



Amtsblatt für Brandenburg

35. Jahrgang
Potsdam, den 31. Juli 2024
Nummer 30

Inhalt	Seite
--------	-------

BEKANNTMACHUNGEN DER LANDESBEHÖRDEN

Landesregierung

Leitlinie für die Informationssicherheit in der Landesverwaltung Brandenburg und der Justiz (Informationssicherheitsleitlinie)	574
--	-----

Ministerium für Wirtschaft, Arbeit und Energie

Erste Änderung der Richtlinie des Ministeriums für Wirtschaft, Arbeit und Energie über die Gewährung von Zuschüssen an kleine und mittlere Unternehmen im Land Brandenburg zur Beschäftigung von Werkstudierenden und Innovationsassistentinnen beziehungsweise Innovationsassistenten „Brandenburger Innovationsfachkräfte (BIF 2022)“	583
---	-----

Richtlinie des Ministeriums für Wirtschaft, Arbeit und Energie des Landes Brandenburg zur Förderung der Regionalen Energiemanager und Energiemanagerinnen zur Umsetzung der Regionalen Energiekonzepte (REM 2024 - 2027)	585
--	-----

Ministerium für Landwirtschaft, Umwelt und Klimaschutz

Festgesetztes Überschwemmungsgebiet der Unteren Oder mit Alter Oder, Westoder und Welse ..	587
--	-----

Der Landeswahlleiter

Wahl zum 10. Europäischen Parlament am 9. Juni 2024	587
---	-----

BEKANNTMACHUNGEN DER LANDESBETRIEBE

Landesbetrieb Straßenwesen Brandenburg, Betriebssitz Hoppegarten

Verfügung zur (Teil-)Umstufung der Landesstraße (L) 215 in der Gemeinde Templin im Landkreis Uckermark	589
--	-----

SONSTIGE BEKANNTMACHUNGEN

Ungültigkeitserklärung von Dienstaussweisen	590
---	-----

STELLENAUSSCHREIBUNGEN	590
------------------------------	-----

BEKANNTMACHUNGEN DER LANDESBEHÖRDEN

Leitlinie für die Informationssicherheit in der Landesverwaltung Brandenburg und der Justiz (Informationssicherheitsleitlinie)

Beschluss der Landesregierung
Vom 25. Juni 2024

Inhalt

- 0 Präambel
- 1 Gegenstand und Geltungsbereich
- 2 Definitionen
 - 2.1 Informationssicherheit
 - 2.2 Informationssicherheitsmanagementsystem
 - 2.3 Informationstechnik
 - 2.4 Informationseigentümerinnen oder Informationseigentümer
 - 2.5 Sicherheitsdomänen
- 3 Ziele der Informationssicherheit
- 4 Grundsätze der Sicherheitspolitik
 - 4.1 Angemessenheit von Sicherheitsmaßnahmen
 - 4.2 Bereitstellung von ausreichenden Ressourcen für die Informationssicherheit
 - 4.3 Einbindung aller Mitarbeiterinnen und Mitarbeiter in den Sicherheitsprozess
 - 4.4 Informationsklassifizierung und Informationsschutz
 - 4.5 Sicherheit der Informationssysteme während des Lebenszyklus
 - 4.6 Bildung von Sicherheitsdomänen
- 5 Rollen und Verantwortlichkeiten
 - 5.1 Dienststellenleitung
 - 5.2 Informationseigentümerinnen und Informationseigentümer
 - 5.3 Nutzerinnen und Nutzer
 - 5.4 Informationssicherheitsmanagement
- 6 Die Informationssicherheitsorganisation
 - 6.1 Informationssicherheitsmanagement-Team
 - 6.2 Die landesweite Informationssicherheitsmanagerin oder der landesweite Informationssicherheitsmanager
 - 6.3 Die Informationssicherheitsbeauftragten der Ressorts
 - 6.4 CERT
- 7 Der landesweite Sicherheitsprozess
 - 7.1 Planung des ISMS
 - 7.2 Umsetzung und Durchführung des ISMS
 - 7.3 Überwachung und Prüfung des ISMS
 - 7.4 Aufrechterhaltung und Verbesserung des ISMS
- 8 IT-Sicherheitsstandards

9 Durchsetzung

10 Schlussbestimmungen

Anlage Erläuterungen

0 Präambel

Für die Staatskanzlei, die Landesministerien und die ihnen nachgeordneten Behörden, Einrichtungen und Landesbetriebe - im Folgenden Landesverwaltung - sowie für die Gerichte, Staatsanwaltschaften und für den Justizvollzug des Landes - im Folgenden Justiz - ist die Unversehrtheit, die Verfügbarkeit und die Vertraulichkeit von Informationen von größter Bedeutung.

Maßgaben zur Informationssicherheit sind nicht nur gesetzlich vorgeschrieben, sondern auch Teil der Verpflichtungen gegenüber der parlamentarischen Kontrolle, den Aufsichtsbehörden und den Bürgerinnen und Bürgern. Jede Mitarbeiterin und jeder Mitarbeiter der Landesverwaltung und Justiz muss daher ihr und sein Handeln nach diesen Maßgaben und den daraus abgeleiteten Standards und Richtlinien ausrichten.

Jede Dienststellenleitung beziehungsweise Geschäftsführung ist verantwortlich für die Informationssicherheit in ihrem Bereich.

Bei der Erarbeitung von Richt- beziehungsweise Leitlinien zum Risikomanagement beziehungsweise zum Qualitätsmanagement in der Landesverwaltung und Justiz sind die Regelungen der Informationssicherheitsleitlinie zu berücksichtigen.

Entsprechend der Anlage zur IT-Standardisierungsrichtlinie - IT-Standards Land Brandenburg SAGA-Modul Konformität werden die Begrifflichkeiten „muss“, „sollte“, „kann“, „sollte nicht“ und „darf nicht“ verwendet. Dabei bedeuten:

- muss: Zur Erreichung von Konformität sind keine Abweichungen von verbindlichen Festlegungen zulässig.
- sollte: Unter der Angabe von nachvollziehbaren Gründen (zum Beispiel Wirtschaftlichkeit oder besondere fachliche Anforderungen) kann von positiven Empfehlungen abgewichen werden, ohne die Konformität zu verletzen.
- kann: Kennzeichnet eine gestattete konforme Option.
- sollte nicht: Unter der Angabe von nachvollziehbaren Gründen (zum Beispiel Wirtschaftlichkeit oder besondere fachliche Anforderungen) kann von negativen Empfehlungen abgewichen werden, ohne die Konformität zu verletzen.
- darf nicht: Zur Erreichung von Konformität müssen verbindliche Verbote eingehalten werden.

1 Gegenstand und Geltungsbereich

Die Informationssicherheitsleitlinie dient der Organisation der Informationssicherheit und ist ein Grundsatzdokument zum Stellenwert, zu den verbindlichen Prinzipien und dem anzustrebenden Niveau der Informationssicherheit der unmittelbaren Landesverwaltung und Justiz. Sie beschreibt den Aufbau und den Betrieb eines zentral koordinierten, ressortübergreifenden Informationssicherheitsmanagementsystems (ISMS).

Ziel des ISMS ist es, durch eine ressortübergreifende Sicherheitskoordinierung und ressortübergreifende Regelwerke die Erfüllung der Sicherheitsziele der Landesverwaltung und Justiz zu gewährleisten.

Die vorliegende Informationssicherheitsleitlinie konkretisiert die vom IT-Planungsrat verabschiedete allgemeine „Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung“ und deren Umsetzungsplanung in der jeweils geltenden Fassung.

Durch die Informationssicherheitsleitlinie soll sichergestellt werden, dass dem jeweiligen Schutzzweck angemessene und dem Stand der Technik entsprechende Sicherheitsmaßnahmen ergriffen werden, um Informationswerte und personenbezogene Daten angemessen zu schützen und um die Verfügbarkeit von informationstechnischen beziehungsweise kommunikationstechnischen Verfahren zu gewährleisten.

Die Informationssicherheitsleitlinie ist Bestandteil eines hierarchisch abgestuften Regelwerks und ist das übergeordnete Regelwerk für Informationssicherheitsrichtlinien und Informationssicherheitskonzepte der Ressorts beziehungsweise einzelner Einrichtungen.

Den besonderen verfassungsrechtlichen Rahmenbedingungen der Justiz ist Rechnung zu tragen. Der Justizgewährleistungsanspruch, die richterliche Unabhängigkeit und das Legalitätsprinzip dürfen nicht beeinträchtigt werden.

Die Informationssicherheitsleitlinie muss von allen Dienststellen der Landesverwaltung und Justiz entsprechend ihrer Aufgabenverantwortung umgesetzt und ausgestaltet werden.

Dem Landtag, dem Landesrechnungshof und der Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht und den Kommunen des Landes Brandenburg wird die Anwendung der Informationssicherheitsleitlinie empfohlen.

Bei Ebenen übergreifenden IT-Verfahren der Verwaltung ist durch die jeweilige Verfahrensverantwortliche oder den jeweiligen Verfahrensverantwortlichen der Landesverwaltung die Umsetzung der Vorgaben dieser Informationssicherheitsleitlinie sicherzustellen. Die oder der jeweilige Verfahrensverantwortliche der Landesverwaltung hat gegenüber Dritten - insbesondere Kommunen und Dienstleistern - im notwendigen Umfang auf die Beachtung der Vorgaben dieser Informationssicherheitsleitlinie hinzuwirken

und diese bei Vereinbarungen oder Verträgen zu gewährleisten.

Länderübergreifende IT-Verbünde auf Grundlage von Staatsverträgen oder Verwaltungsabkommen sind von der Regelung im Zusammenhang mit dieser Leitlinie ausgenommen, soweit die Gewährleistung der Informationssicherheit im entsprechenden Verbund geregelt wird. Das im Verbund erzielte Sicherheitsniveau darf dabei nicht hinter das in dieser Sicherheitsleitlinie beschriebene Niveau zurückfallen.

