



Leitlinie zur Informationssicherheit im Ministerium für Schule und Bildung des Landes Nordrhein-Westfalen

(Informationssicherheitsleitlinie MSB)



Inhaltsverzeichnis

Inhaltsverzeichnis.....	2
1 Einleitung.....	3
2 Stellenwert der Informationssicherheit.....	3
3 Geltungsbereich	4
3.1 Bezirksregierungen	4
3.2 Kommunen.....	5
3.3 Ergänzende Leitlinien.....	5
4 Verantwortungsebenen.....	5
5 Festlegung von Sicherheitszielen	6
6 Informationssicherheitsstrategie	6
7 Organisationsstruktur für Informationssicherheit.....	8
7.1 Leitung des Ministeriums.....	8
7.2 Informationssicherheitsbeauftragte oder Informationssicherheitsbeauftragter des MSB (Ressort-CISO)	9
7.3 Informationssicherheitsbeauftragte (ISB).....	9
7.4 Informationssicherheitsmanagement-Gremium des MSB (ISMG MSB).....	10
8 Aktualisierung der Informationssicherheitsleitlinie.....	10
9 Inkraftsetzung und Veröffentlichung.....	11



1 Einleitung

Diese Leitlinie zur Informationssicherheit beschreibt den Stellenwert, die verbindlichen Prinzipien und das angestrebte Niveau der Informationssicherheit im Ministerium für Schule und Bildung des Landes Nordrhein-Westfalen und dem Geschäftsbereich. Sie formuliert die erforderlichen Sicherheitsziele sowie den organisatorischen Rahmen, in dem diese umgesetzt werden.

Die Regelungen dieser Leitlinie folgen den IT-Grundschutz-Standards des Bundesamtes für Sicherheit in der Informationstechnik (BSI).¹ Sie entsprechen zudem den Festlegungen der vom Kabinett am 23.06.2015 beschlossenen und am 01.07.2015 in Kraft getretenen „Leitlinie zur Informationssicherheit der Landesverwaltung Nordrhein-Westfalen“ (ISL NRW). Mit der ISL NRW wird für das Land Nordrhein-Westfalen der Beschluss des IT-Planungsrates vom 08.03.2013 umgesetzt, welcher die Erstellung von Informationssicherheitsleitlinien für den Bund und die Länder vorsieht.

Auf der Basis der ISL NRW werden in der vorliegenden Informationssicherheitsleitlinie des MSB (ISL MSB) die für das Ministerium für Schule und Bildung des Landes Nordrhein-Westfalen und dem Geschäftsbereich geltenden grundlegenden Ziele der Informationssicherheit festgelegt. Die ISL MSB

- beschreibt den Stellenwert der Informationssicherheit,
- legt den Geltungsbereich der ISL MSB fest,
- enthält das Bekenntnis der Behördenleitung zu ihrer Verantwortung für die Informationssicherheit,
- formuliert die allgemeinen Sicherheitsziele,
- legt die Sicherheitsstrategie fest,
- definiert die Sicherheitsorganisation und
- verpflichtet zur kontinuierlichen Fortschreibung des Regelwerks zur Informationssicherheit.

Diese Leitlinie bildet die Grundlage für die Erstellung weiterer, auch fachspezifischer Richtlinien, Informationssicherheitskonzepte sowie Regelungen und Dienstweisungen zur Informationssicherheit.

