Dienstanweisung zur Behandlung von IT-Sicherheitsvorfällen (DA IT-Sicherheitsvorfallbehandlung)

Vom 11.05.2022

1. Gegenstand 2

2. Geltungsbereich 2

3. Definitionen 2

4. Prozesse 3

4.1 Schwachstellenmanagement 3
4.2 Störungsmanagement 3
4.3 Sicherheitsvorfallmanagement 3

5. Verantwortlichkeiten 3

5.1 Beschäftigte 3
5.2 Support 4
5.3 Informationstreuhänder:innen 4
5.4 Informationssicherheitsbeauftragte:r 4
5.5 IT-Sicherheitsvorfallteam 4
5.6 Leitung IT-Sicherheitsvorfallteam 5

6. Anforderungen an das Störungsmanagement 6

6.1 Erkennung und Meldung 6
6.2 Analyse und Bewertung 6
6.3 Behebung 6

7. Berichtswesen 6

7.1 Dokumentation der Meldungen 6
7.2 Dokumentation der Maßnahmen 7
7.3 Benachrichtigung Dritter 7

8. Nachbereitung 7

9. Verstöße gegen Gesetze und Vorschriften 8

10. Inkrafttreten 9

Anlage 1 - Rollenzuordnungen 10

Anlage 2 – Einordnung von IT-Sicherheitsereignissen 12

1. Gegenstand

Diese Dienstanweisung regelt das Verfahren zur Behandlung von IT-Sicherheitsvorfällen sowie die damit einhergehenden Verantwortlichkeiten und organisatorischen Rahmenbedingungen.

Durch die zunehmende Komplexität der im WDR eingesetzten Informationstechnik (IT) sowie die wachsende Anzahl neuer Bedrohungen aus dem Internet steigt auch die Gefährdungslage für die Informationssicherheit im WDR. Daher muss insbesondere bei der Behandlung von IT-Sicherheitsvorfällen ein rechtzeitiges Handeln sowie ein strukturiertes Vorgehen sichergestellt werden.

2. Geltungsbereich

Diese Dienstanweisung gilt für alle Beschäftigten des WDR.

Durch vertragliche Vereinbarungen ist sicherzustellen, dass die nachfolgenden Regelungen auch von Dritten, die für den WDR IT betreiben oder diesen beim Betrieb der IT unterstützen, eingehalten werden.

3. Definitionen

Ein Sicherheitsereignis liegt dann vor, wenn die Sicherheitsziele des WDR (siehe Informationssicherheitsordnung) gefährdet sind oder sein könnten. Beispiele sind, wenn ein vermuteter, möglicher oder tatsächlicher Verlust der Vertraulichkeit, Integrität oder der Verfügbarkeit von Informationen, IT-Systemen, Anwendungen oder Diensten des WDR droht beziehungsweise vorliegt oder wenn im Zusammenhang mit IT-Systemen gegen Gesetze und Vorschriften verstoßen wird. Sicherheitsereignisse werden unterschieden in Schwachstellen, Störungen und Sicherheitsvorfälle.

Eine Schwachstelle ist eine Sicherheitslücke oder eine Fehlfunktion in einem IT-System, einer Anwendung oder einem Dienst, die zu einer Verletzung der Vertraulichkeit, Integrität oder Verfügbarkeit von Informationen führen kann.

Eine Störung liegt dann vor, wenn vorrangig die Verfügbarkeit von Informationen, Systemen, Anwendungen oder Diensten nicht mehr gewährleistet ist (bspw. Ausfall eines Dienstes).

Ein Sicherheitsvorfall liegt dann vor, wenn vorrangig die Vertraulichkeit oder Integrität von Systemen, Diensten oder digitalen Informationen verletzt wurde, der Verlust der Verfügbarkeit vorsätzlich beziehungsweise fahrlässig herbeigefügt wurde oder Informationen unwiederbringlich verloren gegangen sind.

4. Prozesse

4.1 Schwachstellenmanagement

Der Umgang mit und die Behebung von Schwachstellen erfolgen im Rahmen der Standard-Betriebsprozesse (beispielsweise das Patch- und Änderungsmanagement).

