MINDESTANFORDERUNGEN AN DIE INFORMATIONS-SICHERHEIT DER KOMMUNEN IN NRW

Handreichung
der kommunalen Spitzenverbände NRW
und des Dachverbandes kommunaler IT-Dienstleister in NRW (KDN)

STÄDTETAG NRW

LANDKREISTAG NORDRHEIN-WESTFALEN

Kommunen.NRW
Städte- und Gemeindebund Nordrhein-Westfalen

KDN

Handreichung
Mindestanforderungen an die Informationssicherheit der Kommunen in NRW

Management Summary

Informationssicherheit ist eine rechtlich gebotene Kernaufgabe und unverzichtbare Grundlage für die dauerhafte Handlungsfähigkeit der Kommunen in Nordrhein-Westfalen. Die Handreichung „Mindestanforderungen an die Informationssicherheit der Kommunen in NRW“ schafft hierfür einen verbindlichen und praxisnahen Orientierungsrahmen.

Angesichts zunehmender Cyberbedrohungen, wachsender IT-Komplexität und hoher Abhängigkeit kommunaler Prozesse von digitalen Infrastrukturen ist ein angemessenes Sicherheitsniveau zwingend erforderlich. Der gemeinsame IT-Lenkungsausschuss der kommunalen Spitzenverbände in NRW hat daher organisatorische und technische Mindestanforderungen definiert. Ziel ist es, kommunalen Handlungsbedarf systematisch zu identifizieren und ein flächendeckendes, belastbares Sicherheitsniveau sicherzustellen.

Informationssicherheit ist als strategische, ressortübergreifende Querschnittsaufgabe zu verankern, mit klaren Zuständigkeiten, ausreichenden Ressourcen und kontinuierlicher Steuerung. Orientierung bietet insbesondere der IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI), einschließlich des kommunalen Grundschutzprofils und der WiBA-Checklisten als Einstieg in die Basis-Absicherung.

Zu den organisatorischen Mindestanforderungen zählen die Einführung eines Informationssicherheits-Managementsystems (ISMS), eine verbindliche Informationssicherheitsleitlinie, die Benennung einer für die Umsetzung von Informationssicherheit beauftragten Person (ISB), regelmäßige Sensibilisierungs- und Schulungsmaßnahmen sowie ein strukturiertes und regelmäßig geübtes IT-Notfallmanagement. Technisch werden unter anderem verpflichtende Multifaktor-Authentifizierung bei externen Zugriffen, klare Passwortvorgaben, der Einsatz moderner EDR/XDR-Lösungen, Netzwerksegmentierung sowie regelmäßige Schwachstellenscans gefordert.

Die Handreichung versteht sich als Mindeststandard und Einstieg in eine kontinuierliche Weiterentwicklung der Informationssicherheit. Nur durch eine konsequente strukturelle Verankerung und die aktive Mitwirkung aller Ebenen kann die kommunale IT wirksam geschützt, die Daseinsvorsorge gesichert und das Vertrauen der Bürgerinnen und Bürger dauerhaft erhalten werden.

Informationssicherheit in der Verwaltung als Grundvoraussetzung für kommunales Handeln

Informationssicherheit ist eine grundlegende Voraussetzung für funktionsfähiges kommunales Handeln. Ein Kernaspekt des täglichen Verwaltungsgeschäfts ist dabei die strukturierte Daten- und Informationsverarbeitung rund um verwaltungsinterne Abläufe sowie die Belange der Bürgerinnen und Bürger. Diese Informationsverarbeitung erfolgt in der Regel über erlernte Routinen der Mitarbeitenden bzw. in IT-Systemen hinterlegte Prozesse. Dringen Unbefugte – seien es Kriminelle oder staatliche Akteure – in die Systeme ein, hat dies weitreichende Folgen. Betroffen sind die mitunter sensiblen persönlichen Daten der Bürgerinnen und Bürger, geschützte Unternehmensdaten, Daten zu Mitarbeitenden in der Verwaltung oder gar der (kritischen) Infrastruktur der Kommune bzw. den Einrichtungen der Kommunalverwaltung.