2 Stellenwert der Informationssicherheit

Der Stellenwert von informationsverarbeitenden Systemen für die Geschäftstätigkeit des gesamten Ressorts steigt seit vielen Jahren an. Sei es bei der täglichen Arbeit am dienstlichen Rechner vor Ort wie auch im Rahmen der mobilen Arbeit, bei der Kommunikation mit Kolleginnen, Kollegen und Geschäftskontakten per E-Mail oder

¹ Vgl. <https://www.bsi.bund.de/>



beim Einsatz spezieller Fachverfahrenssoftware. Schon heute wäre ein Ausfall der IT-Systeme des MSB mit erheblichen Auswirkungen für die Arbeitserledigung und das Ansehen des Ressorts verbunden. Mit der Umsetzung des E-Government-Gesetzes NRW gewinnt die Informationstechnik nochmals mehr an Bedeutung. Doch auch bei nicht-IT-gebundenen Informationen sind Sicherheitsbetrachtungen notwendig, ganz gleich ob es sich um das Wissen der Mitarbeiterinnen und Mitarbeiter, die Organisation von Geschäftsprozessen oder die Arbeit mit Papierdokumenten handelt.

Die Informationssicherheit ist deshalb für das MSB ein unverzichtbarer Grundwert, um den folgenden Anforderungen gerecht werden zu können:

- Die rechtlichen Vorschriften, beispielsweise zum Datenschutz, müssen eingehalten werden, Dienst- und Amtsgeheimnisse müssen gewahrt bleiben.
- Alle Dienstleistungen, vor allem Online-Dienste, für Bürgerinnen und Bürger, Wirtschaft und Verwaltung müssen sicher, zuverlässig und vertrauenswürdig erbracht werden.
- Die Risiken von Schadensfällen sind durch angemessene Vorsorgemaßnahmen auf ein vertretbares Maß zu reduzieren.
- Ein Reputationsverlust durch die Verletzung der Informationssicherheitsziele ist zu vermeiden.

3 Geltungsbereich

Die vorliegende Leitlinie gilt dem Schutz aller geschäftsrelevanten Informationen und deren Verarbeitung im MSB und im Geschäftsbereich. Dazu zählen neben dem Ministerium für Schule und Bildung

- die Qualitäts- und Unterstützungsagentur – Landesinstitut für Schule,
- das Landesprüfungsamt für Lehrämter an Schulen,
- die Zentren für schulpraktische Lehrerbildung,
- das Haus für Lehrerfortbildung Kronenburg und
- die Staatlichen Schulen.

3.1 Bezirksregierungen

Soweit den Bezirksregierungen Aufgaben für den Geschäftsbereich des MSB übertragen sind, liegt die Fachaufsicht beim MSB. Die Bezirksregierungen übernehmen die Dienst- und Fachaufsicht über ihnen nachgeordnete Behörden und Einrichtungen im Geschäftsbereich des MSB. Die Dienstaufsicht über die Bezirksregierungen hat das Ministerium des Innern (IM). Das MSB ist oberste Dienstbehörde für die Beschäftigten seines Geschäftsbereichs und übt insoweit die Dienstaufsicht aus. Zur Klärung



von Zuständigkeiten und Regelungen zur Koordinierung der Informationssicherheit in den Bezirksregierungen, die den Geschäftsbereich des MSB betreffen, stimmen sich MSB und IM anlassbezogen ab.

3.2 Kommunen

Für die Kommunen hat unter Anwendung des Beschlusses des IT-Planungsrats die ISL NRW nur empfehlenden Charakter. Die öffentlichen Schulen in kommunaler Trägerschaft sowie die staatlichen Schulämter und die Ämter für Ausbildungsförderung bei den Kreisen und kreisfreien Städten fallen daher nicht in den Geltungsbereich und sind dementsprechend von dieser Leitlinie ausgenommen.

Die Anwendung dieser Leitlinie wird für diese Einrichtungen und Behörden empfohlen. In der Verantwortung für das Schulwesen, die Schülerinnen und Schüler und die Landesbeschäftigten wirkt das MSB unabhängig vom Geltungsbereich auf eine möglichst weitgehende Umsetzung der Sicherheitsziele und der Informationssicherheitsstrategie dieser Leitlinie im gesamten Schulbereich hin.

Entsprechendes gilt für die Ersatzschulen, die Schulen gemäß § 124 Absatz 4 SchulG (BASS 1-1) und die sonstigen unter der Aufsicht des MSB stehenden juristischen Personen des öffentlichen Rechts.