2 Definitionen

Für die Informationssicherheitsleitlinie gelten die folgenden Definitionen.

2.1 Informationssicherheit

Informationssicherheit ist die Sicherung und Aufrechterhaltung der:

- Vertraulichkeit: Gewährleistung des physikalischen beziehungsweise logischen Zugangs zu Informationen nur für die Zugriffsberechtigten,
- Integrität: Sicherstellung der Richtigkeit und Vollständigkeit von Informationen und Verarbeitungsmethoden,
- Verfügbarkeit: Gewährleistung des bedarfsorientierten Zugangs zu Informationen und zugehörigen Werten für berechtigte Benutzerinnen und Benutzer.

2.2 Informationssicherheitsmanagementsystem

Unter einem ISMS wird der Teil des gesamten Managementsystems verstanden, der auf Basis eines Geschäftsrisikoansatzes die Entwicklung, Implementierung, Durchführung, Überwachung, Überprüfung, Aufrechterhaltung und Verbesserung der Informationssicherheit abdeckt. Das Managementsystem umfasst dabei Strukturen, Richtlinien, Planungsaktivitäten, Verantwortlichkeiten, Praktiken, Verfahren, Prozesse und Ressourcen einer Organisation.

2.3 Informationstechnik

Informationstechnik (IT) im Sinne der Informationssicherheitsleitlinie umfasst alle Formen der elektronischen Informationsverarbeitung und Telekommunikation.

2.4 Informationseigentümerinnen und Informationseigentümer

Zu jedem Geschäftsprozess und jeder Fachanwendung muss eine Ansprechpartnerin oder ein Ansprechpartner benannt werden, die oder der als sogenannte Informationseigentümerin oder sogenannter Informationseigentümer für alle Fragen der Informationsverarbeitung und der Informationssicherheit im Rahmen dieses Geschäftsprozesses verantwortlich ist.

Die oder der Verantwortliche für einen Geschäftsprozess soll als Informationseigentümerin oder Informationseigentümer (siehe Nummer 5.2) sicherstellen, dass die für ihren

oder seinen Geschäftsprozess relevanten Informations-sicherheitsmaßnahmen dem Sicherheits- und Kontrollumfang der Schutzbedarfsfeststellung entsprechen.

2.5 Sicherheitsdomänen

Sicherheitsrichtlinien beziehungsweise Sicherheitskonzepte beziehen sich auf eine bestimmte Sicherheitsdomäne. Als Sicherheitsdomäne wird dabei ein logisch, organisatorisch oder räumlich zusammengehöriger Bereich mit einheitlichen Sicherheitsanforderungen und/oder einheitlicher Sicherheitsadministration bezeichnet. Insbesondere bilden die Ressorts eigene Sicherheitsdomänen.

3 Ziele der Informationssicherheit

Allgemeingültige Sicherheitsziele innerhalb der Landesverwaltung und Justiz sind:

- zuverlässige Unterstützung der Geschäftsprozesse durch die IT und Sicherstellung der Kontinuität der Arbeitsabläufe innerhalb der Organisation,
- Realisierung sicherer und vertrauenswürdiger E-Government-Verfahren, Erhaltung der in Technik, Informationen, Arbeitsprozessen und Wissen investierten Werte,
- Sicherung der umfangreichen, möglicherweise unwiederbringlichen Werte der verarbeiteten Informationen,
- Erhalt beziehungsweise Gewährleistung der aus gesetzlichen Vorgaben resultierenden Anforderungen,
- Wahrung des Rechts der betroffenen Person auf den Schutz ihrer personenbezogenen Daten,
- Reduzierung der im Schadensfall entstehenden Kosten sowie
- Wahrung besonderer Dienst- oder Amtsgeheimnisse.

Jedes Ressort soll für seinen Bereich weitere angepasste Informationssicherheitsziele aufstellen.

4 Grundsätze der Sicherheitspolitik

Bei der Erstellung von Sicherheitsrichtlinien beziehungsweise Sicherheitskonzepten sind folgende Grundsätze zu berücksichtigen.

4.1 Angemessenheit von Sicherheitsmaßnahmen

Aufwand und Ziele von Sicherheitsmaßnahmen müssen in einem angemessenen Verhältnis zueinander stehen, wobei das Verhältnis nach den Methoden der BSI-Standards 200-x des Bundesamtes für Sicherheit in der Informationstechnik (BSI) bestimmt werden muss. Neben der Beachtung gesetzlich vorgeschriebener Sicherheitsanforderungen müssen sich daraus ergebende Sicherheitsmaßnahmen zugleich auch immer im Verhältnis zum Schutzzweck einer Angemessenheitsprüfung unterzogen werden. Bei der Auswahl und Umsetzung von Sicherheitsmaßnahmen ist darauf zu achten, dass der Ablauf von Geschäftsprozessen möglichst wenig durch die Sicherheitsmaßnahmen beeinträchtigt wird.

4.2 Bereitstellung von ausreichenden Ressourcen für die Informationssicherheit

Zur Erreichung und Aufrechterhaltung eines angemessenen Maßes an Informationssicherheit müssen ausreichende finanzielle und personelle Ressourcen durch die Behörden und Einrichtungen der Landesverwaltung und Justiz bereitgestellt werden.

Beim Festlegen des Sicherheitsniveaus und bei der Formulierung konkreter Sicherheitsanforderungen für die jeweilige Einrichtung ist darauf zu achten, dass das angestrebte Sicherheitsniveau auch wirtschaftlich sinnvoll ist.

4.3 Einbindung aller Mitarbeiterinnen und Mitarbeiter in den Sicherheitsprozess

Informationssicherheit betrifft ohne Ausnahme alle Mitarbeiterinnen und Mitarbeiter. Jede einzelne Person soll durch verantwortungs- und sicherheitsbewusstes Handeln dabei helfen, Schäden zu vermeiden und zum Erfolg beitragen. Sensibilisierung für Informationssicherheit und fachliche Schulungen der Mitarbeiterinnen und Mitarbeiter sind eine Grundvoraussetzung für Informationssicherheit. Mitarbeiterinnen und Mitarbeiter müssen über den Sinn von Sicherheitsmaßnahmen aufgeklärt werden.

Dies ist besonders wichtig, wenn diese Sicherheitsmaßnahmen Komfort- oder Funktionseinbußen zur Folge haben.

Die Sicherheitsmaßnahmen müssen für Mitarbeiterinnen und Mitarbeiter transparent und verständlich sein, sofern dadurch kein Sicherheitsrisiko entsteht.

Beauftragende Stellen müssen diese Vorgabe gegenüber externen Mitarbeiterinnen und Mitarbeitern analog verfügen.

4.4 Informationsklassifizierung und Informationsschutz

Alle Informationen, welche im Rahmen von IT-unterstützten Geschäftsprozessen verarbeitet werden, müssen anhand ihres Schutzbedarfs klassifiziert werden. Die Schutzbedarfsfeststellung und deren Dokumentation sollen auf Grundlage festgelegter, landesweit einheitlicher Schutzbedarfskategorien erreicht werden.

4.5 Sicherheit der Informationssysteme während des Lebenszyklus

Vor dem erstmaligen Einsatz von informationstechnischen beziehungsweise kommunikationstechnischen Verfahren ist zu prüfen, ob Risiken gemäß den ermittelten Schutzziele bestehen oder sich durch den Einsatz ergeben können.

Einschlägige rechtliche Regelungen, insbesondere das Brandenburgische E-Government-Gesetz (BbgEGovG), das Brandenburgische Datenschutzgesetz sowie die Datenschutz-Grundverordnung, sind zu berücksichtigen.

Gegebenenfalls sind im Rahmen eines nach den BSI-Standards 200-2 und 200-3 erstellten Sicherheitskonzeptes geeignete Sicherheitsmaßnahmen zur Behandlung der Risiken zu bestimmen und für das Verfahren umzusetzen.

Dabei sollen das IT-Grundschrift-Kompendium des BSI in der jeweils aktuellen Version als Anforderungskatalog sowie das Standard-Datenschutzmodell von Bund und Ländern in der jeweils geltenden Fassung zugrunde liegen. Ausnahmen hiervon sind zulässig, wenn nachgewiesen wird, dass das erreichte Schutzniveau nicht hinter das des IT-Grundschrift-Kompendiums des BSI und des Standard-Datenschutzmodells von Bund und Ländern in der jeweils geltenden Fassung zurückfällt.

Auf bestehende Basis-Sicherheitskonzepte im Brandenburgischen IT-Dienstleister und dem Zentralen IT-Dienstleister der Justiz soll referenziert werden. Für Bereiche mit hohem beziehungsweise sehr hohem Schutzbedarf sind zusätzliche Methoden auf Grundlage des BSI-Standards 200-3 anzuwenden.

Während des Lebenszyklus von Informationssystemen müssen die Risikoanalysen in angemessenen Abständen regelmäßig wiederholt werden, um zu prüfen, ob die ausgewählten Sicherheitsmaßnahmen noch ausreichend sind. Neue Hardware beziehungsweise Software muss mindestens den geltenden IT-Sicherheitsstandards des Landes Brandenburg (siehe Nummer 8) entsprechen.

4.6 Bildung von Sicherheitsdomänen

Sicherheitsdomänen sind durch entsprechende technische und organisatorische Maßnahmen abzugrenzen.

5 Rollen und Verantwortlichkeiten

5.1 Dienststellenleitung

Jede Dienststellenleitung beziehungsweise Geschäftsführung ist verantwortlich für die Informationssicherheit in ihrem Bereich. Sie hat die Risiken, die sich beim Einsatz von IT ergeben, bewusst zu steuern. Optionen zur Behandlung der Risiken sind das Ergreifen geeigneter Maßnahmen zur Verminderung der Risiken, die bewusste und objektive Akzeptanz der Risiken und die Übertragung der Risiken auf Dienstleister beziehungsweise Versicherungen.