Kann eine Schwachstelle im Rahmen der betrieblichen Abläufe nicht behoben werden, ist diese als Sicherheitsvorfall zu behandeln.

4.2 Störungsmanagement

Die Behebung einer Störung erfolgt im Rahmen der Standard-Betriebsprozesse (beispielsweise das Störungsmanagement).

Sofern der Verlust der Verfügbarkeit vorsätzlich herbeigefügt wurde oder Informationen unwiederbringlich verloren gegangen sind, ist die Störung als Sicherheitsvorfall zu behandeln.

4.3 Sicherheitsvorfallmanagement

Die Behandlung eines Sicherheitsvorfalls erfolgt in der Regel im Rahmen des Störungsmanagements.

Die beauftragte Person für Informationssicherheit im WDR (Informationssicherheitsbeauftragte:r) ist über jeden Sicherheitsvorfall umgehend zu informieren.

Können Sicherheitsvorfälle nicht im Rahmen der betrieblichen Abläufe behoben werden, erfolgt nach Lageeinschätzung durch die betreffenden Personen mit Informationstreuhänderschaft (Informationstreuhänder:–innen) eine Meldung an die Leitung des IT-Sicherheitsvorfallteams.

Die Leitung des IT-Sicherheitsvorfallteams bewertet anhand der vorliegenden Informationen die aktuelle Sicherheitslage und entscheidet über die Einberufung des IT-Sicherheitsvorfallteams.

Droht durch einen IT-Sicherheitsvorfall ein besonders schwerwiegender Schaden für den WDR (beispielsweise ein finanzieller Schaden, ein Reputationsschaden oder ein betrieblicher Schaden), erfolgt nach einer ersten Lagebeurteilung durch das IT-Sicherheitsvorfallteam eine Meldung an die Geschäftsleitung.

5. Verantwortlichkeiten

5.1 Beschäftigte

Die Beschäftigten sind verpflichtet, Sicherheitsereignisse unverzüglich dem jeweils zuständigen Support zu melden.

In besonderen Ausnahmefällen kann die beauftragte Person für Informationssicherheit auch direkt kontaktiert werden. Dies kann der Fall sein, wenn besondere Vertraulichkeitsanforderungen vorliegen oder der Sicherheitsvorfall die Meldekette betrifft (zum Beispiel den Support).

5.2 Support

Der jeweils zuständige Support ist die zentrale Meldestelle für Sicherheitsereignisse im WDR. Er ist verantwortlich für die Annahme und Bewertung der eingehenden Meldungen. Des Weiteren ist festzustellen, ob es sich um normale Störungen oder um potentielle Informationssicherheitsvorfälle handelt. Falls keine eindeutige Entscheidung gefällt werden kann, werden die Meldungen als potentielle Sicherheitsvorfälle behandelt.

Störungen werden an die für die Behebung der Störung zuständigen Stellen weitergeleitet. Potentielle Sicherheitsvorfälle werden umgehend an die betreffenden Personen mit Informationstreuhänderschaft gemeldet.

5.3 Informationstreuhänder:innen

Die betreffenden Personen mit Informationstreuhänderschaft sind für das Störungsmanagement verantwortlich. Im Rahmen dessen sind sie auch für die Behebung von Sicherheitsvorfällen zuständig und stellen die Kommunikation zu allen betroffenen Stellen sicher.

5.4 Informationssicherheitsbeauftragte:r

Die beauftragte Person für Informationssicherheit im WDR ist verantwortlich für die Koordination, die Effektivitätsprüfung und Weiterentwicklung des Informationssicherheitsmanagements. Hierzu gehören insbesondere die Überprüfung der Sicherheitsvorfallbehandlung hinsichtlich möglicher Verbesserungen sowie die abschließende Analyse und Bewertung von Sicherheitsvorfällen. Darüber hinaus unterstützt sie das IT-Sicherheitsvorfallteam bei der Lagebeurteilung aus übergeordneter Sicht sowie bei der Auswahl geeigneter Maßnahmen zur Behebung des IT-Sicherheitsvorfalls.

