

Landeshauptstadt Dresden



# Informationssicherheitsleitlinie

Für die Landeshauptstadt Dresden

## Versionsnachweis

Version	Änderungs-Datum	Bearbeiter	Bemerkung
0.9	15.06.2023	ISMS Projektteam	Erstellung und Abstimmung Initialentwurf
1.0	08.08.2023	Erik Zimmermann	Beschlussfassung DB OB

Landeshauptstadt Dresden  
Postfach 12 00 20  
01001 Dresden

Telefon (03 51) 4 88 0  
E-Mail [stadtverwaltung@dresden.de](mailto:stadtverwaltung@dresden.de)  
DE-Mail [stadtverwaltung@dresden.de-mail.de](mailto:stadtverwaltung@dresden.de-mail.de)  
Homepage <https://www.dresden.de/>



# Inhalt

<b>1</b>	<b>Präambel</b>	<b>4</b>
<b>2</b>	<b>Geltungsbereich</b>	<b>5</b>
<b>3</b>	<b>Stellenwert der Informationssicherheit</b>	<b>5</b>
<b>4</b>	<b>Ziele der Informationssicherheit</b>	<b>6</b>
<b>5</b>	<b>Kernelemente der Informationssicherheitsstrategie</b>	<b>7</b>
<b>6</b>	<b>Rollen der Informationssicherheit</b>	<b>9</b>
<b>7</b>	<b>Verpflichtung zur Umsetzung</b>	<b>10</b>
<b>8</b>	<b>Kontinuierlicher Verbesserungsprozess</b>	<b>11</b>
<b>9</b>	<b>Inkraftsetzung</b>	<b>12</b>

# 1 Präambel

Der/die Oberbürgermeister/in erlässt gemeinsam mit den Beigeordneten die vorliegende Informationssicherheitsleitlinie als Basis zur Informationssicherheit und zentraler Bestandteil eines Informationssicherheitsmanagementsystems (ISMS). Mit dieser Informationssicherheitsleitlinie bekennt sich die Landeshauptstadt Dresden zur Errichtung und kontinuierlichen Fortschreibung eines ISMS. Die Informationssicherheitsleitlinie definiert dabei die Grundlagen für die Organisation und den Betrieb des ISMS für die gesamte Landeshauptstadt Dresden, unter Beachtung des Sächsischen Informationssicherheitsgesetzes (SächsISichG). Sie beschreibt unter anderem

- den Geltungsbereich des ISMS der Stadtverwaltung,
- den Stellenwert der Informationssicherheit,
- die Ziele des ISMS der Landeshauptstadt Dresden
- die Kernelemente der Informationssicherheitsstrategie der Stadtverwaltung,
- die wesentlichen Rollen der Sicherheitsorganisation,
- das Bekenntnis des/der Oberbürgermeisters/Oberbürgermeisterin zu seiner/ihrer Gesamtverantwortung für die Informationssicherheit,
- sowie die Verpflichtung zur kontinuierlichen Fortschreibung und Verbesserung des Sicherheitsprozesses.

## 2 Geltungsbereich

Die Informationssicherheitsleitlinie gilt für alle Organisationseinheiten der Landeshauptstadt Dresden sowie deren Eigenbetriebe, die die zentralen IT-Infrastrukturkomponenten der LHD nutzen und für alle Organisationseinheiten und Eigenbetriebe, die keine zentralen IT-Infrastrukturkomponenten der LHD nutzen und kein eigenes ISMS, auf Basis anerkannter Standards, vorhalten und nachweisen können. Wenn ein eigenes ISMS vorgehalten wird, ist die Zusammenwirkung mit dem Beauftragten für Informationssicherheit (BfIS) der LHD verpflichtend, um ein überspannendes Informationssicherheitsniveau zu gewährleisten.

Die Informationssicherheitsleitlinie und die daraus resultierenden internen Verwaltungsvorschriften und Maßnahmen, sind von allen Beschäftigten der Landeshauptstadt Dresden sowie verpflichteten Dritten wie z.B. Auftragnehmern, Lieferanten und Herstellern zu beachten und einzuhalten. Maßnahmen und Regelungen können auf Grundlage der Informationssicherheitsleitlinie, den BSI-Standards 200-1, 200-2, 200-3, 200-4 und dem BSI IT-Grundschutz Compendium in internen Verwaltungsvorschriften geregelt werden.

## 3 Stellenwert der Informationssicherheit

Die Landeshauptstadt Dresden besitzt eine enorme Aufgabenvielfalt die permanenten Änderungen unterliegt. Aufgaben, Prozesse und die Aufbauorganisation befinden sich in einem stetigen Wandel und erfordern jeweils eine Anpassung der technischen Möglichkeiten.

