Dienstanweisung zur Informationssicherheit bei der Nutzung von IT-Anwendungen (DA IT-Anwendung)

Vom 06.03.2025

1. Gegenstand ... 2

2. Geltungsbereich ... 2

3. Regelungen ... 3

3.1 Beschaffung ... 3
3.2 Bereitstellung ... 3
3.3 Nutzung ... 3
3.4 Entsorgung ... 4
3.5 Systemzugangskontrolle ... 4
3.5.1 Einrichtung des Arbeitsplatzes ... 4
3.5.2 Anmeldekennung ... 4
3.5.3 Passwörter ... 5
3.5.4 BIOS-Passwörter ... 6
3.5.5 Informationen über die Konfiguration der IT-Umgebung ... 6
3.6 Sorgfaltspflicht ... 6
3.7 Datensicherung ... 6
3.8 Datenschutz ... 7
3.9 Datenspeicherung und Datenaustausch ... 7
3.9.1 Virenschutz ... 7
3.9.2 Mobile Datenträger ... 8
3.9.3 E-Mail / Internet ... 8
3.10 Sicherheitsfunktionen ... 9
3.11 Anwenderberatung ... 9

4. Zusatzregelungen für mobile Endgeräte ... 10

4.1 Virenschutz ... 10
4.2 Datenspeicherung ... 10
4.3 Datensicherung ... 10
4.4 Diebstahlschutz ... 11

5. Schulung ... 11

6. Inkrafttreten ... 11

1. Gegenstand

Die Arbeitsabläufe im Westdeutschen Rundfunk (WDR) sind vom Einsatz der Informationstechnik (IT) geprägt. So werden Arbeitsprozesse von Computern gesteuert und dabei Informationen digital gespeichert, elektronisch verarbeitet und in lokalen sowie öffentlichen Netzen verbreitet. Viele Aufgaben können im WDR ohne eine funktionsfähige IT nicht mehr wahrgenommen (zum Beispiel Hörfunk- und Fernsehproduktionen, Gehaltsabrechnung) oder bei einer Störung nur noch eingeschränkt erfüllt werden (zum Beispiel Sekretariatsaufgaben).

Vor diesem Hintergrund ist die informationstechnische Sicherheit als fester Bestandteil in den Arbeitsabläufen des WDR zu betrachten.

Informationssicherheit im Sinne dieser Dienstanweisung ist der Schutz von IT-Systemen (zum Beispiel Desktop-PCs, Notebooks, Server, Tablets, Smartphones, IT-basierende Produktionsmittel – siehe auch Informationssicherheitsordnung) und digitalen Informationen vor Verlust der Vertraulichkeit, Integrität und Verfügbarkeit.

Ziel dieser Dienstanweisung ist es, die bei der Nutzung von IT-Systemen bestehenden Gefahren und Risiken möglichst gering zu halten. Hierzu soll den Mitarbeiterinnen und Mitarbeitern in dieser Dienstanweisung aufgezeigt werden, an welchen Stellen sie bei der Nutzung der Informationstechnik im WDR aktiv zur Sicherheit der IT-Systeme sowie den darin abgelegten Daten beitragen können.

2. Geltungsbereich

Diese Dienstanweisung gilt für alle Beschäftigten des WDR, sofern sie IT-Systeme nutzen, die vom WDR zur Verfügung gestellt oder deren Betrieb vom WDR freigegeben wurde (IT-Anwender:innen). Dabei ist es unerheblich, ob die Systeme mit dem WDR-Netz verbunden sind. Für die Administration von IT-Systemen gilt zusätzlich die DA IT-Administration.

Sofern Externe (zum Beispiel Personen in freier Mitarbeit oder Personal von Drittfirmen) IT-Systeme des WDR nutzen, ist durch die anfordernde Stelle zu veranlassen, dass die Externen vertraglich auf die Einhaltung der Anforderungen aus dieser Dienstanweisung verpflichtet werden.

3. Regelungen

Zur Wahrung der Informationssicherheit gelten für die Nutzung von IT-Systemen im Westdeutschen Rundfunk die folgenden Regelungen.

3.1 Beschaffung

Die Beschaffung der eingesetzten Hardware erfolgt grundsätzlich über den jeweils zuständigen Supportbereich. Die Beschaffung der eingesetzten Anwendungen und Dienste erfolgt über das zentrale Software-Lizenzmanagement.

