Dienstanweisung zur Informationssicherheit bei der IT-Administration (DA IT-Administration)

Vom 06.03.2025

1. Gegenstand 2

2. Geltungsbereich 2

3. Allgemeines 2

3.1 Verantwortungsbereich 2
3.2 Vertretung 3
3.3 Mitwirkung 3
3.4 Dokumentation 3
3.5 Datenschutz 4

4. Verwaltung der IT-Systeme, Anwendungen und Dienste 4

4.1 Generelle Vorgaben 4
4.2 Schutz der Anwendungen und Dienste 4
4.3 Sicherung der Administrationsarbeiten 5
4.4 Wartung und Pflege 5
4.5 Protokollierung 6
4.6 Entsorgung von schützenswerten Betriebsmitteln 6
4.7 Authentisierung 6

5. Passwortregeln für Administrationskennungen 8

6. IT-Schwachstellen 9

7. Zugangs- und Zugriffskontrolle 9

7.1 Zugang zu IT-Bereichen 9
7.2 Zugriffsregelungen 10

8. Inkrafttreten 11

1. Gegenstand

Ziel dieser Dienstanweisung ist es, die bei der Administration von IT Systemen, Anwendungen und Diensten bestehenden Gefahren und Risiken mittels Umsetzung der vorgegebenen Sicherheitsanforderungen nach dem jeweils aktuellen Stand der Technik zu minimieren, sowie die für die Einhaltung datenschutzrechtlicher Vorschriften erforderlichen Maßnahmen in den Fällen, in denen personenbezogene Daten verarbeitet werden, zu gewährleisten.

2. Geltungsbereich

Diese Dienstanweisung gilt für alle festangestellten Beschäftigten, die vom WDR betriebene IT-Systeme, Dienste oder Anwendungen administrieren. Diese werden im Folgenden IT administrierende Personen (IT-Administratoren:innen) genannt. Sofern der WDR im Bereich der IT-Administration mit externen Dienstleistern zusammenarbeitet, ist durch die anfordernde Stelle zu veranlassen, dass die externen Dienstleister vertraglich zur Einhaltung der Anforderungen aus dieser Dienstanweisung sowie im Falle von Verstößen zu Vertragsstrafen verpflichtet werden.

Können Anforderungen in dieser Dienstanweisung aus technischen oder betrieblichen Gründen nicht umgesetzt werden, sollten mindesten gleichwertige alternative Schutzmaßnamen zur Absicherung eingesetzt und dokumentiert werden. Ausnahmen sind zu begründen, die damit verbundenen Risiken zu dokumentieren und von der Leitung der jeweils zuständigen Direktion zu genehmigen. Die begründeten Abweichungen sind in der zugehörigen Betriebsdokumentation zu dokumentieren. Die beauftragte Person für Informationssicherheit im WDR (Informationssicherheitsbeauftragte:r) und die beauftragte Person für betrieblichen Datenschutz im WDR (Datenschutzbeauftragte:r) sind zu informieren.

3. Allgemeines

3.1 Verantwortungsbereich

IT administrierende Personen werden von den Personen mit Informationstreuhänderschaft (Informationstreuhänder:innen) (siehe Ziffer 2.5 der Informationssicherheitsordnung) benannt,

Sie sind für den sicheren Betrieb und die Sicherheitsbelange der von ihnen betreuten IT-Systeme, Anwendungen und Dienste zuständig und verantwortlich für die Umsetzung der nachfolgenden Sicherheitsanforderungen nach dem jeweils aktuellen Stand der Technik. Neben dieser Dienstanweisung sind ebenfalls die weiteren Vorgaben und Standards zur Informationssicherheit gemäß Anlage 2 der Informationssicherheitsordnung des WDR zu beachten.

Für jedes IT-System, jede Anwendung und jeden Dienst im Westdeutschen Rundfunk muss eine IT administrierende Person benannt sein.

3.2 Vertretung

IT administrierende Personen müssen eine Vertretung einweisen. Sie müssen dafür Sorge tragen, dass der Vertretung die zur Ausübung ihrer Vertretungsaufgabe notwendigen Informationen vorliegen.

3.3 Mitwirkung

Zur Aufrechterhaltung der Informationssicherheit besteht eine wesentliche Aufgabe der IT administrierende Personen in der Kooperation mit den Bereichs-Informationssicherheitsbeauftragten beziehungsweise der beauftragte Person für Informationssicherheit im WDR und gegebenenfalls der beauftragten Person für betrieblichen Datenschutz im WDR. Hierzu gehört auch, bei der Erstellung von Sicherheitsstandards mitzuwirken.