In Abwägung der zu schützenden Werte, der gesetzlichen Anforderungen sowie effizienter und ressourcenschonender Aufgabenerledigung und der damit verbundenen Risiken ist dabei ein angemessenes Informationssicherheitsniveau zu schaffen.

Ein modernes Verwaltungshandeln erfordert den Einsatz aktueller Informationstechnologien um die effiziente und effektive Aufgabenerfüllung der Stadtverwaltung im Sinne der Bürgerinnen und Bürger, ortsansässiger Unternehmen oder weiterer Partner sicherzustellen.

Beim Einsatz von Informationstechnologie muss die Landeshauptstadt Dresden darauf achten, dass der Sensibilität, der ihr übertragenen und von ihr verarbeiteten Informationen mit der nötigen Sorgfalt Rechnung getragen wird. Deshalb muss die Informationssicherheit grundlegend bei dem Verwaltungshandeln beachtet und berücksichtigt werden.

# 4 Ziele der Informationssicherheit

Die Ziele der Informationssicherheit für die Landeshauptstadt Dresden leiten sich aus diversen Faktoren ab. Wesentlichste sind, die weitreichende und fortschreitende Digitalisierung im Allgemeinen sowie die damit verbundenen Anpassungen rechtlicher Rahmenbedingungen bspw. durch das IT-Sicherheitsgesetz 2.0 des Bundes oder dem Gesetz zur Gewährleistung der Informationssicherheit im Freistaat Sachsen (SächsISichG) aber auch hinsichtlich bestehender Verwaltungsziele. Diese Ziele – auch für die Informationssicherheit der Landeshauptstadt Dresden – leiten sich unter anderem aus dem Organisationsentwicklungskonzept (OEK) ab und sollen dessen ungehinderte Umsetzung ermöglichen.

Zu den Zielen des OEK gehören:

- Vernetzte und ermöglichende Verwaltung,
- Bürgernahe und digitale Verwaltung,
- Attraktiver und qualifizierender Arbeitgeber.

Informationssicherheit umfasst die Summe aller organisatorischen, personellen und technischen Maßnahmen, um diese Ziele zu erreichen. Dabei ist es notwendig das Zusammenspiel der Informationen, IT-Fachverfahren, Aufgaben sowie der Infrastruktur der Informationstechnik und Kommunikationskanäle ganzheitlich zu betrachten.

Die Informationssicherheit umfasst den Schutz sämtlicher Informationen jeglicher Art und Herkunft, unabhängig davon, ob sie auf Papier oder digital gespeichert sind. Für den geeigneten Schutz der Informationen sind insbesondere die drei Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit von Informationen durch angemessene Maßnahmen zu gewährleisten.

Vertraulichkeit:

- Zugang zu Informationen nur für Befugte
  - Es gibt klar festgelegte Berechtigungen, welche Personen auf welche Informationen (z.B. sensible Daten, persönliche Informationen, Verschlusssachen) zugreifen dürfen.

Integrität:

- Unversehrtheit und Korrektheit von Informationen
  - Die Informationen sind vollständig und richtig; unautorisierte Änderungen gespeicherter oder übertragener Daten werden ausgeschlossen bzw. erkannt.

Verfügbarkeit:

- Informationen bei Bedarf bereitstellen
  - IT-Systeme, Anwendungen und Informationen sind verfügbar, wenn sie gebraucht werden.

Jede Leistung, Aufgabe oder Information wird entsprechend ihres Schutzbedarfes eingestuft, dessen Feststellung im Rahmen einer Sicherheitskonzeption erfolgt. Aus der Einstufung ergeben sich die Anforderungen zum Erhalt der drei genannten Schutzziele.

Geeignete Sicherheitsmaßnahmen müssen dafür Sorge tragen, dass die Sicherheit von Informationen entsprechend ihres Schutzbedarfs in Hinblick auf die Sicherheitsziele sowie unter Berücksichtigung rechtlicher Bestimmungen, gewährleistet wird. Um dies zu erreichen, ist es unabdingbar, den Schutzbedarf der Informationen zu kennen und die passenden Maßnahmen zu ergreifen.

Die Betrachtung weiterer Schutzziele kann je nach Aufgabe, Projekt oder Fachanforderung definiert werden (z.B. Authentizität, Revisionsfähigkeit, Transparenz).