Bei Änderungen (zum Beispiel Austausch oder Wegfall eines IT-Systems oder Übergabe an eine andere Person) umgehend der zuständige Supportbereich sowie das zentrale Software-Lizenzmanagement zu informieren.

3.2 Bereitstellung

Der zuständige Supportbereich stattet die Arbeitsplätze mit IT-Systemen aus. Dies umfasst Endgeräte (zum Beispiel Desktop-PC, Notebook, Tablet-Computer) einschließlich der erforderlichen Software und Peripheriegeräte (zum Beispiel Drucker, Scanner, Speichermedien) sowie die Anbindung an das WDR-Netz.

3.3 Nutzung

An die IT-Infrastruktur (zum Beispiel Netzwerke, Server) im WDR dürfen ausschließlich IT-Systeme angeschlossen werden, deren Betrieb vom zuständigen Supportbereich freigegeben wurde. Dies gilt auch für den Anschluss von Peripheriegeräten (Regelungen zu mobilen Datenträgern siehe Ziffer 3.9.2).

Die Installation und Nutzung von Anwendungen und Diensten, die nicht durch den zuständigen IT-Betrieb freigegeben wurde, ist zum Schutz der vorhandenen IT-Systeme nicht zulässig. Alle im WDR eingesetzten Anwendungen und Dienste bedürfen einer vorherigen lizenzrechtlichen Prüfung sowie der Genehmigung des jeweils zuständigen IT-Bereichs. Das Kopieren von Software sowie die Weitergabe von Details der Programmierung sind aus lizenzrechtlichen Gründen untersagt.

Hard- und Softwarekomponenten (IT-Systeme, Datennetze, Anwendungen, Dienste, Programme oder Daten Dritter) dürfen ohne eine entsprechende Berechtigung nicht genutzt oder verändert werden. Änderungen an den Systemeinstellungen (zum Beispiel Installation, Deinstallation, Änderungen an der Konfiguration, Wartung) sind nur durch IT administrierende Personen (IT-Administratoren:innen), beziehungsweise Supportbereiche oder mit deren Zustimmung zulässig.

Erkannte oder befürchtete Informationssicherheitsvorfälle sind unmittelbar der IT-Hotline beziehungsweise dem jeweiligen Supportbereich zu melden.

Die Benutzung der IT-Systeme des Westdeutschen Rundfunks für private Zwecke ist gemäß WDR-Geschäftsordnung grundsätzlich nicht zulässig, sofern sie nicht durch andere WDR-Regelungen erlaubt ist (siehe zum Beispiel DV Internet- und E-Mail-Nutzung).

Beschäftigte sind verpflichtet, bei Austritt aus dem Unternehmen ihre privaten Daten auf den IT-Systemen des WDR zu löschen. Alle verbleibenden Daten werden als dienstlich betrachtet. Über die weitere Nutzung dieser Daten entscheidet die betreffende Führungskraft unter der Berücksichtigung datenschutzrechtlicher Vorgaben.

3.4 Entsorgung

Die Vernichtung von Datenträgern (zum Beispiel USB-Sticks, SD-Cards, CDs, DVDs, Festplatten) erfolgt durch den zuständigen Supportbereich.

Die Beschäftigten müssen bei der Rückgabe von entliehenen oder der Aussonderung von dauerhaft zugeordneten IT-Systemen dafür sorgen, dass alle lokal auf dem IT-System gespeicherten Daten gelöscht sind beziehungsweise gelöscht werden können.

3.5 Systemzugangskontrolle

3.5.1 Einrichtung des Arbeitsplatzes

Der Arbeitsplatz ist so einzurichten und zu hinterlassen, dass Unbefugten kein Zugriff auf Daten sowie Anwendungen und Dienste ermöglicht wird. Dies gilt auch bei kurzfristigem Verlassen des Arbeitsplatzes. Die hierfür zur Verfügung stehenden Schutzprogramme (zum Beispiel passwortgeschützte Bildschirmsperre) sind zu nutzen. Alternativ ist eine Abmeldung bei Nichtbenutzung durchzuführen.