5.2 Informationseigentümerinnen und Informationseigentümer

Die Informationseigentümerin oder der Informationseigentümer ist zuständig für:

- die Festlegung der geschäftlichen Relevanz ihrer oder seiner Informationen und die Schutzbedarfsfeststellung durch die Verfahrensverantwortlichen,
- die Sicherstellung, dass Verantwortlichkeiten explizit definiert und Sicherheits- und Kontrollmaßnahmen zur Verwaltung und zum Schutz ihrer oder seiner Informationen implementiert werden.

Die Informationseigentümerin oder der Informationseigentümer muss die Zugänglichkeit auf Informationen sowie den Umfang und die Art der Autorisierung definieren, die im jeweiligen Zugriffsverfahren erforderlich ist. Bei diesen Entscheidungen ist Folgendes zu prüfen:

- die Notwendigkeit, die Informationen entsprechend ihrer geschäftlichen Relevanz zu schützen,
- die Aufbewahrungsvorschriften und die mit den jeweiligen Informationen verbundenen rechtlichen Anforderungen und
- die Zugänglichkeit der für die jeweiligen Geschäftsanforderungen erforderlichen Informationen.

5.3 Nutzerinnen und Nutzer

Nutzerinnen und Nutzer sind bei der Erstellung, Nutzung und Verwaltung von Informationen verpflichtet, die Einhaltung der Informationssicherheitsleitlinie und der IT-Sicherheitsstandards sowie die weiteren Maßgaben der Landesverwaltung und Justiz, denen die Informationssicherheitsleitlinie zugrunde liegt, anzustreben. Hierfür müssen entsprechende Unterweisungen erfolgen.

5.4 Informationssicherheitsmanagement

Für jede Sicherheitsdomäne sind Informationssicherheitsbeauftragte zu benennen.

Zur Unterstützung eines effektiven Informationssicherheitsmanagements in der Landesverwaltung und Justiz ist ein ressortübergreifendes Expertenteam, das Informationssicherheitsmanagement-Team (ISMT), etabliert (siehe Nummer 6.1).

6 Die Informationssicherheitsorganisation

6.1 Das Informationssicherheitsmanagement-Team

Das ISMT hat eine wesentliche Bedeutung für die Informationssicherheit der Landesverwaltung und Justiz.

Es wird durch die landesweite Informationssicherheitsmanagerin oder den landesweiten Informationssicherheitsmanager und die Informationssicherheitsbeauftragten der Staatskanzlei und der Ressorts gebildet.

Die Unabhängigkeit der Informationssicherheitsbeauftragten - und damit des ISMT - soll nicht beeinträchtigt werden.

Vorsitz und Geschäftsführung des ISMT obliegt der landesweiten Informationssicherheitsmanagerin oder dem landesweiten Informationssicherheitsmanager. Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht, der Brandenburgische IT-Dienstleister des Landes sowie der Zentrale IT-Dienstleister der Justiz wirken beratend mit. Der Brandenburgische IT-Dienstleister soll durch das Computersicherheits-Ereignis- und Reaktionsteam (CERT) sowie durch das Kompetenzzentrum

IT-Sicherheit vertreten sein. Der Zentrale IT-Dienstleister der Justiz wird durch die behördliche Informationssicherheitsbeauftragte oder den behördlichen Informationssicherheitsbeauftragten vertreten.

Die Verwaltung des Landtages und der Landesrechnungshof können nach eigenem Ermessen jederzeit beratend mitwirken. Sie werden zu den Sitzungen des ISMT eingeladen und über die Ergebnisse der Sitzungen unterrichtet. Andere Verwaltungseinheiten oder Einzelpersonen, auch Externe, können auf Einladung der oder des Vorsitzenden beratend hinzugebeten werden.

Das ISMT trifft seine Entscheidungen durch Beschluss im Rahmen seiner Sitzungen oder im schriftlichen Umlaufverfahren.

Das ISMT trifft seine Entscheidungen im Konsensprinzip.

Vor ISMT-Beschlussfassungen ist dem RIO-Ausschuss rechtzeitig Gelegenheit zur Stellungnahme einzuräumen.

Jede beziehungsweise jeder Stimmberechtigte des RIO-Ausschusses, die beziehungsweise der im Rahmen der Entscheidungsfindung im ISMT sich nicht ausreichend berücksichtigt sieht, kann mit einem begründeten Antrag die Entscheidung der Amtschefinnen und Amtschefs in der betreffenden Angelegenheit herbeiführen. Es ist insbesondere darzulegen, dass die getroffene Entscheidung des ISMT das antragstellende Ressort unmittelbar und erheblich betrifft. Die beziehungsweise der Vorsitzende des ISMT legt den Antrag unverzüglich der Arbeitsbesprechung der Amtschefinnen und Amtschefs (ABS) zur abschließenden Entscheidung vor.

Im Rahmen einer Sitzung ist das ISMT beschlussfähig, wenn mehr als die Hälfte der ISMT-Mitglieder anwesend sind.

Näheres regelt eine Geschäftsordnung.

Das ISMT hat folgende Aufgaben:

- die Informationssicherheitsleitlinie weiterzuentwickeln,
- Informationssicherheitsziele und -strategien mit Unterstützung des CERT zu entwickeln beziehungsweise weiterzuentwickeln,
- ressortübergreifende landesweite Sicherheitsrichtlinien und IT-Sicherheitsstandards zu entwickeln beziehungsweise weiterzuentwickeln und darüber zu entscheiden,
- die Umsetzung der Informationssicherheitsleitlinie zu kontrollieren,
- an der Erarbeitung von Vorgaben für Hard- und Software mitzuwirken, die der Gewährleistung oder Verbesserung der Informationssicherheit von zentral betriebenen Querschnittsverfahren dienen, wie zum Beispiel Firewall-Lösungen, Virenschutzsoftware, Verschlüsselungssoftware oder VPN-Lösungen,
- zu überprüfen, ob die in den landesweiten Sicherheitsrichtlinien geplanten Sicherheitsmaßnahmen wirksam sind,

- bei der Erstellung der jährlichen Informationssicherheitsberichte und Jahrespläne mitzuwirken sowie
- die Erstellung von Schulungs- beziehungsweise Sensibilisierungsprogrammen für Informationssicherheit zu unterstützen.

6.2 Die landesweite Informationssicherheitsmanagerin oder der landesweite Informationssicherheitsmanager

Der für landesweite Informationssicherheit zuständigen obersten Landesbehörde werden folgende Funktionen und Aufgaben zugewiesen:

- Einsetzung einer landesweiten Informationssicherheitsmanagerin oder eines landesweiten Informationssicherheitsmanagers und einer ISMT-Geschäftsstelle für die Landesverwaltung und Justiz
- strategische Zusammenarbeit mit dem Brandenburgischen IT-Dienstleister und dem Zentralen IT-Dienstleister der Justiz auf dem Gebiet der Informationssicherheit sowie
- Erarbeitung strategischer Vorgaben zum Betrieb einer zentralen Anlaufstelle für präventive und reaktive Maßnahmen in Bezug auf sicherheits- und verfügbarkeitsrelevante Vorfälle in Computer-Systemen (CERT).

Die landesweite Informationssicherheitsmanagerin oder der landesweite Informationssicherheitsmanager hat folgende Aufgaben:

- Vorsitz des ISMT,
- Beratung der oder des IT-Beauftragten der Landesregierung in Informationssicherheitsfragen,
- Beratung des RIO-Ausschusses in Informationssicherheitsfragen,
- Federführung bei der Erstellung des jährlichen Informationssicherheitsberichtes unter Einbeziehung des ISMT, in welchem unter anderem die Ergebnisse des Monitoring-Prozesses zur Überwachung und Prüfung der Wirksamkeit des ISMS in den Ressorts zu berücksichtigen sind,
- jährliche Unterrichtung der Amtschefinnen und Amtschefs der Landesregierung durch einen Informationssicherheitsbericht und Vorlage eines jährlichen ISMT-Jahresplanes, wobei dem RIO-Ausschuss die Gelegenheit zur Stellungnahme gegeben wird,
- regelmäßige oder anlassbezogene Veranlassung von Revisionen der Informationssicherheit in der untermittelbaren Landesverwaltung und Justiz sowie Überprüfung von Sicherheitsvorfällen sowie gegebenenfalls Vorschlag der Einleitung geeigneter Maßnahmen zur Abwendung von Sicherheitsvorfällen unter Beteiligung der oder des zuständigen Ressort-Informationssicherheitsbeauftragten. Ist eine Revision oder Überprüfung von Sicherheitsvorfällen durch die landesweite Informationssicherheitsmanagerin oder den landesweiten Informationssicherheitsmanager aufgrund von Vorschriften der Geheimhaltung (zum Beispiel Verschlusssachenweisung des Landes Brandenburg) nicht möglich, so ist mit der oder dem Informationssicherheitsbeauftragten der Sicherheitsdomäne eine andere geeignete Vorgehensweise abzusprechen und umzusetzen.

Die landesweite Informationssicherheitsmanagerin oder der landesweite Informationssicherheitsmanager fragt jährlich den Stand der Informationssicherheit kennzahlenbasiert in den Ressorts ab. Der Informationssicherheitsbericht schätzt die aktuellen Risiken ein, trifft Aussagen zur Wirksamkeit des ISMS und zur Wirksamkeit der durchgeführten Sicherheitsmaßnahmen und beinhaltet einen Plan zur Behandlung der identifizierten Risiken.