Die Gesamtverantwortung für die Informationssicherheit liegt bei der Verwaltungsspitze, die die strategischen Vorgaben bestimmt, geeignete organisatorische Rahmenbedingungen schafft, die erforderlichen Ressourcen bereitstellt und auch bei einer Aufgabenübertragung verantwortlich bleibt. Informationssicherheit ist dabei als ressort- und einheitenübergreifende Querschnittsaufgabe ausgestaltet, die ein angemessenes Sicherheitsniveau nur durch einen kontinuierlichen Austausch und eine enge Zusammenarbeit zwischen Kommunen, kommunalen IT-Dienstleistern, die ihre fachliche Expertise zur beratenden und unterstützenden Begleitung der Kommunalverwaltungen einbringen, sowie den zuständigen Stellen von Land und Bund erreichen kann. In jeder Kommune ist aber die Verwaltungsspitze gefordert, aufgrund der oben genannten Erwartungen an eine funktionierende kommunale IT die Gefährdungslage ernst zu nehmen und dem Thema Informationssicherheit konsequent die nötige Priorität für die hausinternen Prozesse einzuräumen.

Die digitale Infrastruktur der Kommunalverwaltung umfasst nicht zuletzt auch Passwörter, Verträge und vertrauliche Ratsbeschlüsse. Kommt es zu einem Verlust oder Missbrauch solcher Informationen, kann das erheblichen, mitunter irreparablen Schaden verursachen und vor allem das Vertrauen in demokratische Institutionen nachhaltig beeinträchtigen. Mit wachsender IT-Komplexität, zunehmender Vernetzung und gleichzeitig steigenden Cyberbedrohungen von Kriminellen, aber auch staatlichen Akteuren, nimmt die Notwendigkeit der Kommunen erheblich zu, sichere IT-Systeme einzusetzen. Ohne ein angemessenes Sicherheitsniveau sind eine verlässliche Verwaltungsarbeit, eine erfolgreiche Digitalisierung sowie die Erfüllung der kommunalen Daseinsvorsorge nicht gewährleistet.

Der gemeinsame IT-Lenkungsausschuss der kommunalen Spitzenverbände hat in seiner Sitzung vom 17. Januar 2025 auf Grundlage der Ergebnisse des landesseitigen IT-Sicherheitschecks „B-Hard“ beschlossen, praxistaugliche Mindestanforderungen an die kommunale IT-Sicherheit zu entwickeln. Vor diesem Hintergrund soll das vorliegende Papier eine

Orientierung für die kommunale Praxis bieten und gleichzeitig motivieren, das IT-Sicherheitsniveau stetig zu verbessern. Die dargestellten organisatorischen und technischen Mindestanforderungen dienen als erste Rahmensetzung zur Identifizierung kommunalen Handlungsbedarfs und zur Ableitung erforderlicher Maßnahmen.

Ergänzende Hinweise sowie Unterstützung bei der Umsetzung der Mindestanforderungen an die Informationssicherheit in den Kommunen ergeben sich aus den im Anhang benannten Veröffentlichungen.

Die vorliegende Handreichung adressiert Kommunen und kommunale IT-Dienstleister in NRW.

Mindestanforderungen an die Informationssicherheit der Kommunen

Die folgenden Anforderungen orientieren sich u.a. am IT-Grundschutz-Profil „Basis-Absicherung Kommunalverwaltung“, erstellt von der AG kommunale Basis-Absicherung in Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und sind in organisatorische und technische Maßnahmen unterteilt. Der BSI IT-Grundschutz richtet sich explizit an Behörden und öffentliche Stellen, also auch an Kommunalverwaltungen. Als zentrale Cybersicherheitsbehörde des Bundes definiert das BSI verbindliche Standards für den öffentlichen Sektor. Für Kommunen bedeutet es, dass die Orientierung am BSI IT-Grundschutz sowohl die Einhaltung gesetzlicher Anforderungen sicherstellt als auch Haftungsrisiken reduziert. Das o. g. IT-Grundschutz-Profil sowie die sog. „WiBA-Checklisten“ (Weg in die Basis-Absicherung – WiBA) bieten einen praxisnahen Einstieg, der speziell auf die Bedürfnisse und Ressourcenlagen kommunaler Verwaltungen zugeschnitten ist. Aus diesem Grund sind die genannten Veröffentlichungen idealer Ausgangspunkt für die Anforderungen aus diesem Papier, sodass die beschriebenen Mindestanforderungen nach Erfüllung dann durch weitergehende Maßnahmen aus dem BSI IT-Grundschutz fließend ergänzt werden können.

Organisatorische Maßnahmen zur Informationssicherheit

Die organisatorische Stärkung der Informationssicherheit erfordert einen verbindlichen Rahmen mit klaren Strukturen, Zuständigkeiten, Informationssicherheitsmanagement, strategischer Leitlinie, koordinierender Ansprechperson und fortlaufender Sensibilisierung der Mitarbeitenden.