Kommt es an einem Arbeitsplatz regelmäßig zu Publikumsverkehr, sind die Bildschirme und Drucker nach Möglichkeit so aufzustellen, dass Unbefugte keinen Einblick nehmen können.

Datenträger sind verschlossen und für Unbefugte unzugänglich aufzubewahren.

3.5.2 Anmeldekennung

Zum Schutz der Daten und des ordnungsgemäßen Ablaufs der IT werden die IT-Systeme im WDR mit einer Zugangskontrolle gesichert. Diese dient auch dem Schutz von personenbezogenen Daten vor unberechtigtem Zugriff. Daher ist es grundsätzlich für jedes IT-System erforderlich, dass sich alle Personen, die das System nutzen, mit einer persönlichen Kennung anmelden und so am System identifizieren.

Die Beschäftigten sind verantwortlich für die Nutzung von IT-Systemen, die unter ihrer persönlichen Anmeldekennung erfolgt. Deshalb sie darauf achten, ihre

Zugangsdaten zu schützen und ihre zugehörigen Passwörter, PINs und so weiter geheim zu halten. Persönliche Anmeldekennungen und Passwörter dürfen grundsätzlich nur von den betreffenden Personen genutzt werden. Sofern in anders nicht behebbaren Ausnahmesituationen unter einer fremden Anmeldekennung auf ein IT-System zugegriffen werden muss (zum Beispiel Sicherstellung der Arbeitskontinuität bei Krankheit), ist dies von der Leitung der jeweiligen Organisationseinheit zu genehmigen und zu dokumentieren. Die betroffene Person, deren Anmeldekennungen und Passwörter verwendet wurden, sowie die beauftragte Person für betrieblichen Datenschutz im WDR (Datenschutzbeauftragte:r) sind über den Zugriff zu informieren.

Für ausnahmsweise eingerichtete Funktionskennungen ist die jeweils beantragende Organisationseinheit verantwortlich. Sie muss für eine Nachvollziehbarkeit des Gebrauchs der Funktionskennung Sorge tragen.

Bei Anhaltspunkten, dass sich Dritte missbräuchlich einer persönlichen Anmeldekennung bedienen, müssen die betroffenen Personen, wenn möglich, umgehend ihr Passwort ändern und diesen Verdacht dem jeweiligen Supportbereich sowie der beauftragten Person für betrieblichen Datenschutz im WDR melden.

3.5.3 Passwörter

Zu jeder Anmeldekennung gehört ein Passwort. Folgende Anforderungen an die Qualität und den Gebrauch von Passwörtern bestehen:

- Passwörter müssen eine Mindestlänge von 10 Zeichen haben.
- Passwörter dürfen nicht leicht zu erraten sein und müssen Ziffern, Klein- und Großbuchstaben sowie Sonderzeichen enthalten (Beispielsweise kann das Passwort mittels eines Passwortsatzes gebildet werden, indem das Passwort aus den Anfangsbuchstaben der Worte des Passwortsatzes zusammengesetzt wird: „Maus & Elefant gehen zusammen 1 Pizza essen“ => „M&Egz1Pe“.).
- Passwörter sind spätestens nach 365 Tagen zu wechseln.
- Passwörter sind geheim zu halten und müssen sicher verwahrt werden.
- Bei einer Kompromittierung von Passworten oder dem Verdacht einer Kompromittierung sind die betroffenen Passwörter unverzüglich zu ändern und der zuständige Supportbereich darüber zu informieren.

Weitere Hinweise zum Umgang mit Passwörtern sind im Intranet-Angebot zur Informationssicherheit zu finden.

3.5.4 BIOS-Passwörter

Das BIOS ist das dem Betriebssystem vorgeschaltete Grund-Programm eines IT-Systems. Die BIOS-Einstellungen (zum Beispiel die Boot-Reihenfolge von Desktop-PCs und Notebooks) dürfen nur von IT administrierenden Personen geändert werden. Daher ist auf jedem IT-System – soweit technisch möglich – der Zugriff auf die BIOS-Einstellungen vom zuständigen Supportbereich mit einem Passwortschutz zu versehen.