6.3 Die Informationssicherheitsbeauftragten der Ressorts

Die Staatskanzlei und jedes Ministerium haben eine fachlich qualifizierte Informationssicherheitsbeauftragte oder einen fachlich qualifizierten Informationssicherheitsbeauftragten für ihr Ressort zu benennen.

Die oder der Informationssicherheitsbeauftragte ist zuständig für die Wahrnehmung aller Belange der Informationssicherheit innerhalb des Ressorts. Die Hauptaufgabe der oder des Informationssicherheitsbeauftragten besteht darin, die Dienststellenleitung bei der Wahrnehmung ihrer Aufgaben im Hinblick auf die Informationssicherheit zu beraten und bei deren Umsetzung zu unterstützen.

Die Informationssicherheitsbeauftragten der Ressorts haben ein unmittelbares Vortragsrecht bei ihren jeweiligen Amtschefinnen beziehungsweise Amtschefs. Zur Wahrung der Unabhängigkeit der Ressort-Informationssicherheitsbeauftragten soll sichergestellt werden, dass diese sich in keinem Unterstellungsverhältnis zur oder zum Ressort Information Officer (RIO) befinden. Um Interessenskonflikte zu vermeiden und die Unabhängigkeit der Informationssicherheitsbeauftragten der Ressorts zu wahren, soll darüber hinaus sichergestellt werden, dass die Informationssicherheitsbeauftragten der Ressorts selbst keine operativen IT-Aufgaben wahrnehmen.

Die Aufgaben der oder des Informationssicherheitsbeauftragten der Ressorts umfassen unter anderem:

- im gesamten Sicherheitsprozess mitzuwirken,
- die Erstellung von Sicherheitsrichtlinien,
- bei der Erstellung von Sicherheitskonzepten im Ressort zu unterstützen,
- einen jährlichen Umsetzungsplan zur Informationssicherheit für das Ressort zu erarbeiten und die Umsetzung zu überprüfen,
- ihrer oder seiner Amtschefin beziehungsweise ihrem oder seinem Amtschef zu berichten und diese zu beraten,
- im ISMT des Landes mitzuarbeiten,
- den oder die RIO zu beraten,
- die Realisierung für Informationssicherheitsmaßnahmen zu initiieren und zu überprüfen,
- Sensibilisierungs- und Schulungsmaßnahmen anzuregen. Die oder der Informationssicherheitsbeauftragte kann ressortweit die Durchführung von Sensibilisierungs- und Schulungsmaßnahmen koordinieren und soll sich selbst regelmäßig fachbezogen fortbilden,
- eventuell auftretende sicherheitsrelevante Zwischenfälle festzustellen und zu untersuchen sowie Sicherheitsrevisionen zur Erkennung von Schwachstellen

durchzuführen und gegebenenfalls das CERT hinzuzuziehen,

- den jährlichen Monitoring-Prozess zur Überwachung und Prüfung der Wirksamkeit des ISMS im Geschäftsbereich auf Basis der Empfehlungen der landesweiten Informationssicherheitsmanagerin oder des landesweiten Informationssicherheitsmanagers oder eines entsprechenden Beschlusses des ISMT umzusetzen.

Für geeignete nachgeordnete Bereiche oder abgrenzbare Sicherheitsdomänen in den Ressorts sollen die Ressorts in eigener Zuständigkeit weitere Informationssicherheitsbeauftragte benennen oder die Benennung auf diesen Bereich delegieren. Für einzelne Sicherheitsdomänen berufene Informationssicherheitsbeauftragte stimmen sich bei Bedarf mit der oder dem Informationssicherheitsbeauftragten des Ressorts ab. Die oder der Informationssicherheitsbeauftragte ist bei allen neuen Projekten, die deutliche Auswirkungen auf die Informationsverarbeitung haben, sowie bei der Einführung neuer IT-Anwendungen und IT-Systeme frühzeitig zu beteiligen. Die Arbeitsfähigkeit und die fachliche Qualifikation der Informationssicherheitsbeauftragten in den Ressorts und den nachgeordneten Bereichen sollen durch Freistellung im erforderlichen Umfang sowie durch regelmäßige Fortbildung sichergestellt werden. Als fachliche Qualifikation ist eine Zertifizierung als Informationssicherheitsbeauftragte oder Informationssicherheitsbeauftragter in der öffentlichen Verwaltung nach den Empfehlungen des BSI vorzusehen.

6.4 CERT

Für die Landesverwaltung und Justiz ist beim Brandenburgischen IT-Dienstleister ein CERT als zentrale Anlaufstelle für präventive und reaktive Maßnahmen in Bezug auf sicherheits- und verfügbarkeitsrelevante Vorfälle im Sinne des § 16 BbgEGovG zu betreiben.

Das CERT arbeitet im Verwaltungs-CERT-Verbund (VCV) mit. Die Mindest-Dienstleistungen des CERT werden durch die jeweils aktuelle Fassung der VCV-Geschäftsordnung bestimmt.

Darüber hinausgehende Dienstleistungen des CERT regeln die mit dem für landesweite Informationssicherheit zuständigen Ressort geschlossenen Servicevereinbarungen.

Zu den weiteren Aufgaben des CERT gehören:

- Unterstützung und Beratung der landesweiten Informationssicherheitsmanagerin oder des landesweiten Informationssicherheitsmanagers in allen informationssicherheitstechnischen Aspekten,
- Teilnahme und Mitwirkung an den ISMT-Sitzungen,
- technische Beratung der Informationssicherheitsbeauftragten.

7 Der landesweite Sicherheitsprozess

Der landesweite Sicherheitsprozess hat das Ziel, in allen Ressorts ein ISMS zur Gewährleistung des IT-Grundschutzes entsprechend den BSI-Standards 200-1 und 200-2 zu betreiben.

7.1 Planung des ISMS

Die Ressorts passen ihren Sicherheitsprozess den Vorgaben des BSI-Standards 200-2 in der jeweils geltenden Fassung fortlaufend an.

Die Ressorts verabschieden auf der Grundlage der Informationssicherheitsleitlinie für ihren Geschäftsbereich eine eigene Ressort-Sicherheitsleitlinie, schreiben diese fort und legen Sicherheitsdomänen fest.

Das ISMT kann die Maßnahmen konkretisieren, die sich aus den Anforderungen des IT-Grundschutz-Kompodiums des BSI ergeben. Diese Konkretisierungen sollen durch landesweite Sicherheitsrichtlinien und IT-Sicherheitsstandards erfolgen.

7.2 Umsetzung und Durchführung des ISMS

Alle Dienststellen der Landesverwaltung und Justiz sollen für ihren Bereich (Sicherheitsdomäne) unter Beachtung der Informationssicherheitsleitlinie des Landes und der jeweiligen Sicherheitsleitlinie des Ressorts eine Sicherheitskonzeption nach IT-Grundschutz gemäß BSI-Standard 200-2 in der jeweils geltenden Fassung mit konkreten organisatorischen und technischen Anforderungen, Verantwortlichkeiten, Sicherheitsmaßnahmen und Regeln zur Durchsetzung erstellen. Insbesondere sind für jede Dienststelle der Landesverwaltung und Justiz ein Virenschutzkonzept, ein Datensicherungs- und Archivierungskonzept, ein Notfallvorsorgekonzept und Sicherheitsregeln für die IT-Nutzung zu erarbeiten, soweit nicht auf zentrale Konzepte des Brandenburgischen IT-Dienstleisters referenziert werden kann.

7.3 Überwachung und Prüfung des ISMS

Die Dienststellen sind verpflichtet, alle aufgetretenen Sicherheitsvorfälle dem CERT zu melden. Ausgenommen hiervon ist die Verfassungsschutzbehörde. Das CERT klassifiziert die gemeldeten Vorfälle und informiert je nach Schwere der Sicherheitsvorfälle die landesweite Informationssicherheitsmanagerin oder den landesweiten Informationssicherheitsmanager und die Informationssicherheitsbeauftragten der betroffenen Ressorts.

Das CERT betreibt im Auftrag der landesweiten Informationssicherheitsmanagerin oder des landesweiten Informationssicherheitsmanagers eine Datenbank, in der Sicherheitsverletzungen und -vorfälle erfasst werden.

Der Brandenburgische IT-Dienstleister entwirft ein Design für eine Datenbank und betreibt diese, deren Daten dazu dienen, die Schwachstellenerkennung zu unterstützen und Lagebilder zur IT-Sicherheit zu erstellen. In dieser Datenbank sollen möglichst alle Behörden, Landesbetriebe und Einrichtungen der Landesverwaltung und der Justiz und Kommunen erfasst werden, soweit sie das Landesverwaltungsnetz (LVN) (einschließlich LVN-Kommunal) nutzen.

Eine Übersicht der Anwendungen und Dienste des jeweiligen Ressorts soll für die Ressort-Informationssicherheits-

beauftragte oder den Ressort-Informationssicherheitsbeauftragten einsehbar sein.

Die landesweite Informationssicherheitsmanagerin oder der landesweite Informationssicherheitsmanager überprüft regelmäßig die Wirksamkeit des ISMS. Sie oder er kann dazu in allen Ressorts Penetrationstests oder angemessene Sicherheitsrevisionen unter Beteiligung der oder des zuständigen Ressort-Informationssicherheitsbeauftragten veranlassen. Die Durchführung von Penetrationstests oder Sicherheitsrevisionen wird dann durch die zuständigen Informationssicherheitsbeauftragten der Ressorts gesteuert. Die Sicherheitsrevisionen und Penetrationstests sollen dabei auf Grundlage aktueller Empfehlungen des BSI durchgeführt werden.

7.4 Aufrechterhaltung und Verbesserung des ISMS

Das ISMT setzt die im Informationssicherheitsbericht identifizierten Verbesserungsmöglichkeiten des ISMS um. Die oder der Ressort-Informationssicherheitsbeauftragte nimmt ressortspezifische Verbesserungsmöglichkeiten in ihrem oder seinem Ressort zur Steuerung der Umsetzung mit.