Einführung eines Informationssicherheits-Managementsystem (ISMS) nach BSI IT-Grundschutz

- **Umsetzung:** Ein ISMS ist aufzubauen. Der Einstieg kann über die WiBA-Checklisten oder das IT-Grundschutz-Profil „Basis-Absicherung Kommunalverwaltung“ erfolgen. → relevante Bausteine im BSI IT-Grundschutz: ORP.1, ORP.2, ORP.3

- **Begründung:** Ein ISMS ermöglicht es, Informationssicherheit strukturiert, nachvollziehbar und kontinuierlich zu verbessern. Es hilft, Risiken systematisch zu identifizieren und zu steuern und ist damit ein zentrales Instrument zur Vermeidung von Organisationsverschulden.

Informationssicherheitsleitlinie

- **Umsetzung:** Jede Verwaltung sollte eine gültige Leitlinie zur Informationssicherheit haben, die Ziele, Verantwortlichkeiten und Maßnahmen zur Prävention und Nachsorge definiert. → relevante Anforderung aus dem BSI IT-Grundschutz: ISMS.1.A3, ORP.1.A2

- **Begründung:** Eine verbindliche Leitlinie schafft Klarheit über die Erwartungen und Pflichten aller Beteiligten. Sie ist Grundlage für ein systematisches Sicherheitsmanagement und erhöht die Verbindlichkeit der Maßnahmen. Sie stellt den Einstieg in die Informationssicherheit dar.

Benennung eines Ansprechpartners für Informationssicherheit

- **Umsetzung:** Eine für die Umsetzung von Informationssicherheit beauftragte Person (Informationssicherheitsbeauftragte/r, ISB) muss benannt werden. Sofern diese Person daneben weitere Aufgaben übernehmen soll, ist die Stelle auskömmlich im Sinne der Informationssicherheitsaufgaben zu bewerten, um der Praxis vorzubeugen, keine Zeitanteile zum Ausfüllen der Rolle zur Verfügung zu stellen. Die Ansprechperson sollte über Erfahrungen im IT-Sicherheitsbereich verfügen und mit entsprechenden Zugriffs- bzw. Durchgriffsrechten ausgestattet werden. Der/Die ISB kann nur im Rahmen einer

aktiven Mitwirkung aller Bereiche wirksam handeln. → relevante Anforderungen aus dem BSI IT-Grundschutz: ORP.1.A1, ISMS.1.A4

- **Begründung:** Eine klar benannte Ansprechperson mit ausreichendem Stellenanteil und unmittelbarem Vortragsrecht bei der Hausspitze stellt sicher, dass das Thema kontinuierlich in der Verwaltung betrachtet und weiterentwickelt wird. Die Verantwortung für die Umsetzung liegt jedoch weiterhin bei der Verwaltungsleitung und den jeweiligen Führungskräften.

Awareness und Schulungen

- **Umsetzung:** Alle Mitarbeitenden müssen regelmäßig an Schulungen und Sensibilisierungen zur Informationssicherheit teilnehmen Schulungen zur Informationssicherheit, Sensibilisierungen der Mitarbeitenden und regelmäßige Informationen helfen, das Sicherheitsbewusstsein zur stärken. → relevanter Baustein aus dem BSI IT-Grundschutz: ORP.3

- **Begründung:** Ein Großteil erfolgreicher Angriffe beginnt bei Anwendungsfehlern, z. B. durch das Öffnen von Anlagen oder Links in E-Mails, Chat-Tools, SMS etc. Regelmäßige Schulungen helfen, das Sicherheitsbewusstsein zu erhöhen und die Angriffsfläche zu verringern. Bei Simulationen von IT-Sicherheitsvorfällen werden Verhaltensmuster geprüft.

IT-Notfallmanagement

Das IT-Notfallmanagement bildet einen zentralen Baustein der Informationssicherheit. Es dient der Sicherstellung des Geschäftsbetriebs bei Ausfällen der Informationstechnik und definiert dafür zeitkritische Prozesse, Prioritäten und Maßnahmen. Die Verwaltungsspitze sollte über ein IT-Notfallkonzept den Rahmen für den Notbetrieb sicherstellen, während die kommunale IT-Leitung mit einem Notfallhandbuch, klaren Rollen und Schritt-für-Schritt-Abläufen sowie regelmäßigen Tests und Übungen die operative Umsetzung gewährleisten muss.