3.5.5 Informationen über die Konfiguration der IT-Umgebung

Um das Risiko des unberechtigten Zugangs zu den IT-Systemen des WDR zu minimieren, ist es untersagt, unbefugten Dritten (zum Beispiel unberechtigten Personen außerhalb des WDR) Informationen zu geben, die Rückschluss auf die Konfiguration der IT-Umgebung im jeweiligen Bereich und im WDR-Netz zulassen können. Beispiele hierfür sind:

- IP-Adressen, Port-Nummern
- Rechnernamen
- VPN - Zugänge

3.6 Sorgfaltspflicht

IT-Systeme und Ausrüstungsgegenstände sind pfleglich zu behandeln. Die Geräte sind vor Feuchtigkeit und Verschmutzung zu schützen. Der Verlust oder Diebstahl von Hard- beziehungsweise Software ist unmittelbar der jeweiligen Supportorganisation zu melden. Des Weiteren hat gemäß DA Schadensmeldung eine Schadensmeldung an die dafür zuständigen Stellen zu erfolgen.

Werden IT-Systeme für eine längere Zeit nicht benutzt, zum Beispiel wegen längerer Abwesenheit (Dienstschluss, Wochenende, Urlaub), sind sie von den Personen, die das System zuletzt nutzen, abzuschalten. Server bilden hier eine Ausnahme.

3.7 Datensicherung

Um das Risiko eines Datenverlustes zu reduzieren, sind zur Datenablage vorrangig die Netzlaufwerke zu nutzen, da diese regelmäßig einer automatischen Datensicherung unterliegen.

Für die Sicherung von lokal auf IT-Systemen gehaltenen Daten sind die Personen, die das System nutzen, selbst verantwortlich. Hierzu erfolgt bei Bedarf Unterstützung durch den jeweiligen Supportbereich.

3.8 Datenschutz

Datenschutz ist die Gewährleistung des informationellen Selbstbestimmungsrechts von Betroffenen bei der Verarbeitung ihrer personenbezogenen Daten auch im Rahmen eines Dienst- oder Arbeitsverhältnisses. Keine natürliche Person darf durch die Verarbeitung ihrer Daten in unzulässiger Weise in ihrem Recht beeinträchtigt werden, selbst über die Preisgabe und Verwendung ihrer Daten zu bestimmen. Das heißt, dass personenbezogene Daten nur erhoben, gespeichert, verändert, übermittelt, gesperrt, gelöscht oder sonst genutzt werden dürfen, wenn die betroffene Person eingewilligt hat oder eine Rechtsvorschrift (auch Dienstvereinbarung und Tarifvertrag) die Datenverarbeitung erlaubt.

Die Einhaltung der Datenschutzvorschriften für alle Tätigkeiten im WDR überwacht die beauftragten Person für betrieblichen Datenschutz im WDR.

Näheres zum Datenschutz ist in der DA Datenschutz sowie der EU-Datenschutzgrundverordnung, dem Datenschutzgesetz NRW und weiteren nationalen oder europäischen datenschutzrechtlichen Regelungen geregelt.

3.9 Datenspeicherung und Datenaustausch

Personenbezogene Daten sowie vertrauliche Informationen sind stets gegen fremde Zugriffe zu sichern (zum Beispiel durch Verschlüsselung). Der zuständige Supportbereich stellt hierzu geeignete Verfahren zur Verfügung und ist die Ansprechstelle für Unterstützungsleistung.

Jeder informationstechnische Datenaustausch zwischen externen Stellen und dem WDR-Netz (zum Beispiel Internetzugriff, Zugriff auf das WDR-Netz) muss grundsätzlich über vom WDR zentral bereitgestellte Dienste durchgeführt werden. Ein hiervon abweichendes Verfahren muss über den jeweiligen Supportbereich beantragt und von der Person genehmigt und zentral dokumentiert werden, die für das WDR-Netz die Informationstreuhänderschaft hat (Informationstreuhänder:in).

3.9.1 Virenschutz

Der Virenschutz im WDR folgt dem Grundsatz „Ohne aktuellen Virenschutz kein Netzzugang“.

Der jeweilige Supportbereich stellt hierzu an jedem PC-Arbeitsplatz ein entsprechendes Suchprogramm gegen systemschädliche Programme (Computerviren beziehungsweise Schadcode) zur Verfügung. Bei jedem Verdacht auf systemschädliche Programme ist sofort der jeweilige Supportbereich zu informieren.