Das ISMT überprüft in regelmäßigen Abständen, ob:

- sich Rahmenbedingungen geändert haben, die dazu führen, dass das Vorgehen in Bezug auf Informationssicherheit geändert werden muss,
- die Sicherheitsziele noch angemessen sind und
- ob die Informationssicherheitsleitlinie noch aktuell ist.

8 IT-Sicherheitsstandards

Die Standards in Bezug auf Informationssicherheit sind in der Anlage 2 der IT-Standardisierungsrichtlinie (SAGA.de.bb) in der jeweils geltenden Fassung aufgeführt.

9 Durchsetzung

Die Ressorts regeln in ihren jeweiligen Sicherheitsleitlinien sowie in daraus abgeleiteten ressort- oder behördenspezifischen Sicherheitsrichtlinien die Durchsetzung der Vorgaben der Informationssicherheitsleitlinie des Landes. Stellt die landesweite Informationssicherheitsmanagerin oder der landesweite Informationssicherheitsmanager Verstöße gegen die Vorgaben der Informationssicherheitsleitlinie des Landes oder Sicherheitsverletzungen von Dienststellen im LVN fest, so wird die betreffende Dienststelle über die zuständige Informationssicherheitsbeauftragte oder den zuständigen Informationssicherheitsbeauftragten des Ressorts aufgefordert, in einer angemessenen Frist die Sicherheitsverletzungen zu beheben beziehungsweise die Vorgaben der Informationssicherheitsleitlinie des Landes umzusetzen.

Bei anhaltenden Verstößen gegen die Vorgaben der Informationssicherheitsleitlinie oder bei anhaltenden Sicherheitsverletzungen des LVN durch Dienststellen ergreift die landesweite Informationssicherheitsmanagerin oder der landesweite Informationssicherheitsmanager in Verbindung mit der für die Fachaufsicht des Branden-

burgischen IT-Dienstleisters zuständigen Organisationseinheit in Abstimmung mit dem betroffenen Ressort die erforderlichen Maßnahmen.

10 Schlussbestimmungen

Die Informationssicherheitsleitlinie tritt nach Beschluss des Kabinetts durch Veröffentlichung im Intranet der Landesverwaltung in Kraft und ist binnen fünf Jahren nach Inkrafttreten zu evaluieren.

Anlage

Erläuterungen:

Zu 1 Gegenstand und Geltungsbereich

Der Satz „Die oder der jeweilige Verfahrensverantwortliche der Landesverwaltung hat gegenüber Dritten - insbesondere Kommunen und Dienstleistern - im notwendigen Umfang auf die Beachtung der Vorgaben dieser Informationssicherheitsleitlinie hinzuwirken und diese bei Vereinbarungen oder Verträgen zu gewährleisten.“ stellt auf die Vorgaben der Informationssicherheitsleitlinie des IT-Planungsrates ab. Ebenen übergreifende IT-Verfahren der Verwaltung sind insbesondere dadurch gekennzeichnet, dass nicht alle Teile solcher Verfahren sich in ausschließlicher Verantwortung der Landesverwaltung befinden. Hier soll bei entsprechenden Vereinbarungen mit anderen Verwaltungen außerhalb der Landesverwaltung sichergestellt werden, dass die Vorgaben aus dieser Leitlinie auch auf den Teil solcher Ebenen übergreifenden Verfahren Anwendung zu finden haben oder mindestens darauf hingewirkt worden war.

Zu 2.1 Informationssicherheit

Im Hinblick auf die Verarbeitung personenbezogener Daten sollen zusätzlich die Aspekte Datenminimierung, Nichtverknüpfung, Intervenierbarkeit und Transparenz berücksichtigt werden. Es wird insoweit auf das von der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) verabschiedete Standard-Datenschutzmodell in der jeweils geltenden Fassung hingewiesen.

Zu 2.4 Informationseigentümerinnen und Informations-eigentümer

Diese Vorgaben dienen der Verortung der lokalen Verantwortlichkeit für die Umsetzung von Sicherheitsvorgaben auf Geschäftsprozessebene.

Zu 3 Ziele der Informationssicherheit

Auch wenn Datenschutz und Informationssicherheit Überschneidungen aufweisen, ist klarzustellen, dass Informationssicherheit vorrangig dem Schutz von Werten und Datenschutz vorrangig dem Schutz von Persönlichkeitsrechten dient.

Zu 4.1 Angemessenheit von Sicherheitsmaßnahmen

Sicherheitsmaßnahmen sollen nicht losgelöst Gesichtspunkte der Wirtschaftlichkeit, der Auswirkungen auf die Organisa-

tion der Aufgabenerfüllung der Ressorts, deren Personalbedarf sowie deren Machbarkeit außer Betracht lassen.

Zu 4.2 Bereitstellung von ausreichenden Ressourcen für die Informationssicherheit

Sind die gestellten Sicherheitsanforderungen nicht finanzierbar, sollen die Sicherheitsanforderungen, aber auch die Geschäftsprozesse oder die Art und Weise des IT-Betriebes grundsätzlich überdacht werden.

Diese Soll-Vorgabe richtet sich an verschiedene Stellen. Die für die Organisation der Informationssicherheit zuständige Stelle hat darzulegen, warum die geforderte Sicherheitsanforderung geboten ist. Die für den Geschäftsprozess verantwortliche Stelle hat darzulegen, warum dieser Geschäftsprozess nur so und nicht anders zu betreiben ist. Beide zuständige Stellen haben ihre Überlegungen konkret zu dokumentieren und entsprechenden Einfluss auszuüben.

Zu 4.3 Einbindung aller Mitarbeiterinnen und Mitarbeiter in den Sicherheitsprozess

Der Satz „Beauftragende Stellen müssen diese Vorgabe gegenüber externen Mitarbeiterinnen und Mitarbeitern analog verfügen.“ bedeutet, dass nicht nur die unmittelbar Beschäftigten der Landesverwaltung in die Sicherheitsprozesse einzubeziehen sind, sondern auch die Beschäftigten von externen Dienstleistern, die im Auftrag der Ressorts Dienste verrichten. Gegebenenfalls sind hierfür auch die entsprechenden vertraglichen Regelungen, sofern notwendig, zu schaffen.

Zu 4.4 Informationsklassifizierung und Informationsschutz

Schutzbedarfskategorien werden in den Schutzbedarfen „Normaler Schutzbedarf“, „Hoher Schutzbedarf“, „Sehr hoher Schutzbedarf“ unterschieden. Näheres regelt eine landesweite Sicherheitsrichtlinie.

Zu 4.5 Sicherheit der Informationssysteme während des Lebenszyklus

Hier wird eine weitere Konkretisierung des § 16 Absatz 1 Satz 2 des Brandenburgischen E-Government-Gesetzes für die Landesverwaltung vorgenommen.

Zu 4.6 Bildung von Sicherheitsdomänen

Die technische Abgrenzung kann durch technische Maßnahmen (zum Beispiel durch eine Firewall) und die organisatorische Abgrenzung durch die Bildung einer entsprechenden Informationssicherheitsorganisation erreicht werden. Näheres regeln landesweite Sicherheitsrichtlinien.

Zu 5.1 Dienststellenleitung

Die Informationssicherheitsleitlinie des IT-Planungsrates gibt im Wortlaut vor: „Verantwortlich für Schaffung und Einhaltung der notwendigen Informationssicherheit einer Behörde ist die Behördenleitung“. Dazu zählt insbesondere das Benennen der Verantwortung der Leitungsebene für die Einhaltung gesetz-

licher Regelungen mit Dritten, den reibungsfreien Ablauf wichtiger Geschäftsprozesse und die Entscheidung über den Umgang mit Risiken. Nur die Leitungsebene kann daher für eine reibungslose Integration des Informationssicherheitsmanagements in die bestehenden Organisationsstrukturen sorgen. Zudem ist die Leitungsebene für den wirtschaftlichen Einsatz der Ressourcen verantwortlich.

Zu 5.2 Informationseigentümerinnen und Informations-eigentümer

Der Schutz von Informationen setzt Verantwortlichkeiten voraus. Für alle Informationen soll es eine benannte Informationseigentümerin oder einen benannten Informationseigentümer geben. Diese Eigentümerin oder dieser Eigentümer kann auch ein Gremium und eine Organisationseinheit sein. Dabei soll beachtet werden, dass das Verwenden und das Sammeln von Informationen im Zuge ihrer Bearbeitung oder Übertragung zu einer neuen Informationseigentümerin oder zu einem neuen Informationseigentümer führen kann.

Zu 5.3 Nutzerinnen und Nutzer

Die angesprochenen Unterweisungen der Nutzerinnen und Nutzer können beispielsweise über Schulungen erfolgen.

Zu 6.1 Das Informationssicherheitsmanagement-Team

Beschlussfassungsentwürfe des ISMT sind dem RIO-Ausschuss rechtzeitig, möglichst drei Wochen vor der beabsichtigten ISMT-Beschlussfassung, zur Kenntnis zu bringen und Gelegenheit zur Stellungnahme zu geben. Das ISMT trifft seine Entscheidungen unter Einbeziehung der Stellungnahme des RIO-Ausschusses.

Der Abschnitt:

„Jede beziehungsweise jeder Stimmberechtigte des RIO-Ausschusses, die beziehungsweise der im Rahmen der Entscheidungsfindung im ISMT sich nicht ausreichend berücksichtigt sieht, kann mit einem begründeten Antrag die Entscheidung der Amtschefinnen und Amtschefs in der betreffenden Angelegenheit herbeiführen. Es ist insbesondere darzulegen, dass die getroffene Entscheidung des ISMT das antragstellende Ressort unmittelbar und erheblich betrifft. Die beziehungsweise der Vorsitzende des ISMT legt den Antrag unverzüglich der Arbeitsbesprechung der Amtschefinnen und Amtschefs (ABS) zur abschließenden Entscheidung vor.“

räumt stimmberechtigten Mitgliedern des RIO-Ausschusses eine weitreichende Eskalationsmöglichkeit gegen ISMT-Entscheidungen ein.