3.3 Ergänzende Leitlinien

Die Behörden und Einrichtungen im Geschäftsbereich des MSB können ergänzende Informationssicherheitsleitlinien erstellen. Für die Behörden und Einrichtungen gemäß Absatz 1 ist das Einvernehmen mit dem Ressort-CISO (s. Kapitel 7.2) herzustellen.

4 Verantwortungsebenen

Die Behördenleitung des MSB bekennt sich zu ihrer Gesamtverantwortung für die Informationssicherheit im MSB. Zur Erreichung und Aufrechterhaltung eines angemessenen Maßes an Informationssicherheit werden ausreichende sächliche, personelle und zeitliche Ressourcen bereitgestellt.

Leiterinnen und Leiter von Behörden und Einrichtungen im Geschäftsbereich des MSB sind im Rahmen ihrer Zuständigkeit für die Informationssicherheit verantwortlich.

Hierzu werden geeignete Maßnahmen im Sinne der Informationssicherheitsleitlinie umgesetzt, so dass die Vertraulichkeit, die Integrität und die Verfügbarkeit der Informationen gesichert werden. Dabei sind die Risiken, die sich bei der Verarbeitung und Speicherung von Informationen ergeben, bewusst zu steuern.



5 Festlegung von Sicherheitszielen

Informationssicherheit ist die Sicherung und Aufrechterhaltung der:

- **Vertraulichkeit**
Informationen dürfen ausschließlich einem berechtigten Personenkreis zur Verfügung stehen.
- **Integrität**
Die physische und logische Unversehrtheit von Systemen, Anwendungen und Informationen muss jederzeit gewahrt sein. Dies schließt auch die Verhinderung einer unberechtigten Erstellung, Veränderung oder Löschung von Informationen mit ein.
- **Verfügbarkeit**
Systeme, Anwendungen und Informationen müssen den Berechtigten stets wie vorgesehen zur Verfügung stehen.

Für das MSB werden darüber hinaus die nachstehenden Sicherheitsziele für die Informationssicherheit festgelegt:

- Sicherstellung der Kontinuität der Arbeitsabläufe innerhalb des Ressorts,
- zuverlässige Unterstützung der Geschäftsprozesse durch die IT,
- Realisierung sicherer und vertrauenswürdiger E-Government-Verfahren,
- Erhalt der in Technik, Informationen, Arbeitsprozesse und Wissen investierten Werte,
- Sicherung der hohen, möglicherweise unwiederbringlichen Werte der verarbeiteten Informationen,
- Gewährleistung der aus rechtlichen Vorgaben resultierenden Anforderungen,
- Gewährleistung des informationellen Selbstbestimmungsrechts der Betroffenen bei der Verarbeitung personenbezogener Daten,
- Wahrung der Dienst- oder Amtsgeheimnisse sowie
- Reduzierung der im Schadensfall entstehenden Aufwände durch ausreichende Notfallvorsorge.

Bei der Erreichung dieser Ziele ist eine Verhältnismäßigkeit der eingesetzten Mittel zum Wert der schützenswerten Güter zu beachten.

6 Informationssicherheitsstrategie

Die Informationssicherheitsstrategie für das MSB besteht darin, mit einem angemessenen Ressourceneinsatz ein höchst mögliches Maß an Informationssicherheit zu erreichen und verbleibende Restrisiken zu minimieren.



Informationssicherheitsleitlinie MSB

Bei der Auswahl und Umsetzung von Maßnahmen sind mögliche Auswirkungen auf die Geschäftsprozesse zu berücksichtigen.

Durch die Einführung eines Informationssicherheitsmanagementsystems (ISMS), orientiert an der ISO 27001 auf der Basis von IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI), wird ein kontinuierlicher Informationssicherheitsprozess etabliert. Auf Grundlage des landesweiten ISMS bauen die wesentlichen Dienststellen² im Geschäftsbereich des MSB eigene ISMS auf, dazu gehört auch die Benennung von Informationssicherheitsbeauftragten der jeweiligen Behörde oder Einrichtung.