Personen, die IT des WDR anwenden (IT-Anwender:innen), sind bei der Nutzung von IT-Diensten und der Umsetzung von Sicherheitsmaßnahmen zu unterstützen. IT administrierende Personen haben als Personen, die IT anwenden, auch die DA IT-Anwender:innen zu beachten.

3.4 Dokumentation

Alle Systemeinstellungen und Sicherheitsmaßnahmen sind so zu dokumentieren, dass sie für die Vertretung und andere fachkundige Dritte verständlich sind und die Vertretung mit ihrer Hilfe ihre Aufgaben wahrnehmen kann. Die Betriebsdokumentation ist stets aktuell zu halten.

Fehler und Probleme, die IT-Dienste betreffen und Administrationstätigkeiten sind, sind von den IT administrierende Personen zu dokumentieren. Hierzu ist das im jeweiligen Bereich eingesetzte Werkzeug (zum Beispiel Ticketsystem) zu nutzen.

Alle vergebenen Berechtigungen und IT anwendenden Personen und Personengruppen sind im Rahmen der oben genannten Betriebsdokumentation zu dokumentieren und diese vor Manipulation zu schützen.

3.5 Datenschutz

Personenbezogene Daten, die IT administrierenden Personen im Rahmen ihrer Aufgabenerfüllung zugänglich sind, dürfen von diesen nur zu dem zur jeweiligen Aufgabenerfüllung gehörenden Zweck verarbeitet werden. Näheres regelt die DA Datenschutz.

4. Verwaltung der IT-Systeme, Anwendungen und Dienste

4.1 Generelle Vorgaben

Soft- und Hardware sind durch die IT administrierenden Personen so zu konfigurieren, dass ohne weiteres Zutun der IT anwendenden Personeneine Mindestsicherheit erreicht werden kann:

- Default-Einstellungen der Herstellerfirma sind zu prüfen und – soweit erforderlich – zu ändern. Für wiederkehrende Installations- oder Einrichtungsvorgänge sind die durchzuführenden Aktivitäten zur Änderung der Default-Einstellungen in einer Checkliste zu dokumentieren.

- Vor dem Einsatz sind die Soft- und Hardware nach Möglichkeit zu testen, hierbei sind die Test- und Freigabeverfahren zu beachten.

- Die Nutzung aller nicht ausdrücklich erlaubten Dienste ist, soweit möglich, technisch zu unterdrücken. Dienste und Berechtigungen, die nicht oder nicht mehr benötigt werden, sind zu deaktivieren oder zu löschen.

4.2 Schutz der Anwendungen und Dienste

Zum Umgang mit Diensten und Anwendungen ist Folgendes zu beachten:

- Originaldatenträger von Software sind vor unbefugtem Zugriff zu schützen und zentral zu hinterlegen. Eine Weitergabe darf nur an berechtigte Personen erfolgen, Installationen sollten über Software-Verteilmechanismen erfolgen.

- Beim Einsatz von Diensten und Anwendungen sind die jeweiligen lizenzrechtlichen Bestimmungen einzuhalten. Es dürfen ausschließlich Anwendungen und Dienste verwendet werden, deren Lizenzbestimmungen vorab geprüft und deren Nutzung von dem jeweils zuständigen IT-Bereich freigegeben wurden. Die vorhandenen Installationen sowie die Nutzung von Diensten und Anwendungen sind zu dokumentieren.

4.3 Sicherung der Administrationsarbeiten

Alle Administrationsarbeiten und -zugriffe sind vor unbefugter Nutzung beziehungsweise unbefugtem Mitverfolgen zu schützen. Hierfür sind

- sämtliche Verbindung für den administrativen Zugriff auf IT-Systeme, Anwendungen und Dienste zu verschlüsseln (zum Beispiel ssh) und

- dedizierte, sichere Administrationsnetze zu verwenden (zum Beispiel VLANs)

oder

- mindestens gleichwertige alternative Schutzmaßnahmen zu ergreifen und diese zu dokumentieren.

4.4 Wartung und Pflege

Folgende Anforderungen gelten für Wartungs- und Pflegearbeiten:

- IT administrierende Personen sind dafür verantwortlich, dass die Informationsverarbeitung möglichst störungsfrei abläuft. Hard- und Softwarekomponenten sind daher ordnungsgemäß und nach den sicherheitsrelevanten Vorgaben der Herstellerfirma zu warten.