Zu 6.3 Die Informationssicherheitsbeauftragten der Ressorts

Diese Vorgaben bedeuten nicht zwingend, dass die oder der Informationssicherheitsbeauftragte keine Aufgaben außerhalb der Informationssicherheit wahrnehmen darf. Sie oder er soll jedoch keine Aufgaben in der Informationstechnik wahrnehmen, die Interessenskonflikte hinsichtlich der Informations-

sicherheit hervorrufen können. Im Übrigen beschreibt der in der Landesverwaltung geltende BSI-Standard 200-2 unter Abschnitt 4.4 diese Vorgabe. Ferner ist darauf zu achten, dass die Informationssicherheitsbeauftragten sich regelmäßig zur Informationssicherheit fortbilden. Sie sollen mit entsprechender fachlicher Expertise auch qualitativ in der Lage sein, sich mit den Beschäftigten, die für den operativen IT-Betrieb zuständig sind, adäquat auszutauschen.

Zu 7 Der landesweite Sicherheitsprozess

Die IT-Standards des Landes Brandenburg, veröffentlicht als Runderlass der Landesregierung vom 15. Juni 2004 und zuletzt fortgeschrieben durch Beschluss des RIO-Ausschusses am 28. September 2021, geben diese Soll-Vorschriften (BSI-Standards 200-1 und 200-2) als verbindliche Spezifikation für den Betrieb von Informationsmanagementsystemen landesweit vor. Die vorliegende Leitlinie dient somit als zusätzliche Grundlage, ein ISMS nach diesen Standards zu betreiben.

Zu 7.1 Planung des ISMS

Die Ressorts passen auch ihren Sicherheitsprozess dem verabschiedeten Standard-Datenschutzmodell der DSK in der jeweils geltenden Fassung fortlaufend an.

Die Sätze „Das ISMT kann die Maßnahmen konkretisieren, die sich aus den Anforderungen des IT-Grundschutz-Kompendiums des BSI ergeben. Diese Konkretisierungen sollen durch landesweite Sicherheitsrichtlinien beziehungsweise IT-Sicherheitsstandards erfolgen.“ sind wie folgt zu verstehen. Die IT-Sicherheitsstandards sind Teil der IT-Standards und diese sind Teil des „SAGA Moduls Standards“. Mit der Einarbeitung von IT-Sicherheitsstandards in die IT-Standards als Teil des „SAGA Moduls Standards“ erfolgt eine regelmäßige Fortschreibung. Die Entwürfe zu diesen Fortschreibungen werden im Innenministerium vorbereitet.

Zu 7.3 Überwachung und Prüfung des ISMS

Diese Vorgaben sind eine Konkretisierung des Brandenburgischen E-Government-Gesetzes für die Landesverwaltung selbst. Im § 16 BbgEGovG heißt es: „Es (das CERT) sammelt und bewertet die zur Abwehr von Gefahren für die Sicherheit der Informationstechnik des Landes erforderlichen Daten und analysiert dabei insbesondere Sicherheitslücken, Schadprogramme und Vorgehensweisen bei Angriffen auf die Informationstechnik des Landes.“ Diese minimalen Informationen sind unabdingbare Voraussetzung für das CERT, um prüfen zu können, inwieweit Meldungen an das CERT beispielsweise über Schwachstellen überhaupt für Brandenburg zutreffen. Darüber hinaus ist häufig der Betrieb einer nicht aktuell eingesetzten Softwareversion selbst eine Schwachstelle. Da das CERT selbst einer gesetzlichen Warnpflicht unterworfen ist, muss es über die tatsächlich eingesetzte IT vollständig informiert werden.

Bei der Beachtung des Satzes „Die Durchführung von Penetrationstests oder Sicherheitsrevisionen wird dann durch die zuständigen Informationssicherheitsbeauftragten der Ressorts gesteuert.“ ist zu berücksichtigen, dass bei in den ZIT-BB über-

fürter Informationstechnik der ZIT-BB an Penetrationstests im Vorfeld zu beteiligen ist.

Zu 9 Durchsetzung

Grundsätzlich obliegt die Verantwortung für die Umsetzung der Informationssicherheitsleitlinie den Ressorts. Gleichwohl bedarf es bei anhaltenden Verstößen, die die Informationssicherheit der Landesverwaltung und Justiz gefährden und die Beteiligten diese nicht erkennbar abstellen, einer Handlungsempfehlung. Die Handlungsinitiative zur Umsetzung der Handlungsempfehlung läge in diesem Fall bei der landesweiten Informationssicherheitsmanagerin oder dem landesweiten Informationssicherheitsmanager mit der Maßgabe, auf jeden Fall die Fachaufsicht des Brandenburgischen IT-Dienstleisters einzubinden. Die Begrifflichkeit der „erforderlichen Maßnahmen“ gibt dabei vor, dass von allen geeigneten Maßnahmen immer diejenige zum Einsatz kommen soll, welche zum jeweiligen Zeitpunkt das jeweils mildeste Mittel der Wahl darstellt.

Unter dem jeweils mildesten Mittel der Wahl ist zum Beispiel auch die fristgerechte Kenntnissgabe dieser geeigneten Maßnahmen gegenüber der betroffenen Dienststelle zu verstehen.

Erste Änderung der Richtlinie des Ministeriums für Wirtschaft, Arbeit und Energie über die Gewährung von Zuschüssen an kleine und mittlere Unternehmen im Land Brandenburg zur Beschäftigung von Werkstudierenden und Innovationsassistentinnen beziehungsweise Innovationsassistenten „Brandenburger Innovationsfachkräfte (BIF 2022)“

Erlass
des Ministeriums für Wirtschaft, Arbeit und Energie
Vom 17. Juni 2024

I.

Die Richtlinie des Ministeriums für Wirtschaft, Arbeit und Energie über die Gewährung von Zuschüssen an kleine und mittlere Unternehmen im Land Brandenburg zur Beschäftigung von Werkstudierenden und Innovationsassistentinnen beziehungsweise Innovationsassistenten „Brandenburger Innovationsfachkräfte (BIF 2022)“ vom 22. November 2022 (ABl. S. 985) wird wie folgt geändert:

1. In Nummer 1.3 wird die Angabe „De-minimis-Verordnung (EU) Nr. 1407/2013 vom 18. Dezember 2013 (ABl. L 352 vom 24.12.2013, S. 1“ durch die Angabe „De-minimis-Verordnung (EU) 2023/2831 vom 13. Dezember 2023 (ABl. L, 2023/2831, 15.12.2023“ ersetzt.
2. In Nummer 3.1.3.4 Satz 1 wird die Angabe „1 040“ durch die Angabe „1 076“ ersetzt.

3. Nummer 3.1.4.5 wird wie folgt gefasst:

„3.1.4.5 Die Höhe der Förderung richtet sich nach der Förderstufe, der das Bruttomonatsgehalt der Werkstudentin oder des Werkstudenten zuzuordnen ist. Die je Förderstufe festgelegte Untergrenze für das Bruttomonatsgehalt entspricht den jeweils förderfähigen Gesamtausgaben je Monat. Gefördert werden bis zu 60 Prozent der förderfähigen Gesamtausgaben.

Förderstufe	Bruttomonatsgehalt in Euro	Zulässige Anzahl Wochenarbeitsstunden	Förderbetrag in Euro
1	ab 1 076	bis 20	645
2	ab 1 022	bis 19	610
3	ab 968	bis 18	580
4	ab 914	bis 17	545
5	ab 860	bis 16	515
6	ab 807	15	480

Die Förderung ist ausgeschlossen, wenn die vertraglich vereinbarte Anzahl der Wochenarbeitsstunden die für die betreffende Förderstufe zulässige Anzahl übersteigt. Ein höheres Bruttomonatsgehalt, das die Untergrenze der betreffenden Förderstufe übersteigt, ist hingegen förderunschädlich und ausdrücklich erwünscht.

Die Förderung wird für die Dauer von mindestens sechs bis maximal zwölf vollen Kalendermonaten gewährt.

Der monatliche Zuschussbetrag wird auf Grundlage des im Arbeitsvertrag vereinbarten Bruttomonatsgehalts der Arbeitnehmerin oder des Arbeitnehmers mit dem Zuwendungsbescheid festgelegt und gilt für den gesamten Durchführungszeitraum. Änderungen des Bruttomonatsgehalts während des Durchführungszeitraumes haben nur Auswirkungen auf die Förderung, wenn sich die Wochenarbeitsstundenzahl gegenüber der im Zuwendungsbescheid festgelegten erhöht und/oder das geänderte Bruttomonatsgehalt einer niedrigeren als der im Zuwendungsbescheid festgelegten Förderstufe zuzuordnen ist.

Sofern das Beschäftigungsverhältnis vorzeitig gelöst wird (zum Beispiel auf Grund einer Exmatrikulation), endet die Förderung mit dem letzten vollen Kalendermonat vor Ende des Beschäftigungsverhältnisses.“

4. In Nummer 3.1.5.5 Absatz 1 wird die Angabe „(ANBest-EU 21)“ durch die Wörter „sowie aus dem EU-Fonds ELER finanzierte Vorhaben in der Förderperiode 2023 bis 2027 (ANBest-EU 21) - ausgenommen Finanzinstrumente in Form von Fonds -“ ersetzt.