# 5 Kernelemente der Informationssicherheitsstrategie

Die vorliegende Informationssicherheitsleitlinie gibt den Rahmen für das Management der Informationssicherheit in der Landeshauptstadt Dresden vor. Ein wesentliches Kernelement ist hierbei die Etablierung eines geeigneten Werkzeugs zur Steuerung.

Daher muss das ISMS als kontinuierlicher Verbesserungsprozess implementiert werden, welcher die vier Schritte des PDCA-Zyklus beinhaltet:

- Planung (Plan): Festlegung der Vorgaben für den Sicherheitsprozess und das ISMS,
- Umsetzung (Do): Aufbau eines ISMS, Erstellung und Umsetzung eines Sicherheitskonzeptes sowie Etablierung eines Sicherheitsprozesses,
- Überprüfung (Check): Erfolgskontrolle der Erreichung der Sicherheitsziele,
- Aufrechterhaltung (Act): Durchführung von Korrekturen zur Optimierung des Sicherheitsprozesses und der Sicherheitsorganisation.



Abbildung 1: PDCA-Zyklus

Das angestrebte Sicherheitsniveau der einzelnen Organisationseinheiten und Eigenbetriebe der Landeshauptstadt Dresden orientiert sich hierbei wesentlich am BSI-Standard 200-2, sowie der IT-Grundschutz-Methodik.

In Referenz auf die IT-Grundschutz-Methodik wird zur Umsetzung der Informationssicherheit folgende Dreiteilung vorgenommen, welche sich auf die Größe und Kritikalität der zu sichernden Organisationseinheiten beruft.

## Basis-Absicherung

- Organisationseinheiten und Eigenbetriebe mit „niedriger“ oder „mittlerer“ Kritikalität

## Standard-Absicherung

- Bereiche deren Kritikalität als „hoch“ oder „unabdingbar“ eingestuft wurde

### Kern-Absicherung

- bei erhöhtem Schutzbedarf für einzelne Verfahren unter Betrachtung der Anforderungen
- nicht vorgesehen für gesamte Organisationseinheiten oder Eigenbetriebe

Ziel der Informationssicherheitsstrategie der Landeshauptstadt Dresden ist es, ein der jeweiligen Bedarfslage angemessenes Sicherheitsniveau zu erreichen und aufrechtzuerhalten.

Die Landeshauptstadt Dresden führt dazu Bedarfsermittlungen durch und legt die Mindestsicherheitsstandards für die eingesetzten Verfahren fest. Bei behördenübergreifenden Verfahren sind die entsprechenden Festlegungen des Bundes oder des Landes und ggf. weiterer Dritter (z. B. Träger der Sozialversicherung wie Krankenkassen oder Rentenkasse) umzusetzen. Die Informationssicherheitsleitlinie ist dabei bedarfsgerecht fortzuschreiben.

Weitere Eckpunkte und Kernelemente der Strategie zur Informationssicherheit sind:

- Verankerung des Themas Informationssicherheit in der Organisation über eine geeignete Informationssicherheits-Organisation, die aktiv das Thema Informationssicherheit betreibt und ausreichend finanzielle und personelle Ressourcen sowie die notwendige zeitliche Kapazität zur Verfügung gestellt bekommt,
- klar formulierte Sicherheitsvorgaben, die für alle Beschäftigten verbindlich sind,
- die weitere, kontinuierliche und stets zu überprüfende Integration von Sicherheitsaspekten in alle aus Sicht der Informationssicherheit relevanten Prozesse,
- kontinuierliche und flächendeckende Sensibilisierungsmaßnahmen für alle Beschäftigten,
- Mitberücksichtigung der Informationssicherheit bei Änderungen und Neuerungen (bspw. Beschaffungen, Einführung von Verfahren, Zugangsberechtigungen) von Beginn an,
- sukzessive Absicherung der IT-Infrastruktur(en) durch Umsetzung geeigneter Sicherheitsmaßnahmen auf der Infrastrukturebene,
- Orientierung und Rücksichtnahme bei allen Aktivitäten zur Informationssicherheit an den aktuellen Standards und Best Practices.

Die Sicherheitsmaßnahmen müssen in einem wirtschaftlich vertretbaren Verhältnis zum Schaden stehen, der durch Sicherheitsvorfälle verursacht werden kann. Dieser definiert sich durch den Wert der zu schützenden Informationen und der IT-Systeme selbst. Zu bewerten sind die Auswirkungen auf die körperliche und seelische Unversehrtheit von Menschen, das Recht auf informationelle Selbstbestimmung, finanzielle Schäden, Beeinträchtigung der Aufgabenerfüllung, Schädigung des Ansehens der Behörde und die Folgen von Gesetzesverstößen.