Der Aufbau eines Informationssicherheitsmanagementsystems auf der Basis des IT-Grundschutzes des BSI bildet den Kern der Sicherheitsstrategie und beinhaltet insbesondere folgende Komponenten:

- **Sensibilisierung**
Die Beschäftigten werden durch Informationsveranstaltungen und Schulungen in die Lage versetzt, den Stellenwert der Informationssicherheit im Rahmen ihrer Tätigkeit nachzuvollziehen, die Notwendigkeit von Maßnahmen zu verstehen und ihr eigenes Handeln an den Sicherheitszielen auszurichten.
- **Risikoanalyse**
Im Rahmen einer ganzheitlichen Analyse der bestehenden Informationsverarbeitung, technisch wie konventionell, werden alle Elemente bezüglich ihrer Gefährdungen und der damit verbundenen Schadenshöhe bewertet. Darauf aufbauend erfolgt die Auswahl und Umsetzung spezifischer Maßnahmen zur Behandlung dieser Risiken.
- **Vorfallmanagement**
Für die Behandlung von sicherheitsrelevanten Vorkommnissen werden Verantwortlichkeiten und Vorgehensweisen festgelegt.
- **Notfallmanagement**
Der Wiederanlauf und die Wiederherstellung des Geschäftsbetriebs in Not- und Krisenfällen werden durch Notfallkonzepte und -pläne gewährleistet. Dabei wird die Informationssicherheit auch in solchen Ausnahmesituationen sichergestellt.

Zusammenarbeit mit den Kommunen

Das MSB kooperiert insbesondere mit den kommunalen Spitzenverbänden, den kommunalen IT-Dienstleistern, den Schulleitungen und den benannten IT-Sicherheitsbeauftragten der Kommunen.

² im Sinne des Kabinettsbeschlusses zur Informationssicherheit in der Landesverwaltung vom 23.06.2015