Zudem ist sie verantwortlich für die Sensibilisierung aller am Prozess beteiligten Personen.

In besonderen Fällen nimmt die beauftragte Person für Informationssicherheit auch direkt Meldungen über Sicherheitsvorfälle entgegen (siehe Ziffer 5.1).

5.5 IT-Sicherheitsvorfallteam

Das IT-Sicherheitsvorfallteam ist nach Einberufung verantwortlich für die angemessene Reaktion auf IT-Sicherheitsvorfälle. Es besteht aus einem Kernteam und einem erweiterten Team.

Das Kernteam setzt sich aus mehreren Rollen zusammen, die für die Behandlung von Informationssicherheitsvorfällen immer benötigt werden. Im Einzelnen sind dies

- die Leitung des IT-Sicherheitsvorfallteams,
- die verantwortliche Person für IT und Medientechnik,
- die verantwortliche Person für zentrale Anwendungen der Verwaltung,
- die verantwortliche Person für das technische Netzwerk der Gebäudewirtschaft,
- die beauftragte Person für Informationssicherheit im WDR,
- die betreffenden Personen mit Informationstreuhänderschaft sowie
- die betroffene informationsverantwortliche Person.

Die Besetzung der Rollen ist in Anlage 1 beschrieben.

Zum erweiterten Team gehören das Kernteam, die zuständigen Bereichs-Informationssicherheitsbeauftragten, die beauftragte Person für betrieblichen Datenschutz im WDR (Datenschutzbeauftragte:r), je eine Person aus dem Justiziariat, der HA Revision, der Abteilung Kommunikation, dem Personalrat und gegebenenfalls weitere interne oder externe Fachleute.

Das IT-Sicherheitsvorfallteam deckt alle Kompetenzfelder, die für die effiziente Behebung eines Informationssicherheitsvorfalls erforderlich sind, ab. Dazu gehören insbesondere die Veranlassung weiterer notwendiger Maßnahmen (beispielsweise die korrekte Sicherstellung und forensische Analyse von Beweismitteln).

Nach Einschätzung der Lage kann die Leitung des IT-Sicherheitsvorfallteams Personen aus dem erweiterten Team für die Behandlung des IT-Sicherheitsvorfalls hinzuziehen.

5.6 Leitung IT-Sicherheitsvorfallteam

Die Leitung des IT-Sicherheitsvorfallteams ist verantwortlich für die Steuerung und Koordination des IT-Sicherheitsvorfallteams und entscheidet über die Umsetzung der erforderlichen Maßnahmen sowie den weiteren Ressourceneinsatz zur Behebung eines IT-Sicherheitsvorfalls.

Bei besonders schwerwiegenden IT-Sicherheitsvorfällen informiert die Leitung des IT-Sicherheitsvorfallteams die Geschäftsleitung und stimmt mit dieser das weitere Vorgehen ab.

6. Anforderungen an das Störungsmanagement

Schwachstellen, Störungen und Sicherheitsvorfälle werden im Rahmen der betrieblichen Abläufe (Standardprozesse) weiter behandelt. Dies ist Gegenstand der jeweiligen betrieblichen Abläufe.

Folgende Aspekte der Behandlung von Sicherheitsvorfällen sind in diese Prozesse zu integrieren.

6.1 Erkennung und Meldung

In dieser Phase werden alle Meldungen über Sicherheitsereignisse entgegengenommen. Annehmende Stellen sind die IT-Hotline beziehungsweise die jeweils zuständige Supportorganisation.

Die Meldungen über Sicherheitsereignisse werden dort gemäß Anlage 2 eingeordnet und an die betreffenden Personen mit Informationstreuhänderschaft weitergeleitet.