- Die Wartungs- und Reparaturarbeiten sind – sofern möglich oder bei Beeinträchtigung des laufenden Betriebs – in den vereinbarten Wartungsfenstern durchzuführen. Die jeweilige Supportorganisation ist hierüber in Kenntnis zu setzen und informiert die IT anwendenden Personenüber anstehende Wartungs- und Reparaturarbeiten.

- Die mit Pflege und Wartung verbundenen Maßnahmen sind nach Art, Inhalt und Zeitpunkt zu dokumentieren.

- Bei Arbeiten an Diensten mit sensiblen Informationen ist nach Möglichkeit das Vier-Augen-Prinzip anzuwenden.

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

- Sofern möglich, sind Fernwartungszugänge ausschließlich für den Wartungsvorgang und nach Absprache mit dem Wartungspersonal zu aktivieren. Unmittelbar nach dem Wartungsvorgang und bei Nichtgebrauch sind die Wartungszugänge zu deaktivieren.

- Lokale Wartungsarbeiten sind revisionssicher zu dokumentieren (beispielsweise Datum, Uhrzeit, Wartungspersonal, Beauftragende Person, Grund der Wartung, vorgenommene Änderungen).

- Beim Einsatz von externem Wartungspersonal sowie bei Fernwartung sind die DA IT-Wartung und die jeweils geltenden Bestimmungen zum Datenschutz zu beachten.

4.5 Protokollierung

Folgende Angaben zur Systemnutzung sind, soweit technisch möglich, automatisiert zu protokollieren und an das zentrale Log-Management des WDR zu übertragen:

- Berechtigte Zugriffe (Anmeldekennungen, Zeitpunkt der An- und Abmeldung, Ursprung der Netzwerkverbindung)

- Privilegierte Aktionen (Bspw. Benutzung Super-User, Systemstart/-stopp, Anschluss/Entfernung von Ein-/Ausgabegeräten)

- Unberechtigte Zugriffsversuche

- Ggf. sind weiter Log-Daten mit dem zentralen Logmanagement des WDR abzustimmen.

Bei der Protokollierung und Auswertung der Log-Daten ist Ziffer 4.4 der Informationssicherheitsordnung zu beachten.

4.6 Entsorgung von schützenswerten Betriebsmitteln

Informationen können durch unbedachte Entsorgung oder Wiederverwendung von Geräten oder Unterlagen unbefugten Dritten bekannt werden. Deshalb ist Folgendes zu beachten:

- Speichermedien mit sensiblen Informationen sind vor der Entsorgung oder sonstiger Entfernung aus dem WDR auf sichere Weise zu löschen;

- falls dies nicht möglich oder zweckmäßig ist, sind sie physikalisch zu zerstören.

4.7 Authentisierung

Folgende Anforderungen sind für eine sichere Authentisierung an IT-Systeme, Anwendungen und Dienste zu erfüllen und - soweit möglich - technisch sicherzustellen. Sofern einzelne Anforderungen technisch nicht umgesetzt werden können, sind gegebenenfalls organisatorische Regelungen einzusetzen und die Mitarbeitenden hinsichtlich der Regelungsinhalte in Kenntnis zu setzten und gegebenenfalls zu schulen.

- Voreingestellte Authentisierungsinformationen (z. B. Standard- oder Initialkennungen und Passwörter des Herstellers bei Auslieferung von IT-Systemen) müssen noch vor der Inbetriebnahme des IT-Systems in den Produktivbetrieb geändert werden.

- Es sind vorrangig zentrale Authentifizierungsdienste zu verwenden.

- Für Fernzugriffe auf Ressourcen und IT-Systeme des WDR aus externen oder öffentlichen Netzen sowie für Zugriffe auf cloudbasierte Ressourcen des WDR in externen oder öffentlichen Netzen ist eine Multi-Faktor-Authentisierung einzusetzen.

- Für Konten mit erhöhten Privilegien sowie für Administrationskonten ist grundsätzlich eine Multi-Faktor-Authentisierung zu verwenden.

- Sofern technisch möglich, müssen bei einer Multi-Faktor-Authentisierung (MFA) „phishing-resistente“ MFA-Verfahren zur Anwendung kommen. Hierbei ist zu beachten, dass die Sicherheit des gewählten Verfahrens bei allen Arten von Anmeldeszenarien auf allen Gerätetypen gewährleistet ist. Zudem sind unsichere Faktoren (bspw. Telefon, SMS, E-Mail) durch sichere Authentisierungsfaktoren nach dem Stand der Technik zu ersetzen.