5. In Nummer 3.2.3.8 Buchstabe a wird nach Satz 2 folgender Satz eingefügt:

„Soweit für diese eine nahtlose Anschlussbeschäftigung als Innovationsassistentin oder Innovationsassistent nicht möglich ist, gelten sozialversicherungspflichtige Beschäftigungen nach dem Ende der Förderung als Werkstudentin oder Werkstudent für einen Überbrückungszeitraum von bis zu sechs Monaten als förderunschädlich.“

6. Nummer 3.2.4.5 wird wie folgt gefasst:

„3.2.4.5 Die Höhe der Förderung richtet sich nach der Förderstufe, der das Bruttomonatsgehalt der Innovationsassistentin oder des Innovationsassistenten zuzuordnen ist. Die je Förderstufe festgelegte Untergrenze für das Bruttomonatsgehalt entspricht den jeweils förderfähigen Gesamtausgaben je Monat. Gefördert werden bis zu 60 Prozent der förderfähigen Gesamtausgaben.“

Förderstufe	Bruttomonatsgehalt in Euro	Zulässige Anzahl Wochenarbeitsstunden	Förderungsbetrag in Euro
1	ab 2 750	keine Vorgabe	1 650
2	ab 2 533	unter 38	1 515
3	ab 2 171	unter 35	1 300
4	ab 1 809	unter 30	1 085
5	ab 1 447	mind. 20 bis unter 25	865

Die Förderung ist ausgeschlossen, wenn die vertraglich vereinbarte Anzahl von Wochenarbeitsstunden die für die betreffende Förderstufe zulässige Anzahl übersteigt. Ein höheres Bruttomonatsgehalt, das die Untergrenze der betreffenden Förderstufe übersteigt, ist hingegen förderunschädlich und ausdrücklich erwünscht.

Die Förderung wird für die Dauer von mindestens zwölf und höchstens achtzehn vollen Kalendermonaten gewährt.“

7. In Nummer 3.2.4.6 Satz 1 wird die Angabe „18“ durch die Angabe „24“ ersetzt.
8. In Nummer 3.2.5.1 Absatz 3 wird in dem siebenten Aufzählungsstrich das Komma durch einen Punkt ersetzt und folgender Satz wird angefügt:
- „Soweit dieses im Zeitpunkt der Antragstellung noch nicht ausgestellt wurde, ist zunächst eine Bestätigung der Hochschule über den erfolgreichen Abschluss des Studiums einzureichen und das Abschlusszeugnis nachzureichen.“
9. In Nummer 3.2.5.5 Absatz 1 wird die Angabe „(ANBest-EU 21)“ durch die Wörter „sowie aus dem

EU-Fonds ELER finanzierte Vorhaben in der Förderperiode 2023 bis 2027 (ANBest-EU 21) - ausgenommen Finanzinstrumente in Form von Fonds -“ ersetzt.

10. Nummer 4.1 wird wie folgt geändert:

- a) Satz 1 wird wie folgt gefasst:

„Bei den Förderungen nach dieser Richtlinie handelt es sich um „De-minimis“-Beihilfen im Sinne der Verordnung (EU) 2023/2831 der Kommission vom 13. Dezember 2023 über die Anwendung der Artikel 107 und 108 des Vertrags über die Arbeitsweise der Europäischen Union auf De-minimis-Beihilfen.“

- b) Satz 2 wird wie folgt geändert:

aa) Das Wort „Steuerjahren“ wird durch das Wort „Jahren“ und die Angabe „200 000 Euro“ durch die Angabe „300 000 Euro“ ersetzt.

bb) Die Angabe „(für Unternehmen im Straßentransportsektor: 100 000 Euro)“ wird gestrichen.

- c) In Satz 4 wird das Wort „Steuerjahren“ durch das Wort „Jahren“ und das Wort „Steuerjahr“ durch das Wort „Jahr“ ersetzt.

11. In Nummer 4.3 Absatz 1 Satz 1 wird die Angabe „den Artikeln 49 und 50“ durch die Angabe „Artikel 50“ ersetzt.

12. In Nummer 4.6 Absatz 1 werden nach dem Wort „Richtlinie“ die Wörter „beziehungsweise im Zuwendungsbescheid“ gestrichen.

13. Nach Nummer 4.7 wird folgende Nummer 4.8 eingefügt:

„4.8 Veröffentlichung

Es wird darauf hingewiesen, dass ab dem 1. Januar 2026 Informationen über jede Einzelbeihilfe innerhalb von 20 Arbeitstagen nach Gewährung der Beihilfe auf einer ausführlichen Beihilfen-Website der Europäischen Kommission veröffentlicht werden müssen.“

14. Nummer 5 wird wie folgt gefasst:

„5 Geltungsdauer

Diese Förderrichtlinie tritt mit Unterzeichnung in Kraft und mit Ablauf des 31. Dezember 2028 außer Kraft.“

II.

Dieser Erlass tritt am 29. Juni 2024 in Kraft.

**Richtlinie des Ministeriums für Wirtschaft,
Arbeit und Energie des Landes Brandenburg
zur Förderung der Regionalen Energiemanager
und Energiemanagerinnen zur Umsetzung
der Regionalen Energiekonzepte
(REM 2024 - 2027)**

Vom 12. Juli 2024

1 Zuwendungszweck, Rechtsgrundlage

- 1.1 Das Land Brandenburg gewährt nach Maßgabe dieser Förderrichtlinie sowie der §§ 23 und 44 der Landeshaushaltsordnung (LHO) und der dazu ergangenen Verwaltungsvorschriften für Zuwendungen an Gemeinden (GV) (VVG) in der jeweils geltenden Fassung Zuwendungen für die Umsetzung der regionalen Energiekonzepte durch die Regionalen Energiemanager und Energiemanagerinnen zur Unterstützung der Ziele der Energiestrategie 2040 des Landes Brandenburg.
- 1.2 Zuwendungen nach dieser Richtlinie stellen keine staatliche Beihilfe im Sinne des Artikels 107 Absatz 1 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) dar.¹
- 1.3 Auf die Gewährung der Zuwendung besteht kein Rechtsanspruch. Vielmehr entscheidet die Bewilligungsbehörde auf Grund ihres pflichtgemäßen Ermessens im Rahmen der verfügbaren Haushaltsmittel.

2 Gegenstand der Förderung

Zuwendungsfähig sind nicht investive Vorhaben. Dazu zählen insbesondere:

- Mitwirkung bei den Maßnahmen zur Umsetzung der Energiestrategie 2040 und Wasserstoffstrategie mit Regionalbezug
- Mitwirkung bei der Umsetzung von Maßnahmen der Regionalen Energiekonzepte in den Planungsregionen
- Zusammenarbeit und Austausch mit der Energieagentur Brandenburg
- Erstellung eines jährlichen Monitoringberichts zu den Aktivitäten und dem Umsetzungsstand von Maßnahmen aus den Regionalen Energiekonzepten

Darüber hinaus können folgende nicht investive Vorhaben gefördert werden:

- Initiierung und Durchführung von regionalen Projekten in den Bereichen Energieeffizienz, Energieeinsparung, Erneuerbare Energien und Akzeptanz

- Wissenstransfer zwischen beteiligten Akteuren
- Unterstützung der Kommunen bei der Erarbeitung und Umsetzung kommunaler Energiekonzepte
- Zusammenarbeit mit den kommunalen Energiemanagern und Energiemanagerinnen sowie Klimaschutzmanagern und Klimaschutzmanagerinnen
- Kommunikation mit kommunalen Akteuren zu Förderprogrammen
- Bereitstellung und Vermittlung von Informationen über konkrete Beispiele und Modelle der Bürgerbeteiligung
- Bereitstellung und Vermittlung von Informationen zur regionalen Wertschöpfung
- Erhöhung der Internetpräsenz und Sichtbarmachung der Angebote der Regionalen Energiemanager und Energiemanagerinnen auf einer gemeinsamen Website
- Fortführung der gemeinsamen Öffentlichkeitsarbeit der Regionalen Energiemanager und Energiemanagerinnen

3 Zuwendungsempfangende

Zuwendungsempfangende sind die Regionalen Planungsgemeinschaften (§ 4 des Gesetzes zur Regionalplanung und zur Braunkohlen- und Sanierungsplanung [RegBkPIG]) Havelland-Fläming, Lausitz-Spreewald, Oderland-Spree, Prignitz-Oberhavel und Uckermark-Barnim im Rahmen ihrer nicht wirtschaftlichen Tätigkeiten.

4 Zuwendungsvoraussetzungen

4.1 Zuwendungsfähig sind Vorhaben, die

- der Umsetzung der Ziele der Energiestrategie 2040 des Landes Brandenburg dienen,
- im Land Brandenburg durchgeführt werden und
- zum Zeitpunkt der Bestätigung der zuständigen Bewilligungsbehörde über den Antragseingang noch nicht begonnen worden sind. Als Vorhabenbeginn zählt der erste Abschluss eines der Ausführung zuzurechnenden Lieferungs- oder Leistungsvertrages.

4.2 Ausgeschlossen von einer Zuwendung sind Vorhaben, die

- gesetzlich vorgeschrieben sind und/oder behördlich angeordnet wurden,
- von anderen Stellen durchgeführt werden oder deren Ausgaben vollständig von anderen Stellen zu tragen sind.

4.3 Die Zuwendungsempfangenden dürfen im Rahmen ihrer Vorhaben nicht wirtschaftlich tätig werden. Die Trennung der geförderten nicht wirtschaftlichen Tätigkeiten von den wirtschaftlichen Tätigkeiten ist durch die Zuwendungsempfangenden zu gewährleisten und mit einer Trennungsrechnung zu dokumentieren.

¹ Bekanntmachung der Kommission zum Begriff der staatlichen Beihilfe im Sinne des Artikels 107 Absatz 1 des Vertrags über die Arbeitsweise der Europäischen Union (ABl. C 262 vom 19.7.2016, S. 1), insbesondere Nummern 2 und 7.2.1.