6.2 Analyse und Bewertung

Sofern Meldungen als Sicherheitsvorfälle identifiziert wurden, werden diese seitens der betreffenden Personen mit Informationstreuhänderschaft zunächst analysiert und bewertet. Wurde ein Sicherheitsvorfall vorsätzlich herbeigeführt beziehungsweise besteht dieser Verdacht, sind die für die weitere Ermittlung notwendigen Informationen nach Möglichkeit revisionssicher zu dokumentieren und bei Bedarf IT-forensisch zu untersuchen.

Über das Ergebnis sind die die beauftragte Person für Informationssicherheit sowie die jeweils zuständigen Bereichs-Informationssicherheitsbeauftragten zu informieren.

6.3 Behebung

Die Behebung der Informationssicherheitsvorfälle findet im Rahmen des Störungsmanagements des jeweils zuständigen Bereiches statt. Hierzu gehört neben der Einleitung von Sofortmaßnahmen auch eine weitere Detailanalyse.

IT-Sicherheitsvorfälle sind abschließend durch die betreffenden Personen mit Informationstreuhänderschaft zu dokumentieren. Die Dokumentation erhält der oder die Informationssicherheitsbeauftragte zur Nachbereitung.

7. Berichtswesen

7.1 Dokumentation der Meldungen

Jede Ebene des Meldeweges protokolliert zumindest folgende Informationen bei Ankunft oder Weiterleitung von Sicherheitsvorfall-Meldungen:

- Eindeutige Identifikation der Meldung,
- Beschreibung des Ereignisses,
- Name, E-Mail-Adresse und Telefonnummer der meldenden Person,
- Datum und Uhrzeit der Ankunft und gegebenenfalls Weiterleitung der Meldung.

7.2 Dokumentation der Maßnahmen

Alle durchgeführten Tätigkeiten werden nachvollziehbar festgehalten. Für jede Handlung werden folgende Informationen erfasst:

- Datum und Uhrzeit,
- Ziel und Zweck der Maßnahmen,
- Beschreibung der ausgeführten Maßnahmen,
- Ergebnis der Maßnahmen,
- Bewertung des Ergebnisses.

7.3 Benachrichtigung Dritter

Eine öffentliche Information Dritter oder eine interne Information der Beschäftigten über IT-Sicherheitsvorfälle des WDR erfolgt grundsätzlich über die Abteilung Kommunikation. Davon ausgenommen ist der vertrauliche Austausch von Informationen auf technischer Ebene zur konkreten Behebung eines IT-Sicherheitsvorfalls oder zur Warnung Dritter.

8. Nachbereitung

Jeder Informationssicherheitsvorfall ist von der beauftragten Person für Informationssicherheit mit dem Ziel auszuwerten, Verbesserungen für den Umgang mit Informationssicherheitsvorfällen präventiv zu erreichen oder Rückschlüsse auf die Wirksamkeit der bestehenden IT-Sicherheitskonzeptionen zu ziehen.

Dabei sind insbesondere die folgenden Punkte zu bewerten beziehungsweise zu erfassen:

- Reaktionszeiten,

- Effektivität des Meldeweges,
- Effektivität der Analyse,
- Aufwände zur Behebung des IT-Sicherheitsvorfalls,
- Verbesserungspotentiale und
- Dokumentation des Informationssicherheitsvorfalls.

Die beauftragte Person für Informationssicherheiterstellt auf Grundlage der genannten Punkte einen Abschlussbericht und einen priorisierten Maßnahmenkatalog.

9. Verstöße gegen Gesetze und Vorschriften

Wird bei einem IT-Sicherheitsvorfall ein Verstoß gegen Gesetze oder Vorschriften festgestellt, sind geeignete Maßnahmen zur Beweissicherung durchzuführen und das weitere Vorgehen mit dem Justiziariat abzustimmen.

Liegt eine Datenschutzverletzung vor, ist zudem umgehend die beauftragte Person für betrieblichen Datenschutz im WDR (Datenschutzbeauftragte:r) einzubinden und gegebenenfalls eine Meldung an die zuständige Aufsichtsbehörde, beziehungsweise eine Benachrichtigung der betroffenen Personen zu veranlassen.