- Authentisierungsinformationen müssen verschlüsselt gespeichert und übertragen werden. Ihre Verarbeitung ist technisch so abzusichern, dass eine unberechtigte Kenntnisnahme (z.B. Auslesen) ausgeschlossen bzw. unter nachvollziehbarer Risikobewertung und -behandlung wesentlich erschwert ist.

- Es sind geeignete Maßnahmen einzurichten, um ein manuelles bzw. automatisiertes Ausprobieren von Passwortkombinationen oder anderen Authentisierungsinformationen zu unterbinden (z.B. Begrenzung von oder Zeitverzögerung nach nicht erfolgreichen Anmeldeversuchen, Schutz vor unberechtigtem Zugriff auf Passwortdateien).

- Zur Identifizierung einer für die Nutzung eines IT-Systems berechtigten Person sind personenbezogene Konten einzurichten. Das jeweilige Konto muss eindeutig einer natürlichen Person zugeordnet sein.

- Die Vergabe und das Einrichten von Funktions- bzw. Gruppenkonten („Nicht-personalisierten Konten“) sind nur in Ausnahmefällen zulässig, wenn eine Aufgabe mittels eines personenbezogenen Kontos nicht durchgeführt werden kann oder wenn eine nachvollziehbare Risikobewertung und –behandlung vorliegt. Sofern ein Funktions- bzw. Gruppenkonto zum Einsatz kommt, muss eine eindeutige Zuordnung der nutzenden Person auf anderem Wege (z.B. Dienstplan, Zuordnungstabelle) gewährleistet werden. Es ist sicherzustellen, dass für jedes Funktions- bzw. Gruppenkonto eine verantwortliche Person festgelegt ist.

- Technische Konten (z.B. wenn sich ein Server dauerhaft mit einem Netzlaufwerk oder einer Datenbank verbindet) dürfen nur bei zwingenden technischen Gründen eingerichtet werden. Eine interaktive Anmeldung ist technisch zu unterbinden. Für jede Schnittstelle bzw. jede technische Anwendung ist nach Möglichkeit ein eigenes technisches Konto anzulegen. Es ist sicherzustellen, dass für jedes technische Konto eine verantwortliche Person festgelegt ist.

- Es ist technisch sicherzustellen, dass ausschließlich komplexe Passwörter verwendet werden. Insbesondere Trivialpasswörter (z.B. „password“), gängige Zeichenketten und Tastaturmuster („123456“, „asdf“) sowie Passwörter, die nur unwesentlich von den vorherigen Passwörtern abweichen, dürfen nicht verwendet werden.

- Kennungen mit Standardprivilegien müssen eine Passwortlänge von mindestens 10 Zeichen haben. Die Passworte sind alle 365 Tage zu ändern.

- Kennungen mit erhöhten Privilegien müssen eine Passwortlänge von mindestens 15 Zeichen haben. Bei Einsatz einer Multi-Faktor-Authentisierung kann eine reduzierte Passwortlänge von 10 Zeichen zum Einsatz kommen. Die Passworte sind alle 365 Tage zu ändern.

- Kennungen von technischen Konten müssen eine Passwortlänge von mindestens 25 Zeichen haben.

- Das Zurücksetzen von Authentisierungsinformationen darf nur erfolgen, wenn die Identität der nutzenden Person glaubhaft überprüft worden ist. Dieser Vorgang kann durch einen Passwort-Self-Service unterstützt und realisiert werden.

- Wird für eine IT anwendende Person ein vorläufiges Passwort vergeben, so darf dieses nur der betreffenden Person bekannt gegeben werden. Bei der ersten Anmeldung ist ein Passwortwechsel erforderlich.

- Nach Ablauf der Gültigkeit ihres Passwortes sind IT anwendende Personen vom System – soweit möglich – automatisch zu sperren. Das Entsperren kann nur von IT administrierenden Personen durchgeführt werden.

IT administrierenden Personenhaben die Passwortregeln für Anwenderinnen und Anwender (siehe DA IT-Anwender:innen) technisch umzusetzen und deren Einhaltung technisch zu unterstützen.

5. Passwortregeln für Administrationskennungen

Folgende Anforderungen an die Qualität und den Gebrauch von Administrationspasswörtern bestehen:

- Administrationspasswörter müssen eine Mindestlänge von 15 Zeichen haben. Bei Einsatz einer Multi-Faktor-Authentisierung kann eine reduzierte Passwortlänge von mindestens 10 Zeichen verwendet werden.

- Administrationspasswörter dürfen nicht leicht zu erraten sein und müssen Ziffern, Klein- und Großbuchstaben sowie Sonderzeichen enthalten.