Zum Schutz vor systemschädlichen Programmen ist der Datenaustausch per Mail oder Datenträger auf das dienstlich Notwendige zu beschränken. Jegliche Daten, die per Mail oder Datenträger gesendet oder empfangen werden, sind vor dem Versenden, Öffnen beziehungsweise der Ausführung auf systemschädliche

Programme zu überprüfen. Dies gilt auch beim Einsatz von IT-Systemen, die über keine automatisierte Virensuchfunktion verfügen, weil sie zum Beispiel nicht dem WDR-Standard entsprechen oder nicht mit dem WDR-Netz verbunden sind (zum Beispiel mobile Endgeräte wie Notebooks, Tablets, Smartphones).

Im WDR-Intranet sind unter dem Angebot zur Informationssicherheit weiterführende Informationen zum Virenschutz bereit gestellt. Hierzu gehören eine Anleitung für die Virenüberprüfung von Datenträgern und detaillierte Verhaltensregeln für den Virenschutz.

3.9.2 Mobile Datenträger

Beschäftigte, die mobile Datenträgern (zum Beispiel USB-Sticks, SD-Cards, CDs, DVDs, externe Festplatten) verwenden, haben eine besondere Verantwortung und Sorgfaltspflicht, damit eine missbräuchliche Verwendung der so gespeicherten Daten ausgeschlossen ist.

Risiken bestehen insbesondere durch:

- Unbefugtes beziehungsweise unkontrolliertes Einspielen von Software,
- unberechtigte Nutzung und Kopieren von Daten,
- Verlust von ungesichert auf einem Speichermedium gehaltenen Daten,
- unkontrolliertes Booten eines IT-Systems,
- Befall durch Schadsoftware.

Daher ist die Verwendung von externen Datenträgern nur gestattet, wenn diese ausschließlich für dienstliche Zwecke genutzt werden und nur an IT-Systemen betrieben werden, die über einen aktuellen Virenschutz verfügen.

Sensible Daten (beispielsweise unternehmensinterne Dokumente, vertrauliche Informationen, personenbezogene Daten) sind auf mobilen Datenträger vor unbefugtem Zugriff zu schützen (beispielsweise mittels Verschlüsselung). Hierzu ist gegebenenfalls der jeweilige Supportbereich zu kontaktieren.

Aus Sicherheitsgründen kann die Verwendung von mobilen Datenträgern an bestimmten IT-Systemen seitens des Betreibers unterbunden beziehungsweise untersagt werden.

3.9.3 E-Mail / Internet

Der Informationsaustausch über das Internet, insbesondere per E-Mail oder über das World-Wide-Web (WWW) erfolgt in der Regel im Klartext. Aus diesem Grund dürfen personenbezogene Daten oder vertrauliche Informationen nur verschlüsselt über

diese Wege übermittelt werden. Hierfür stellt der jeweilige Supportbereich geeignete Programme zur Verfügung.

Die Einrichtung einer automatischen Weiterleitung von E-Mails an außerhalb des WDR-Netzes befindliche Empfänger ist aus Gründen des Datenschutzes und der Informationssicherheit nicht zulässig.

Personen, die IT-Systeme des WDR nutzen, sollten E-Mail-Anhänge (Attachments) und aus dem Internet herunterladbare Dateien nur dann laden, öffnen oder starten, wenn

- ihnen die Herkunft bekannt ist oder die Übermittlung von Attachments vorher in geeigneter Weise vereinbart wurde und
- sie wissen, worum es sich dabei handelt.

Im WDR-Intranet sind im Angebot zur Informationssicherheit weiterführende Informationen sowie Verhaltensregeln zur sicheren E-Mail- und Internetnutzung bereit gestellt.

3.10 Sicherheitsfunktionen

Sicherheitsfunktionen, die die Anwendungen (zum Beispiel passwortgeschützte Bildschirmsperre) anbieten, sind zu nutzen. Bei Einführung neuer Anwendungen und Dienste werden die betroffenen Personen vom jeweiligen Supportbereich auf die neuen Sicherheitsfunktionen hingewiesen und im Gebrauch unterwiesen.

Voreingestellte Sicherheitsfunktionen dürfen nur von IT administrierenden Personen deaktiviert oder geändert werden.