Es sind sowohl die gesetzlichen Vorschriften, insbesondere die nationale und europäische Datenschutzregelungen (zum Beispiel die Datenschutz-Grundverordnung) als auch das Landespersonalvertretungsgesetz NRW, sowie die einschlägigen Regelungen des WDR (zum Beispiel Ordnungen, Dienstvereinbarungen und Dienstanweisungen) zu beachten.

10. Inkrafttreten

Diese Dienstanweisung tritt mit Wirkung vom 01.06.2022 in Kraft und ersetzt die Dienstanweisung zur Behandlung von IT-Sicherheitsvorfällen vom 17.07.2019.

Die beauftragte Person für Informationssicherheit im WDR kann die Anlagen jederzeit aktualisieren, ohne dass es hierzu einer Änderung dieser Dienstanweisung bedarf.

Köln, den 11.05.2022
gez. Tom Buhrow
Intendant

Anlage 1 - Rollenzuordnungen

1. IT-Sicherheitsvorfallteam

Rolle	Stelle
Leitung des IT-Sicherheitsvorfallteams bei Vorfällen, die die zentralen Anwendungen der Verwaltung betreffen (beispielsweise SAP-Systeme, Mediendatensysteme)	Leitung der Abteilung Informationsmanagement
Leitung des IT-Sicherheitsvorfallteams bei Vorfällen, die das technische Netzwerk der Gebäudewirtschaft betreffen (zum Beispiel Gebäudeleittechnik, Stationsleittechnik, Sicherheitstechnische Anlagen)	Leitung der Abteilung Gebäudebetrieb
Leitung des IT-Sicherheitsvorfallteams bei allen anderen oder übergreifenden IT-Sicherheitsvorfällen	Leitung der HA IT und Medientechnik
Verantwortliche Person für IT und Medientechnik	Leitung der HA IT und Medientechnik
Verantwortliche Person für zentrale Anwendungen der Verwaltung	Leitung der Abteilung Informationsmanagement
Verantwortliche Person für das technische Netzwerk der HA Gebäudewirtschaft	Leitung der Abteilung Gebäudebetrieb
Informationssicherheitsbeauftragte:r	Siehe Informationssicherheitsordnung Ziffer 2.2.
Informationstreuhänder:in	Siehe Informationssicherheitsordnung Ziffer 2.5.
Informationsverantwortliche:r	Siehe Informationssicherheitsordnung Ziffer 2.4.

2. Support

Rolle	Stelle
Support für IT und Medientechnik	Abteilung Service und Support
Support für das technische Netzwerk der HA Gebäudewirtschaft	Abteilung Gebäudebetrieb

Anlage 2 – Einordnung von IT-Sicherheitsereignissen

1. Betroffene Werte
    - 1.1 Verfügbarkeit
        - 1.1.1 Unwiederbringlicher Verlust
    - 1.2 Vertraulichkeit
    - 1.3 Integrität
2. Art des IT-Sicherheitsereignisses
    - 2.1 Zufällig
        - 2.1.1 Technischer Fehler
        - 2.1.2 Ausfall essentieller Dienste
        - 2.1.3 Elementarereignisse
        - 2.1.4 Andere
    - 2.2 Vorsätzlich
        - 2.2.1 Diebstahl
        - 2.2.2 Betrug
        - 2.2.3 Informationsabfluss
        - 2.2.4 Sabotage/Physische Beschädigung
        - 2.2.5 Schadsoftware
        - 2.2.6 Hacking/Ausspähung von Daten
        - 2.2.7 Vorsätzliches Stören/Denial of Service
        - 2.2.8 Nicht autorisierte Verwendung von Ressourcen
        - 2.2.9 Andere

- 2.3 Fehlhandlung
  - 2.3.1 Wartungsfehler
  - 2.3.2 Fehlbedienung
  - 2.3.3 Planungsfehler
  - 2.3.4 Unachtsamkeit
- 2.4 Sonstiges

3. Status
   - 3.1 Tatsächlich eingetreten
   - 3.2 Versuch
   - 3.3 Verdacht
   - 3.4 Möglichkeit (Schwachstelle)