Technische Anforderungen

Technische Anforderungen zur Erhöhung der kommunalen Informationssicherheit umfassen Reduktion von Angriffsflächen, Multifaktor-Authentifizierung, starke Passwortrichtlinien, moderne Schutztechnologien, getrennte Arbeitsumgebungen (konkret z.B. XDR und Netztrennungen), Netzwerksegmentierung sowie regelmäßige Schwachstellenprüfungen zur Stärkung der Widerstandsfähigkeit, Patches und Updates.

Multifaktor-Authentifizierung (MFA) bei externen Zugängen

- **Umsetzung:** Jeder Zugriff auf das Verwaltungsnetz über VPN (o.Ä.) muss mit MFA abgesichert sein. Nur Benutzername und Passwort reichen nicht aus. → relevante Anforderungen aus dem BSI IT-Grundschutz: ORP.4.A4, OPS.1.1.2.A16 (Admins), NET.3.3

- **Begründung:** Über 80 % der erfolgreichen Angriffe auf Verwaltungsnetze beginnen mit kompromittierten Zugangsdaten – oft über ungesicherte VPN-Zugänge. Der Einsatz von MFA kann diese Angriffsfläche drastisch reduzieren, da gestohlene Passwörter allein dann nicht mehr für den Zugang ausreichen.

Passwortsicherheit

- **Umsetzung:** Passwörter müssen mindestens zwölf Zeichen lang und komplex sein. Es wird die Verwendung eines Passwortmanagers empfohlen. Es muss einen Prozess geben, der Benutzerkonten automatisch deaktiviert, wenn sie nicht mehr gebraucht werden. → relevante Anforderungen aus dem BSI IT-Grundschutz: ORP.4.A8, A22, ORP.4.A2

- **Begründung:** Schwache oder mehrfach verwendete Passwörter gehören zu den häufigsten Einfallstoren für Angreifer. Eine starke Passwortpolitik mit automatischer Deaktivierung inaktiver Konten verhindert, dass veraltete oder kompromittierte Zugangsdaten ausgenutzt werden.

EDR/XDR statt klassischem Virenschutz

- **Umsetzung:** Klassische Antivirenlösungen sollen mittelfristig durch moderne Technologien wie EDR/XDR ersetzt werden. → relevante Anforderungen aus dem BSI IT-Grundschutz: OPS.1.1.4

- **Begründung:** Klassische Virenscanner erkennen viele moderne Angriffe nicht mehr zuverlässig. EDR/XDR-Lösungen analysieren das Verhalten von Systemen und erkennen auch unbekannte oder gezielt entwickelte Schadsoftware – ein entscheidender Vorteil bei gezielten Angriffen auf Verwaltungen.

Tiering-Modell für Administration

- **Umsetzung:** Server, Active Directory (AD) und Netzwerke dürfen nur von speziellen Admin-Workstations („Jump-Hosts“) verwaltet werden. Eine Administration von normalen Arbeitsplätzen aus ist zu unterbinden. Ziel: Langfristig zentrale AD-Administration. → relevanter Baustein aus dem BSI IT-Grundschutz: OPS.1.1.2

- **Begründung:** Angreifer steuern gezielt administrative Konten an, um sich schnell weitreichende Rechte zu verschaffen. Durch die Trennung von Admin- und Benutzerarbeitsplätzen (Jump-Hosts) wird die sogenannte „Laterale Bewegung“ im Netzwerk massiv erschwert.

Netzsegmentierung

- **Umsetzung:** Verwaltungsnetze müssen logisch oder physisch voneinander getrennt sein, um Angriffsflächen zu minimieren. → relevante Anforderungen aus dem BSI IT-Grundschutz: NET.1.1

- **Begründung:** Durch die Segmentierung von Netzen wird verhindert, dass sich ein Angreifer nach einem erfolgreich verschafften Zugriffungehindert im gesamten Verwaltungsnetz bewegen kann. Das reduziert die Auswirkungen eines Angriffs erheblich.

Regelmäßige Schwachstellenscans

- **Umsetzung:** Die IT-Infrastruktur muss regelmäßig auf Schwachstellen geprüft werden. Ergebnisse sind der Verwaltungsleitung vorzulegen und müssen bearbeitet werden. → relevante Anforderungen aus dem BSI IT-Grundschutz: ISMS.1.A12, DER.1.A3

- **Begründung:** Viele Angriffe nutzen bekannte Schwachstellen, für die längst Updates verfügbar wären. Regelmäßige Scans helfen, diese Lücken frühzeitig zu erkennen und zu schließen – bevor sie ausgenutzt werden können.