Bei Fragen zu Sicherheitsfunktionen steht der jeweilige Supportbereich zur Verfügung.

3.11 Anwenderberatung

Für die Anwenderberatung ist der jeweilige Supportbereich zuständig. Sofern erforderlich, wird eine Einweisung bei der Aufstellung oder der Installation von IT-Systemen gegeben.

Treten während des Betriebes unerwartete oder fehlerhafte Funktionen auf, so ist der jeweilige Supportbereich unverzüglich zu benachrichtigen.

4. Zusatzregelungen für mobile Endgeräte

Im WDR werden neben stationären Desktop-PCs zunehmend auch mobile Endgeräte (zum Beispiel Notebooks, Smartphones und Tablets) eingesetzt.

Prinzipiell gelten für mobile Endgeräte – und die auf ihnen gespeicherten Daten – die gleichen Anforderungen wie für jeden Desktop-PC im WDR. Mobile Endgeräte kommen jedoch durch Reisen oder ähnliches oftmals auch außerhalb der WDR-Gebäude zum Einsatz. Zudem stellen sie einen hohen Wert dar, der potentielle Diebe anlockt, zumal diese Geräte leicht veräußert werden können.

Deshalb sind folgende zusätzlichen Vorkehrungen zum Schutz vor Verlust und Beschädigung der mobilen Endgeräte und der auf ihnen gespeicherten Daten erforderlich.

4.1 Virenschutz

Für mobile Endgeräte bestehen besondere Gefährdungen, da sie unter Umständen mit Drittnetzen (Internet) ohne die zentralen Virenschutzmaßnahmen des WDR verbunden werden. Zudem können Virenschutzsoftware und die Virendefinitionen nicht immer tagesaktuell gehalten werden, weil zum Beispiel ein Notebook nicht ständig mit dem WDR-Netz verbunden ist.

Auch für mobile Endgeräte gilt jedoch der Grundsatz „Ohne aktuellen Virenschutz kein Netzzugang“. Deshalb müssen Personen, die mobile Endgeräte des WDR verwenden, die vom WDR eingerichtete Aktualisierung und Virenüberprüfung nutzten. Dies geschieht im Normalfall automatisiert bei der Anmeldung an das WDR-Netzwerk.

4.2 Datenspeicherung

Personenbezogene Daten sowie vertrauliche Informationen dürfen nur verschlüsselt auf mobilen Endgeräten gespeichert werden. Der zuständige Supportbereich stellt hierzu geeignete Verfahren zur Verfügung und ist die Ansprechstelle für Unterstützungsleistung.

4.3 Datensicherung

Anders als bei Desktop-PCs ist es bei mobilen Endgeräten meist unvermeidbar, dass Daten zumindest zeitweise lokal anstatt auf einem zentralen Server gespeichert werden. Dem Verlust dieser Daten muss durch geeignete Datensicherungsmaßnahmen vorgebeugt werden. Personen, die mobile Endgeräte des WDR verwenden, sind für die notwendigen Aktivitäten (Datensicherung und Wiederherstellung) selbst verantwortlich. Der zuständige Supportbereich stellt hierzu geeignete Verfahren zur Verfügung und ist Ansprechpartner für Unterstützungsleistung.

4.4 Diebstahlschutz

Zum Schutz vor Diebstahl sind Zeiten, in denen das mobile Endgerät unbeaufsichtigt bleibt, auf ein Minimum zu beschränken. Notebooks sind außerhalb der Nutzungszeit vor Diebstahl zu sichern (zum Beispiel verschlossener Schrank, PKW Kofferraum, Verwendung eines Seilschlosses).

5. Schulung

Alle Personen, die IT-System des WDR nutzen, sind angehalten, sich für die von ihnen genutzten Anwendungen auf einen aktuellen Kenntnisstand zu halten. Hierzu sind die vom WDR zur Verfügung gestellten Schulungs- und Beratungsmöglichkeiten zu nutzen.

6. Inkrafttreten

Diese Dienstanweisung tritt zum 01.03.2025 in Kraft und ersetzt die Dienstanweisung IT-Anwendung vom 11.05.2022.

Köln, 06.03.2025
gez. Katrin Vernau
Intendantin