

## Sicherheitshinweise für Administratoren im ZDF

Stand: Mai 2008



## INHALTSVERZEICHNIS

<b>1</b>	<b>EINLEITUNG .....</b>	<b>3</b>
1.1	VERSIONSHISTORIE .....	3
1.2	ZIELSETZUNG .....	3
1.3	ADRESSATENKREIS.....	3
1.4	GÜLTIGKEIT .....	3
<b>2</b>	<b>VERANTWORTUNGSBEREICH.....</b>	<b>4</b>
<b>3</b>	<b>VERWALTUNG DER IT-DIENSTE .....</b>	<b>4</b>
3.1	KONFIGURATION DER IT-DIENSTE .....	4
3.2	WARTUNG.....	5
<b>4</b>	<b>ÜBERPRÜFUNG .....</b>	<b>5</b>
<b>5</b>	<b>ZUGANGS- UND ZUGRIFFSKONTROLLE.....</b>	<b>5</b>
5.1	ALLGEMEINES .....	5
5.2	PASSWORT-REGELUNGEN .....	5
<b>6</b>	<b>NOTFALLVORSORGE.....</b>	<b>6</b>
6.1	VIRENSCHUTZ .....	6
6.2	SICHERHEITSUPDATES .....	6
6.3	DATENSICHERUNG .....	6
<b>7</b>	<b>VERHALTEN BEI EINGETRETENEN STÖRUNGEN.....</b>	<b>6</b>
<b>8</b>	<b>HINWEIS FÜR EXTERNE ADMINISTRATOREN .....</b>	<b>7</b>

## 1 Einleitung

### 1.1 Versionshistorie

Stand		Verfasser
Februar	2006	Uwe Metzroth
Mai	2008	Claus Bayer

### 1.2 Zielsetzung

Durch den zunehmenden Einsatz und die daraus resultierende Abhängigkeit von der IT können Bedrohungen für das ZDF entstehen. Neben dem Verlust der Vertraulichkeit, Verfügbarkeit und Integrität personenbezogener, vertraulicher und weiterer sensibler Informationen durch IT-Fehlfunktionen und durch menschliches Fehlverhalten (bewusst oder unbewusst), kann das ganze System Ziel von Angriffen sein (von innen und außen). Um einen geordneten Betrieb von Informations- und Kommunikationssystemen zu gewährleisten, ist der Einsatz von Administratoren erforderlich. Dieser Personenkreis verfügt über tiefgehende Kenntnisse und hohe Berechtigungs-Accounts der Ihnen anvertrauten IT-Systeme. Die nachfolgenden Sicherheitshinweise dienen gleichermaßen dem Schutz der betreuten IT-Systeme wie auch den damit befassten Administratoren.

Diese Sicherheitshinweise basieren auf den Vorgaben des IT-Grundschutzhandbuchs des BSI (Bundesamt für Sicherheit in der Informationstechnologie).

### 1.3 Adressatenkreis

- IT-Administratoren im ZDF oder Personen mit administrativen Aufgaben im Bereich der IT
- IT-Sicherheitsverantwortliche im IT-Betrieb des ZDF
- Externe Vertragspartner des ZDF, welche mit administrativen Aufgaben im IT-Umfeld des ZDF beauftragt werden

### 1.4 Gültigkeit

Die „Sicherheitshinweise für Administratoren“ werden durch die „Regelung für die Administration der informationstechnischen Systeme im ZDF“ vom 13.06.2005 in Kraft gesetzt und sind bis zum Widerruf derselbigen uneingeschränkt gültig.



## 2 Verantwortungsbereich

Der Administrator ist innerhalb seines ihm zugewiesenen Bereichs dafür verantwortlich, dass durch wirksame Maßnahmen die Ziele der IT-Sicherheit realisiert werden und ihre Einhaltung kontrolliert werden kann.

Dabei sind neben geltenden, einschlägigen Gesetzen und Vorschriften ZDF interne Richtlinien zu befolgen und technisch durch den Administrator zu unterstützen bzw. zu ermöglichen.

