsberechtigungen unterschieden: Generalberechtigter, teilberechtigter und begleiteter Zutritt:

Eine **Generalberechtigung** erhalten Personen, die einen freien Zutritt zu allen Bereichen der Datacenter benötigen. Zu diesen zählen insbesondere Beschäftigte des Dezernates FM (Klima-, Elektrotechnik und Leitwarte). Sie sind zu jedem Zeitpunkt für die Sicherheit der Bereiche und für alle Personen verantwortlich, denen sie Zutritt gewähren. Generalberechtigte erhalten ihre Zutrittsberechtigung anhand ihres Sicherheitstokens.

Eine **Teilberechtigung** erhalten Personen, die Zutritt zu Teilbereichen der Datacenter benötigen. Zu diesen zählen insbesondere Beschäftigte der Bereiche und Fakultäten. Sie sind zu jedem Zeitpunkt für die Sicherheit des Bereichs und für alle Personen verantwortlich, denen sie Zutritt gewähren. Teilberechtigte erhalten ihre Zutrittsberechtigung anhand ihres Sicherheitstokens.

Einen **begleiteten Zutritt** („Gastzutritt“) zu den Datacentern erhalten Personen nur in Begleitung einer Person mit General- oder teilberechtigtem Zutritt. Eine Person mit begleitetem Zutritt hat nicht das Recht, anderen Personen den Zutritt zu den Datacentern zu gewähren. Sie hat sich zu jedem Zeitpunkt an die Anweisungen der Person mit berechtigtem Zutritt zu halten und den Bereich auf Aufforderung zu verlassen.

Der oder die Verwalter/in des Zutrittskontrollsystems prüft regelmäßig, jedoch mindestens einmal pro Jahr, die korrekte Vergabe der Zutrittsberechtigungen für die Datacenter. Das Ergebnis der Prüfung wird dem oder der IT-Sicherheitsbeauftragten zusammen mit einer aktualisierten Liste der Zutrittsberechtigungen mitgeteilt.

Zugangsberechtigte Einrichtungen werden auf Antrag durch den oder die Verwalter/in des Zutrittskontrollsystems über die vergebenen Zutrittsberechtigungen für ihren Zutrittsbereich informiert.

2.4 Türen

Die Türen der Datacenter sind zu jedem Zeitpunkt geschlossen und nur für eine notwendige Zeitspanne geöffnet zu halten um beispielsweise:

- autorisierten Zutritt und Ausgang von Personen zu gestatten.
- Material, überwacht durch Personen mit Zutrittsberechtigung in die Datacenter zu befördern.
- im Falle eines Klimadefekts für ausreichende Luftzirkulation in die Datacenter zu sorgen. In diesem Fall muss der Ein- und Ausgang durch Beschäftigte mit Zutrittsberechtigung kontrolliert werden.

3. Organisatorische Maßnahmen

Das HRZ stellt sicher, dass Brandschutzübungen in ausreichendem Maß geplant und durchgeführt werden.

Wartungsarbeiten und –zeiten werden den betroffenen Nutzern der Datacenter rechtzeitig bekanntgegeben. Störungen des Betriebs bzw. der Infrastruktur der Datacenter werden durch den Leiter des HRZ bzw. die HRZ Anwenderberatung umgehend an die betroffenen Nutzer kommuniziert.

Die Einhaltung dieser Richtlinie wird regelmäßig, jedoch mindestens einmal pro Jahr durch den oder die IT-Sicherheitsbeauftragte/n geprüft.

4. Behandlung von Ausnahmen

Ausnahmen von den Regelungen dieser Richtlinie sind nur bei Gefahr in Verzug wie bspw. Feuer, medizinische Notfälle etc. gestattet.

Die Verletzung dieser Richtlinie ist der HRZ Anwenderberatung, Durchwahl 2398, umgehend mitzuteilen. Dieser informiert umgehend den Leiter des HRZ und den oder die IT-Sicherheitsbeauftragte/n.

Jeder Versuch, die Datacenter gewaltsam oder unautorisiert zu betreten, ist dem Sicherheitsdienst, Durchwahl 3277 umgehend mitzuteilen.

5. Ansprechpersonen

Bereich	Durchwahl	Ansprechfall
Anwenderberatung HRZ	2398	Wartungsarbeiten Systeme, außergewöhnliche Vorkommnisse, Verstoß gegen Richtlinie, Notfall
Zentrale Leitwarte	7777	Wartungsarbeiten Infrastruktur, Notfall
Sicherheitsdienst	3277	Gewaltsamer Zutritt, Einbruch

6. Durchsetzung, Eskalation und Revision

Der oder die IT-Sicherheitsbeauftragte trägt die Verantwortung für die Durchsetzung dieser Richtlinie. Regelungen dieser Richtlinie, die von betroffenen Personen oder Bereichen nicht einvernehmlich umgesetzt werden, können an den oder die CIO-IT der Universität eskaliert werden.

Diese Richtlinie wird regelmäßig, jedoch mindestens einmal pro Jahr, durch den oder die IT-Sicherheitsbeauftragte/n auf Ihre Aktualität und Konformität mit den IT-Sicherheitsregelungen der Universität Bielefeld überprüft.

7. Benutzungsrichtlinie für die Datacenter

Die Benutzungsrichtlinie formulieren als Teil der „IT-Sicherheitsrichtlinie für Datacenter“ konkrete Regeln bei der Nutzung der Datacenter. Die Benutzungsrichtlinien sind gut sichtbar in den Datacentern auszuhängen.

- Das Mitnehmen von Speisen und Getränken in die Datacenter ist verboten.
- Verpackungsmaterial, CDs, Reinigungsmittel und andere sicherheitsgefährdende Materialien dürfen nicht in den Datacentern gelagert werden.
- Alle Verpackungsmaterialien müssen nach dem Entpacken der Hardware sofort aus den Datacentern entfernt werden.
- Das bearbeiten jeglichen Materials (Zerspanung, Bohren, Schneiden etc.) ist in den Datacentern untersagt.
- Beschäftigte dürfen ausschließlich Zutritt zu den Sicherheits-Bereichen und Server-Schränken der Datacenter haben, für die eine Zutrittsnotwendigkeit besteht.
- Arbeiten von Personen an der Infrastruktur und den Systemen der Datacenter, sind dem HRZ bzw. der zentralen Leitwarte rechtzeitig vor Beginn mitzuteilen.
- Es ist ausschließlich autorisierten Beschäftigten gestattet, Decken und Zwischenböden zu entfernen bzw. diese zu betreten.
- Gästen ist der Aufenthalt in den Datacentern nur in Begleitung von Zutrittsberechtigten gestattet. Diese tragen die Verantwortung für die Gäste.
- Die Sicherheit der Datacenter muss zu jedem Zeitpunkt gewährleistet sein. Alle Zutrittsberechtigten sind gehalten, umgehend die HRZ Anwenderberatung (-2398) zu informieren, wenn Personen die Sicherheit gefährden oder Funktionalität stören.
- Außergewöhnliche Vorkommnisse, die die Datacenter betreffen, sind zu dokumentieren und der HRZ Anwenderberatung umgehend mitzuteilen. Diese informiert den Leiter des HRZ. Bei einem Notfall sind die zentrale Leitwarte (-7777) und die HRZ Anwenderberatung sofort zu alarmieren (-2398 und hrz-hotline@uni-bielefeld.de). Beachten Sie die ausgehängten Notfall- und Alarmpläne.