Dafür sind Regelungen für ein angemessenes Risikomanagement und ein internes Kontrollsystem (IKS) zu berücksichtigen. Der/die Oberbürgermeister/in ist zu informieren, falls notwendige Sicherheitsmaßnahmen aus bestimmten Gründen nicht umgesetzt werden können.



# 6 Rollen der Informationssicherheit

Die Planung, Umsetzung, Überprüfung und Verbesserung der Informationssicherheit ist ein Prozess, der zur Feststellung des aktuellen Sicherheitsniveaus und daraus resultierenden Festlegungen von Maßnahmen führen soll.

Die Einführung und Aufrechterhaltung dieses Prozesses ist Aufgabe des/der Oberbürgermeisters/Oberbürgermeisterin. Er/sie trägt die Gesamtverantwortung für die Informationssicherheit. Zum Verantwortungsbereich zählen folgende Aufgaben:

- Schaffung organisatorischer Rahmenbedingungen zur nachhaltigen Gewährleistung von Informationssicherheit,
- Definition und Festlegung der erforderlichen Verantwortlichkeiten und Befugnisse,
- Einrichtung eines Informationssicherheits-Managements,
- Bereitstellung der erforderlichen Rechte und Finanz- und Personalressourcen, für die Planung und Umsetzung von organisatorischen, personellen, infrastrukturellen und technischen Sicherheitsmaßnahmen,
- Verankern und Durchsetzen der Informationssicherheit in die Strukturen und Arbeitsabläufe der Landeshauptstadt Dresden.

Die Einhaltung der Informationssicherheit gehört dabei zu den Dienstpflichten von allen **Beschäftigten**. Nur wenn alle eigenverantwortlich die für die Aufgabenerfüllung relevanten Gesetze, Vorschriften, Richtlinien, Dienstordnungen, Dienstanweisungen und vertraglichen Verpflichtungen beachten, kann ein geeignetes Niveau der Informationssicherheit erreicht werden.

**Führungskräfte** der Landeshauptstadt Dresden haben die Aufgabe, zu planen, zu koordinieren, anzuleiten und Beschäftigte regelmäßig über Verwaltungsvorschriften zu informieren. Sie stellen bei der Ausübung ihrer Leitungsverantwortung auch sicher, dass die Einheit der Stadtverwaltung gewahrt wird.

Zur Aufgabenbewältigung wird die Verantwortung für die laufenden Angelegenheiten zum Informationssicherheitsmanagement an mehrere Verantwortliche in der Landeshauptstadt Dresden delegiert. Insbesondere wird eine für die gesamte Stadtverwaltung zuständige, Stelle für Informationssicherheit eingerichtet.

Die bzw. der sogenannte **Beauftragte für Informationssicherheit (BfIS)** wird von der Landeshauptstadt Dresden als zentrale Sicherheitsinstanz benannt und ist zuständig für den Betrieb und die Aufrechterhaltung des Informationssicherheitsmanagementsystems. Die bzw. der BfIS ist dem/der Oberbürgermeister/in unterstellt, arbeitet fachlich weisungsfrei und ist gegenüber allen Beschäftigten fachlich weisungsbefugt, soweit Themen der Informationssicherheit betroffen sind. Die organisatorische Zuordnung des BfIS obliegt dem/der Oberbürgermeister/in. Der bzw. dem BfIS sind geeignete Qualifizierungsmaßnahmen zu ermöglichen, um ihrer bzw. seiner Verantwortung gerecht zu werden.

Zur Unterstützung der bzw. des BfIS ist ein **Informationssicherheitsmanagement-Team (ISMT)** zu gründen, welches bei strategischen Entscheidungen, bei der Bewältigung von Sicherheitsvorfällen, bei operativen Aufgaben oder Einzelmaßnahmen (z.B. bei Projekten entsprechender Größenordnung) zur Berücksichtigung der Anforderungen der Informationssicherheit mitwirkt. Das

ISMT übernimmt notwendige Aufgaben aus dem laufenden Managementsystem und definiert Maßnahmen, die unter Punkt 4 genannten Gesichtspunkte zu einem geeigneten Schutzniveau führen sollen. Das ISMT unterstützt die bzw. den BfIS bei der Umsetzung von Sicherheitsmaßnahmen in den Ämtern und Eigenbetrieben der Landeshauptstadt Dresden.