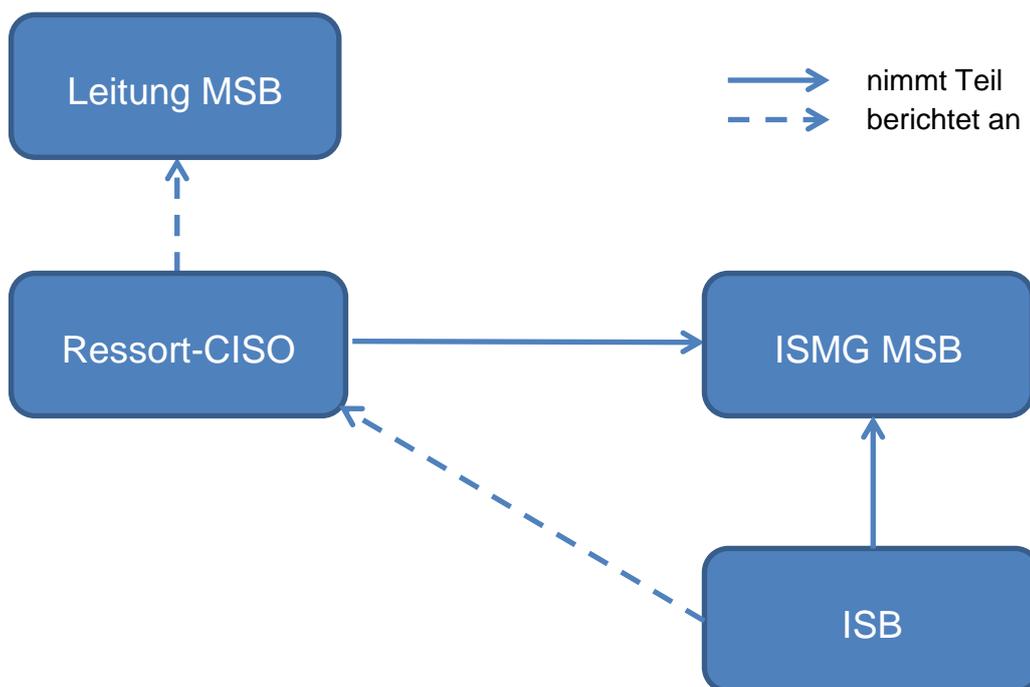


Für die sächliche Ausstattung der öffentlichen Schulen sowie für die der staatlichen Schulämter und der Ämter für Ausbildungsförderung sind die Kommunen zuständig. Die Schulleitungen und die Landesbeschäftigten in Leitungsfunktionen haben auf die Sachausstattung, die installierte Software, die Netzwerke und die Sicherheitsmechanismen in der Regel keinen Einfluss. Beschaffung, Wartung, Pflege und Administration von informationsverarbeitenden Systemen sind in kommunaler Hand.

7 Organisationsstruktur für Informationssicherheit

Die Organisationsstruktur für Informationssicherheit im Geschäftsbereich des MSB besteht aus:

- der Leitung des MSB,
- der oder dem Informationssicherheitsbeauftragten des MSB (Ressort-CISO),
- dem Informationssicherheitsmanagement-Gremium des MSB (ISMG MSB),
- den Informationssicherheitsbeauftragten (ISB) im Ressort.



7.1 Leitung des Ministeriums

Die Leitung des MSB trägt die Gesamtverantwortung für die Informationssicherheit und unterstützt alle angemessenen und geeigneten Maßnahmen zu ihrer Etablierung, Aufrechterhaltung und kontinuierlichen Verbesserung. Sie steht im vollen Umfang hinter der Informationssicherheitsstrategie und den Informationssicherheitszielen, die in dieser Leitlinie festgelegt werden. Sie schafft organisatorische Rahmenbedingungen und sorgt für ausreichende Ressourcen um diese Ziele umsetzen zu können.



7.2 Informationssicherheitsbeauftragte oder Informationssicherheitsbeauftragter des MSB (Ressort-CISO)

Die oder der Ressort-CISO („Chief Information Security Officer“) koordiniert den Informationssicherheitsprozess im MSB sowie dem Geschäftsbereich und unterstützt die bzw. den NRW-CISO in allen Fragen der Informationssicherheit, insbesondere bei der Erstellung von Berichten zur Informationssicherheit. Sie oder er verfügt über ausreichendes Wissen und Erfahrung auf dem Gebiet der Informationssicherheit und Informationstechnologie bzw. eignet sich dies in angemessener Zeit an.

Die oder der Ressort-CISO ist für alle Fragen im Zusammenhang mit der Informationssicherheit im Geschäftsbereich des MSB zuständig, sie oder er berät und unterstützt die Leitung des MSB in allen Angelegenheiten der Informationssicherheit. Sie oder er ist über alle für die Informationssicherheit relevanten Themen und Veränderungen, die übergreifend den Geschäftsbereich des MSB betreffen, unaufgefordert, frühzeitig und umfassend zu unterrichten. Auf Nachfrage kann sie oder er sich insoweit jederzeit umfassend informieren lassen.

7.3 Informationssicherheitsbeauftragte (ISB)

In den Behörden und Einrichtungen (bzw. in einer Sicherheitsdomäne³) kann von der Leitung jeweils eine (behördliche) Informationssicherheitsbeauftragte oder ein (behördlicher) Informationssicherheitsbeauftragter (ISB) benannt werden. Solange keine Benennung erfolgt, wird die Aufgabe unmittelbar von der jeweiligen Leitung wahrgenommen.

Die oder der Ressort-CISO des MSB kann gleichzeitig zu der oder dem behördlichen Informationssicherheitsbeauftragten benannt werden.