- Sie sind spätestens nach 365 Tagen zu wechseln.
- Passwörter sind geheim zu halten und müssen sicher verwahrt werden.
- Sofern Administrationspasswörter für den Vertretungsfall benötigt werden, sind diese revisionssicher und vor unautorisiertem Zugriff geschützt zu hinterlegen.
- Bei einer Kompromittierung oder dem Verdacht einer Kompromittierung von Administrationspasswörtern ist dies als Informationssicherheitsvorfall zu behandeln. Die betroffenen Passwörter müssen unverzüglich geändert werden.

6. IT-Schwachstellen

Zur Vermeidung von Störungen und Sicherheitsvorfällen gilt:

- IT administrierende Personenmüssen sich regelmäßig innerhalb ihres Aufgabengebietes über sicherheitsrelevante Patches, Updates oder sonstige Informationen zu IT-Schwachstellen und Sicherheitslücken informieren und entsprechende Handlungsempfehlungen unverzüglich umsetzen.
- Sie müssen Entwicklungen in dem verantworteten Bereich verfolgen und gegebenenfalls vor neuen informationstechnischen Sicherheitsproblemen oder Sicherheitsvorfällen warnen.

7. Zugangs- und Zugriffskontrolle

Die folgenden Abschnitte stellen – aus dem Blickwinkel der IT administrierenden Personen – Anforderungen aus der Informationssicherheitsdokumentation des WDR dar (siehe auch Leitfaden zur Informationssicherheit bei Planung und Betrieb von IT-Systemen). Die Realisierung dieser Anforderungen liegt im Verantwortungsbereich der dort angesprochenen Zielgruppe. Die Mitwirkungspflicht der IT administrierenden Personenbesteht darin, ihre Tätigkeiten nach den Vorgaben auszurichten und bei festgestellten Abweichungen die betreffenden Personen mit Informationstreuhänderschaft zu informieren.

7.1 Zugang zu IT-Bereichen

Für den physikalischen Schutz von IT-Systemen ist von IT administrierenden Personen folgendes zu beachten:

- IT-Systeme für wichtige oder sensible Geschäftsinformationen müssen in räumlich getrennten Bereichen (zum Beispiel Serverräumen) betrieben werden.

- Diese Bereiche müssen durch definierte Sicherheitsgrenzen geschützt und mit entsprechenden Sicherheitsschranken und Zutrittskontrollen versehen sein.

- Die IT-Systeme müssen physisch vor unberechtigtem Zugang, Beschädigung und Störung geschützt sein.

7.2 Zugriffsregelungen

Jede Nutzung eines IT-Systems oder einer Anwendung muss grundsätzlich über einen Anmeldeprozess initiiert werden (Ziffer 4.3 Informationssicherheitsordnung). Dieser Vorgang muss folgenden Anforderungen genügen:

- Den IT administrierenden Personen obliegt die Zugangsverwaltung einschließlich der Verwaltung der Zugriffsrechte, soweit hierfür keine Sonderregelungen bestehen. Sie müssen hierbei die von den Informationsverantwortlichen vorgegebenen Sicherheitsanforderungen (zum Beispiel Vergabe von Zugriffsrechten) berücksichtigen.

- Es sind eindeutige Nutzerkennungen zu vergeben beziehungsweise zu verwenden. Funktions- und Gruppenkennungen sind nur in Ausnahmefällen (siehe 7.2) erlaubt und müssen von den jeweiligen Informationsverantwortlichen genehmigt werden. Die Genehmigungen, sowie die festgelegten Einzelheiten zur Vergabe, Pflege, Änderung und Löschung dieser Kennungen sind zu dokumentieren.

- Zugriffsrechte sind so zu beschränken, dass die Personen nur die für die Aufgabenerfüllung notwendigen Berechtigungen erhalten. Zugriffsrechte für Personen, die nicht beim WDR angestellt sind, dürfen immer nur zeitlich befristet vergeben werden. Soweit möglich, ist dies durch technische Maßnahmen zu überwachen beziehungsweise zu automatisieren.

- Die Zugriffsrechte der IT administrierenden Personen sind mit den betreffenden Personen mit Informationstreuhänderschaft abzustimmen.

- Zugangskennungen und Zugriffsrechte sind mindestens einmal pro Jahr dahingehend zu prüfen, ob sie noch benötigt werden und gegebenenfalls zu löschen.

8. Inkrafttreten

Diese Dienstanweisung tritt zum 17.03.2025 in Kraft und ersetzt die Dienstanweisung IT-Administration vom 11.05.2022.

Köln, 06.03.2025
gez. Katrin Vernau
Intendantin