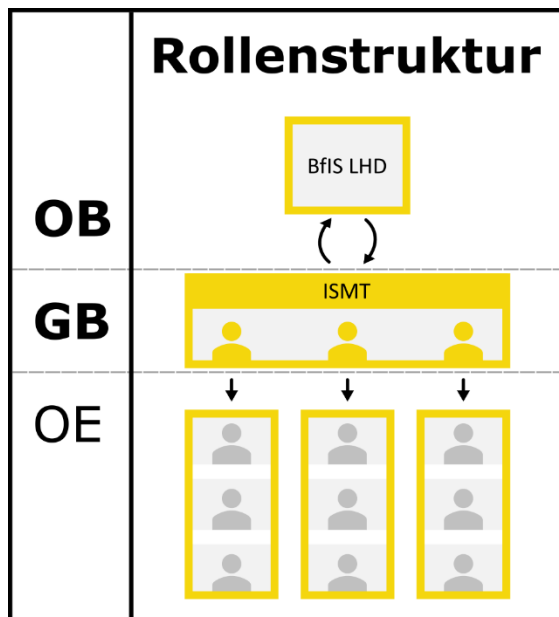


Abbildung 2: Schematische Darstellung der Rollenstruktur

## 7 Verpflichtung zur Umsetzung

Der/die Oberbürgermeister/in der Landeshauptstadt Dresden trägt die Gesamtverantwortung für die Informationssicherheit. Es obliegt ihm/ihr, für die Umsetzung der Maßnahmen zur Gewährleistung der Informationssicherheit zu sorgen und die dafür benötigten Ressourcen bereitzustellen.

Der Aufwand für die Bereitstellung von Personal- und Finanzmitteln zur Gewährleistung der Informationssicherheit dient dazu, ein angemessenes Informationssicherheitsniveau zu schaffen.

# 8 Kontinuierlicher Verbesserungsprozess

Der/die Oberbürgermeister/in als Gesamtverantwortliche/r ist regelmäßig bzw. im Einzelfall akut über den aktuellen Sicherheitszustand durch die bzw. den BfIS zu informieren, welche bzw. welcher für die Absicherung der Kontinuität des Sicherheitsprozesses verantwortlich zeichnet. Der Sicherheitsprozess umfasst den gesamten Lebenszyklus von Planung, Umsetzung, Kontrolle und Verbesserung der Informationssicherheit in einer Organisation und muss regelmäßig auf seine Aktualität, Wirksamkeit und die Übereinstimmung mit den Informationssicherheitszielen überprüft werden.

Hierbei sind getroffene Sicherheitsmaßnahmen zu steuern. Das sind alle organisatorischen, personellen, technischen oder infrastrukturellen Aktionen, die dazu dienen, Sicherheitsrisiken zu behandeln und zur Erfüllung von Sicherheitsanforderungen, welche aus gesetzlichen, vertraglichen oder internen Regelungen entstehen, mitzuwirken.

Die bzw. der BfIS ist bei allen organisatorisch-technischen Neuerungen oder Änderungen, die Auswirkungen auf die Informationssicherheit haben können, frühzeitig einzubinden. Die bzw. der BfIS hat ein unabhängiges Mitspracherecht.

Durch eine kontinuierliche Revision der Regelungen und deren Einhaltung soll das angestrebte Sicherheitsniveau dauerhaft erhalten werden. Abweichungen müssen untersucht und mit dem Ziel analysiert werden, die Informationssicherheit zu verbessern und stets aktuell zu halten.

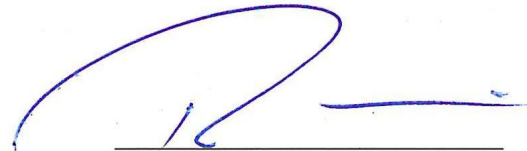
Verantwortlich für die Weiterentwicklung und Umsetzung der Informationssicherheitsleitlinie ist die bzw. der BfIS, wobei sie bzw. er von dem Informationssicherheitsmanagement-Team bestmöglich unterstützt wird. Alle Beschäftigten sind angehalten, mögliche Verbesserungen oder Schwachstellen an die entsprechenden Stellen in der Stadtverwaltung zur Informationssicherheit oder an die bzw. den BfIS weiterzugeben.

Sämtliche Regelungen in diesem Dokument sind anlassbezogen, andernfalls aber regelmäßig aller zwei Jahre auf ihre Wirksamkeit, Effektivität und Anwendbarkeit mit den vorhandenen Strukturen in der Landeshauptstadt Dresden zu prüfen.

# 9 Inkraftsetzung

Die Informationssicherheitsleitlinie tritt am 08.08.2023 in Kraft.

Dresden 20. SEP. 2023  
Ort, Datum

  
Der Oberbürgermeister