Fazit

Informationssicherheit ist eine rechtlich gebotene Kernaufgabe. Sie muss strukturell verankert, gesteuert, fortlaufend angepasst und verantwortet werden und beginnt bei der Verwaltungsspitze. Sie kann nur gelingen, wenn alle Bereiche und Ebenen der Verwaltung Verantwortung übernehmen und aktiv mitwirken. Informationssicherheit ist kein technisches Randthema, sondern eine strategische Querschnittsaufgabe, die in Prozessen, Strukturen und im täglichen Handeln verankert sein muss. Nur wenn sie als gemeinsame und kontinuierliche Aufgabe verstanden und gelebt wird, können die Kommunen und ihre IT-Dienstleister den wachsenden Bedrohungen wirksam begegnen, ihre Handlungsfähigkeit sichern und das Vertrauen der Bürgerinnen und Bürger sichern und erhalten.

Anhang

Weg in die Basis-Absicherung (WiBA)
↗ https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/WIBA/Weg_in_die_Basis_Absicherung_WiBA.html

IT-Grundschutz-Kompendium
↗ https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium/IT_Grundschutz_Kompendium_Edition2023.pdf?__blob=publicationFile&v=4#download=1

Handreichung zur Ausgestaltung der Informationssicherheitsleitlinie in Kommunalverwaltungen
↗ https://www.staedtetag.de/files/dst/docs/Themen/2024/Handreichung-ISLL-2024.pdf

IT-Grundschutz-Profil „Basis-Absicherung Kommunalverwaltung“
↗ https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Profile/Basis_Absicherung_Kommunalverwaltung.pdf?__blob=publicationFile&v=12

BSI IT-Grundschutz Standard 200-2
↗ https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_2.pdf?__blob=publicationFile&v=2

Weitere Hinweise auf relevante Leitfäden, Handreichung oder Checklisten erhalten Sie beim BSI:

Bundesamt für Sicherheit in der Informationstechnik
Referat I 12 Umsetzungsberatungsberatung – Länder und Kommunen
Kontakt: sicherheitsberatung-regional@bsi.bund.de

Autorenschaft

Die vorliegende Handreichung wurde von der AG Kommunale Mindestanforderungen für Informationssicherheit in Nordrhein-Westfalen erarbeitet:

Karim Ahajliu, LKT NRW
Stanislaw Chernin, StGB NRW
Marianne Grofe-Juhlke, Stadt Krefeld
Philip Hannack, Kreis Soest
Michael Harmann, SIT NRW
Patrick Lawitzky, Stadt Würselen
Bernd Lehmann, Kreisstadt Siegburg
Johannes Osing, StGB NRW
Dirk Saphörster, Kreis Warendorf
Tobias Scherbaum, Stadt Oberhausen
Michael Schuchardt, KDN
Hanna Sommer, Städtetag NRW
Thomas Stasch, regio iT
Simon Üffing, KAAW
Christian Völz, KDVZ Rhein-Erft-Rur
Christian von Grone, SIT NRW
Dirk Wallenstein, kdvz Rhein-Erft-Ruhr
Horst Weiner, Rhein-Kreis Neuss (Sitzungsleitung)

Besonderer Dank gilt Herrn Thomas Stasch von der regio IT für den Entwurf und seine breite fachliche Expertise sowie Herrn Weiner für die ergebnisreiche Leitung der Sitzungen. Unser Dank gilt ebenso dem BSI für die wertvollen Überarbeitungshinweise.

Beschlossen vom

Gemeinsamen IT-Lenkungsausschuss der kommunalen Spitzenverbände in Nordrhein-Westfalen am 18. Juni 2026

Vorstand des Städtetages Nordrhein-Westfalen am 9. September 2026

KONTAKT

Städtetag NRW
Dr. Hanna Sommer
hanna.sommer@staedtetag.de
www.staedtetag-nrw.de

Landkreistag NRW
Karim Ahajliu
k.ahajliu@lkt-nrw.de
www.landkreistag-nrw.de

Städte- und Gemeindebund NRW
Dr. Stanislaw Chernin
stanislaw.chernin@kommunen.nrw
www.kommunen.nrw

KDN
Kerstin Pliquett
kerstin.pliquett@kdn.de
www.kdn.de

Titelbild: Irene – stock.adobe.com