Die behördlichen Informationssicherheitsbeauftragten koordinieren den Informationssicherheitsprozess in der jeweiligen Behörde und informieren direkt die oder den Ressort-CISO über sicherheitsrelevante Vorkommnisse. Die oder der ISB ist für alle Fragen im Zusammenhang mit der Informationssicherheit in der jeweiligen Behörde oder Einrichtung (bzw. Sicherheitsdomäne) zuständig, sie oder er berät und unterstützt die Behördenleitung in allen Angelegenheiten der Informationssicherheit. Sie oder er ist über alle für die Informationssicherheit relevanten Themen und Veränderungen unaufgefordert, frühzeitig und umfassend zu unterrichten. Auf Nachfrage kann sie oder er sich insoweit jederzeit umfassend informieren lassen. Dies gilt unter anderem für die Erstellung und Einführung von Web-Verfahren, Hard- und Software sowie anderen Verfahren bei denen dienstliche Informationen, auch im Auftrag durch Dritte, verarbeitet werden.

³ Als Sicherheitsdomäne wird dabei ein logisch, organisatorisch oder räumlich zusammengehöriger Bereich mit einheitlichen Sicherheitsanforderungen und/oder einheitlicher Sicherheitsadministration bezeichnet. Dies ist in der Regel eine Behörde, eine Einrichtung oder Sondervermögen, kann aber auch mehrere Behörden, Einrichtungen oder Sondervermögen umfassen.



Bei direkter Kommunikation mit dem CERT NRW im Notfall binden sie die oder den Ressort-CISO nachrichtlich in die Kommunikation ein oder informieren zeitnah im Nachgang.

7.4 Informationssicherheitsmanagement-Gremium des MSB (ISMG MSB)

Im Geschäftsbereich des MSB wird ein Informationssicherheitsmanagement-Gremium (ISMG MSB) gebildet, welches sich zusammensetzt aus

- der oder dem Ressort-CISO (Vorsitz),
- den behördlichen Informationssicherheitsbeauftragten (ISB) des Ressorts,

als ständige Mitglieder sowie – soweit eine Fachanwendung betroffen ist – mindestens einem von der oder dem Ressort-CISO zugezogenen Vertretung der betroffenen Fachreferate bzw. der fachlich zuständigen Stelle als nichtständiges Mitglied.

Die bzw. der Datenschutzbeauftragte des MSB die bzw. der Geheimschutzbeauftragte des MSB sowie Beschäftigte des IT-Dienstleisters des MSB oder andere externe Dienstleister sind bei Bedarf hinzuzuziehen.

Mitglieder der jeweils zuständigen Personalvertretungen werden eingeladen, wenn dies im Sinne einer vertrauensvollen Zusammenarbeit oder aus personalvertretungsrechtlichen Gründen angezeigt ist.

Das Gremium erarbeitet und berät anlassbezogen ressortspezifische Regelungen, Konzepte und Richtlinien zur Verbesserung der Informationssicherheit. Das ISMG MSB unterstützt dabei die oder den Ressort-CISO bei der Wahrnehmung ihrer oder seiner Aufgaben.

Die oder der Ressort-CISO berichtet im ISMG über alle relevanten Themen aus den Sitzungen der ressortübergreifenden Koordinierungsgruppe Informationssicherheit des Landes (KG InfoSic NRW).

8 Aktualisierung der Informationssicherheitsleitlinie

Im Rahmen des Informationssicherheitsprozesses überprüft die oder der Ressort-CISO diese Leitlinie jeweils nach spätestens fünf Jahren auf ihre Aktualität und initiiert ggf. eine Anpassung. Im Falle einer grundlegenden organisatorischen Veränderung ist eine zeitnahe Anpassung der Informationssicherheitsleitlinie vorzunehmen.



9 Inkraftsetzung und Veröffentlichung

Die vorliegende Informationssicherheitsleitlinie tritt am 29.10.2018 in Kraft. Sie wird im Amtsblatt veröffentlicht.

Diese Richtlinie wurde am 07.11.2022 zuletzt aktualisiert.

Ministerin Dorothee Feller