Insbesondere sind die IT-relevanten Vorschriften, Richtlinien, Merkblätter, Hinweise zu beachten, welche im Bereich „IT-Sicherheit“ im Intranet des ZDF (ZDF.Inside) aufgeführt werden:

**<http://inside.zdf.de/default.aspx?id=2278>**

Zur Verbesserung der IT-Sicherheit hat ein Administrator mit dem IT-Sicherheitsbeauftragten zu kooperieren. Darüber hinaus hat er sich regelmäßig in dem ZDF-weit zur Verfügung gestellten IT-Sicherheitsinformationsdienst über sicherheitsrelevante Patches, Updates oder sonstige Anleitungen zur Behebung von Sicherheitslücken zu informieren.

IT-Benutzer sind bei Ihrer täglichen Arbeit an IT-Diensten und der damit verbundenen Umsetzung von IT-Sicherheitsmaßnahmen zu unterstützen.

Jeder Administrator hat einen Vertreter einzuweisen und diesen auch laufend zu informieren. Dokumentationen sind so zu gestalten, dass der Vertreter mit ihrer Hilfe seine Aufgaben wahrnehmen kann.

Der Administrator hat bei der Erstellung von Sicherheitskonzepten (z. B. Administratoren, Virenschutz- oder Notfallkonzept) mitzuwirken.

## 3 Verwaltung der IT-Dienste

### 3.1 Konfiguration der IT-Dienste

Vor dem Einsatz ist jegliche Soft- und Hardware in einer geeigneten Testumgebung zu testen.

Es sind im Einzelfall Test- und Freigabeverfahren zu erstellen und zu dokumentieren.

Soft- und Hardware sind durch den Administrator möglichst so zu konfigurieren, dass ohne weiteres Zutun des Benutzers optimale Sicherheit erreicht werden kann. Es sind Sicherheitsprodukte einzusetzen, welche dem jeweiligen System entsprechend notwendigen Sicherheitsstandart genügen.

Default-Einstellungen des Herstellers sind zu prüfen und eventuell zu ändern.

Die Nutzung aller nicht ausdrücklich erlaubten Dienste ist technisch zu unterdrücken. Dienste und Berechtigungen, die nicht oder nicht mehr benötigt werden, sind durch den Administrator zu deaktivieren (Härten des Systems).

Die Sicherheitssysteme sind so zu konfigurieren und zu administrieren, dass sie den Sicherheitsbedürfnissen des ZDF gerecht werden. Hier sind insbesondere die "Regelungen für die Administratoren der informationstechnischen Systeme des ZDF" zu beachten.

Elektronische Datenträger mit vertraulichen Informationen, die nicht weiter benötigt werden, sind vor der Entsorgung sicher zu löschen. Bei der Aussonderung von IT-Systemen ist ebenfalls darauf zu achten, dass keine vertraulichen Informationen mehr zugänglich sind.

### **3.2 Wartung**

Der Administrator ist dafür verantwortlich, dass die Informationsverarbeitung möglichst störungsfrei abläuft. Hard- und Softwarekomponenten sind daher ordnungsgemäß zu warten. Die Wartungs- und Reparaturarbeiten sind – sofern möglich – außerhalb der produktiven Nutzung durchzuführen, wenn diese zu Beeinträchtigungen des laufenden Betriebs führen können. Ansonsten sind die Benutzer vorab unter Berücksichtigung einer angemessenen Vorlaufzeit und durch einen möglichst detaillierten Zeitplan zu informieren.

Die mit Pflege und Wartung verbundenen Maßnahmen an Diensten mit sensiblen Informationen und Systemen sind nach Art, Inhalt und Zeitpunkt zu protokollieren.

Bei Arbeiten, ist nach Möglichkeit das Vier-Augen-Prinzip anzuwenden.

Wird Hardware außer Haus gegeben, sind – sofern möglich – alle sensiblen Informationen, die sich auf Datenträgern befinden, vorher sicher zu löschen. Die Übergabe bzw. der Transport ist sicher zu gestalten.

## **4 Überprüfung**

Alle Systemeinstellungen und Sicherheitsmaßnahmen sind so zu dokumentieren, dass sie für den Vertreter und andere fachkundige Dritte verständlich sind.

Es ist eine regelmäßige Kontrolle der Funktionalität der IT-Dienste, der IT-Sicherheit und der Einhaltung der Richtlinien durchzuführen.

## **5 Zugangs- und Zugriffskontrolle**

### **5.1 Allgemeines**

Die Zugangs- und Zugriffsrechte sind vom Administrator einzurichten, zu dokumentieren und vor Manipulationen zu schützen.

Der Administrator hat seiner Rolle angepasste Zugangsrechte zu nutzen (Trennung zwischen Administratoren- und Benutzerrechten). Administrative Berechtigungen dürfen ausschließlich zur Durchführung administrativer Tätigkeiten benutzt werden.

### **5.2 Passwort-Regelungen**

Voreingestellte Passwörter des Herstellers sind unverzüglich zu ändern.

#### *(1) Administratoren-Passwort*

Die Passwort-Regeln der IT-Benutzer gelten für den Administrator gleichermaßen (siehe Dokument „Regelungen für die Administratoren der informationstechnischen Systeme des ZDF“).

Die Administrator-Passwörter sind in regelmäßigen Abständen zu wechseln.

## (2) Benutzer-Passwort

Der Administrator hat die Passwort-Regeln der IT-Benutzer (siehe Dokument "Regelungen für die Administratoren der informationstechnischen Systeme des ZDF") technisch umzusetzen und deren Einhaltung technisch zu unterstützen.

Nach Ablauf der Gültigkeit des Passwortes ist der Nutzer vom System automatisch zu sperren. Das Entsperren darf nur von einem Administrator durchgeführt werden.

Die Passwörter sind innerhalb der Systeme zugriffssicher zu speichern.

Vorläufige Passwörter sind den Benutzern auf sichere Art zu übergeben.

## 6 Notfallvorsorge

### 6.1 Virenschutz

Es ist ein Viren-Schutzprogramm zu installieren. Updates sind entsprechend ihrer Notwendigkeit durchzuführen und die Viren-Signaturen aktuell zu halten. Können solche Programme aus berechtigten Gründen (betriebliche Notwendigkeit) nicht installiert werden, sind geeignete Schutzmassnahmen zu ergreifen (siehe "Regelungen für die Administratoren der informationstechnischen Systeme des ZDF" Teil B – spezifische Regelungen).

### 6.2 Sicherheitsupdates

Um potentiellen Angreifern eine möglichst geringe Angriffsfläche zu bieten, sind bekannt gewordene Sicherheitslücken umgehend durch entsprechend verifizierte Patches, Updates oder Workarounds des jeweiligen Herstellers zu schließen. Um eine übergreifende und einheitliche Informationsbasis zu bieten, sind alle Administratoren des ZDF dazu verpflichtet sich in dem zur Verfügung gestellten IT-Sicherheitsinformationssystem zu informieren, bzw. alarmieren zu lassen.

Bekannte gewordene Sicherheitslücken sind entsprechend ihrer Dringlichkeit zeitnah zu schließen und die Wirksamkeit der Maßnahmen anschließend zu überprüfen.

Zugang zu dem IT-Sicherheitsinformationsdienst erhalten die Administratoren durch Ihren IT-Sicherheitsmanager oder den IT-Sicherheitsbeauftragten.

### 6.3 Datensicherung

Es sind regelmäßige Datensicherungen durchzuführen. Dies hat anhand eines Datensicherungsplans zu geschehen.

## 7 Verhalten bei eingetretenen Störungen

Der Administrator hat bei Verlust der Netz- oder Systemintegrität schnellstmöglich diese Störungen zu beseitigen und den IT- Sicherheitsbeauftragten zu informieren.

Die Ursachen dieser Störungen sind anhand der erstellten Protokolle zu analysieren und Verbesserungen zu erarbeiten.



## **8 Hinweis für externe Administratoren**

Die hier dokumentierten Hinweise und Regelungen sind auch für Administratoren, welche über externe Dienstleister im ZDF eingesetzt werden, uneingeschränkt gültig. Darüber hinaus ist externen Administratoren über die jeweiligen vertraglichen Regelungen jegliche private Nutzung der vom ZDF zur Verfügung gestellten Arbeitsmittel (PC, Notebook, Handy, Internetzugang, Email, ...) untersagt. Das in der „Administratorenrichtlinie“ eingeräumte Kontrollrecht des Datenschützers und IT-Sicherheitsbeauftragten bleibt davon unbenommen.

Der IT-Sicherheitsbeauftragte