- 4.4 Die Zuwendungen dürfen nicht zu einer mittelbaren staatlichen Beihilfe an Unternehmen führen.

5 Art und Umfang, Höhe der Zuwendung

- 5.1 Zuwendungsart: Projektförderung
- 5.2 Finanzierungsart: Anteilfinanzierung
- 5.3 Form der Zuwendung: Zuschuss

5.4 Bemessungsgrundlage

5.4.1 Zuwendungsfähige Ausgaben

Zuwendungsfähig sind Personalausgaben und vorhabenbezogene Sachausgaben, die nicht bereits nach § 10 RegBkPIG aus der Übernahme von Aufgaben nach § 4 RegBkPIG erstattet werden. Für die Berechnung der zuwendungsfähigen Ausgaben werden die Beträge vor Abzug von Steuern und sonstigen Abgaben herangezogen. Die zuwendungsfähigen Ausgaben sind durch schriftliche Unterlagen zu belegen.

5.4.1.1 Personalausgaben

Personalausgaben sind in Höhe des nachgewiesenen Arbeitgeberbruttos für eine Vollzeitstelle pro Vorhaben zuwendungsfähig.

5.4.1.2 Sachausgaben

Zuwendungsfähig sind vorhabenbezogene Sachausgaben für:

- Marketingmaterialien
- Dienstreisen (Reisekosten nach Bundesreisekostengesetz [BRKG])
- Teilnahmegebühren für projektbezogene Veranstaltungen und Kongresse
- eigene Veranstaltungen
- Nettokaltmiete für zusätzlich ausschließlich vorhabenbezogen angemietete Räume
- Konzepte, Monitoring

5.4.2 Höhe der Zuwendung

Die Zuwendung beträgt, je nach finanzieller Leistungsfähigkeit der antragstellenden Regionalen Planungsgemeinschaften, bis zu 80 Prozent der zuwendungsfähigen Ausgaben.

5.4.2.1 Die Zuwendung muss im Einzelfall mehr als 25 000 Euro betragen.

5.4.2.2 Der Förderhöchstbetrag wird auf 65 000 Euro je Regionale Planungsgemeinschaft pro Jahr festgesetzt.

5.4.3 Eine Förderung erfolgt für die Dauer von maximal 36 Monaten.

6 Kumulation öffentlicher Mittel

Die Kumulation von Mitteln, die im Rahmen dieser Richtlinie bewilligt werden, mit anderen Mitteln des Bundes, des Landes Brandenburg oder der Europäischen Union für dasselbe Vorhaben ist nicht zulässig.

7 Verfahren

7.1 Antragsverfahren

Anträge auf Förderung einschließlich der erforderlichen Unterlagen können schriftlich bei der Investitionsbank des Landes Brandenburg (ILB), Babelsberger Straße 21, 14473 Potsdam eingereicht oder über das Internetportal der ILB (siehe Online-Antragsverfahren unter www.ilb.de) gestellt werden.

7.2 Bewilligungsverfahren

Über die Gewährung der Zuwendung entscheidet die ILB als Bewilligungsbehörde. Die Grundlage für die Bewilligung bilden der Antrag und die dazu einzureichenden Anlagen. Maßgeblich für die Beurteilung der Zuwendungsfähigkeit des Vorhabens ist die Sach- und Rechtslage zum Zeitpunkt der Entscheidung über die Bewilligung der Förderung. Die Antragstellenden dürfen erst nach von der ILB bestätigtem Eingang des schriftlichen Antrags mit allen erforderlichen Inhalten mit der Durchführung der beantragten Maßnahmen beginnen. Aus dieser Erlaubnis zum vorzeitigen Maßnahmenbeginn leitet sich jedoch kein Anspruch auf eine Zuwendung ab.

7.3 Anforderungs- und Auszahlungsverfahren

Die Anforderung der Zuwendung erfolgt quartalsweise online über das Internetportal der ILB. Dafür ist das dort bereitgestellte Formular „Mittelanforderung“ zu verwenden. Abweichend von Nummer 1.4 der Allgemeinen Nebenbestimmungen für Zuwendungen zur Projektförderung an Gemeinden (ANBest-G) darf eine Auszahlung der Zuwendung nur insoweit und nicht eher angefordert werden, als sie der Erstattung zuwendungsfähiger, tatsächlich entstandener und gezahlter Ausgaben der Zuwendungsempfängenden im Rahmen des Zuwendungszwecks dient (Erstattungsprinzip). Dabei darf die Zuwendung jeweils nur anteilig mit den vorgesehenen eigenen Mitteln der Zuwendungsempfängenden verwandt werden.

7.4 Verwendungsnachweisverfahren

Die Einreichung des Verwendungsnachweises nach Nummer 7 ANBest-G erfolgt online über das Internetportal der ILB.

7.5 Zu beachtende Vorschriften

Für die Bewilligung, Auszahlung und Abrechnung der Zuwendung sowie für den Nachweis und die Prüfung der Verwendung und die gegebenenfalls erforderliche

Aufhebung des Zuwendungsbescheides und die Rückforderung der gewährten Zuwendung gelten die VVG zu § 44 LHO, soweit nicht in den Förderrichtlinien Abweichungen zugelassen worden sind.

7.6 Monitoring

Die Zuwendungsempfangenden sind zur Erstellung eines jährlichen Monitoringberichts zu Konzepten und Vorhaben in den jeweiligen Regionen verpflichtet.

8 Geltungsdauer und Inkrafttreten

Diese Richtlinie tritt am Tag nach der Veröffentlichung im Amtsblatt für Brandenburg in Kraft und mit Ablauf des 30. September 2027 außer Kraft.

Festgesetztes Überschwemmungsgebiet der Unteren Oder mit Alter Oder, Westoder und Welse

Bekanntmachung des Ministeriums für Landwirtschaft,
Umwelt und Klimaschutz des Landes Brandenburg
Vom 27. Juni 2024

Gemäß § 100 Absatz 1 Satz 2 und Absatz 3 des Brandenburgischen Wassergesetzes in der Fassung der Bekanntmachung vom 2. März 2012 (GVBl. I Nr. 20), das zuletzt durch Artikel 29 des Gesetzes vom 5. März 2024 (GVBl. I Nr. 9 S. 14) geändert worden ist, in Verbindung mit § 76 Absatz 2 Satz 1 Nummer 1 des Wasserhaushaltsgesetzes vom 31. Juli 2009 (BGBl. I S. 2585), das zuletzt durch Artikel 7 des Gesetzes vom 22. Dezember 2023 (BGBl. 2023 I Nr. 409) geändert worden ist, werden die Karten zu dem nach § 100 Absatz 1 Satz 2 des Brandenburgischen Wassergesetzes als festgesetzt geltenden Überschwemmungsgebiet der Unteren Oder mit Alter Oder, Westoder und Welse hiermit für verbindlich erklärt.

Das Überschwemmungsgebiet liegt im Gebiet der Städte Angermünde, Bad Freienwalde (Oder) und Schwedt/Oder sowie der Ämter Britz-Chorin-Oderberg und Gartz (Oder). Das Über-

schwemmungsgebiet ist in Karten im Maßstab 1 : 2 500 auf der Grundlage des Liegenschaftskatasters dargestellt. Beglaubigte Abschriften der Karten sind bei den unteren Wasserbehörden der Landkreise Barnim (16225 Eberswalde, Carl-von-Ossietzky-Straße 11), Märkisch-Oderland (15306 Seelow, Puschkinplatz 12) und Uckermark (17291 Prenzlau, Karl-Marx-Straße 1) niedergelegt. Der gesamte niedergelegte Kartensatz enthält 97 Kartenblätter.

Mit dieser öffentlichen Bekanntmachung der Verbindlichkeit der Karten gilt das in den Karten dargestellte Überschwemmungsgebiet als festgesetztes Überschwemmungsgebiet. Damit gelten im Überschwemmungsgebiet die besonderen Schutzvorschriften gemäß § 78 Absatz 1, 3, 4 und 7, § 78a Absatz 1 und 3 und § 78c Absatz 1 und 3 des Wasserhaushaltsgesetzes sowie des § 101 Satz 1 und 2 des Brandenburgischen Wassergesetzes.

Gleichzeitig tritt gemäß § 100 Absatz 6 des Brandenburgischen Wassergesetzes der Beschluss Nr. 0189 vom 7. Dezember 1989 des Rates des Bezirkes Frankfurt (Oder) über Hochwassergebiete im Bezirk Frankfurt (Oder) insoweit außer Kraft, als Hochwassergebiete an der Oder, der Welse, der Westoder, der Hohensaaten-Friedrichsthaler-Wasserstraße und der Schwedter Querfahrt von der Hohenwutzener Chaussee in Hohenwutzen bis zur Landesgrenze zur Republik Polen festgelegt wurden.

Wahl zum 10. Europäischen Parlament am 9. Juni 2024

Bekanntmachung des Landeswahlleiters
Vom 11. Juli 2024

Gemäß § 72 Absatz 1 Nummer 2 der Europawahlordnung in der Fassung der Bekanntmachung vom 2. Mai 1994 (BGBl. I S. 957), die zuletzt durch Artikel 1 der Verordnung vom 11. August 2023 (BGBl. I S. 215) geändert worden ist, gibt der Landeswahlleiter bekannt, dass der Landeswahlausschuss in seiner öffentlichen Sitzung am 21. Juni 2024 das endgültige Ergebnis der Wahl der 96 Abgeordneten des Europäischen Parlaments aus der Bundesrepublik Deutschland vom 9. Juni 2024 für das Land Brandenburg wie nachstehend festgestellt hat:

I. Wahlberechtigte	2 079 233
II. Wähler	1 402 780
III. Ungültige Stimmen	19 270
IV. Gültige Stimmen	1 383 510
davon entfallen folgende gültige Stimmen auf die einzelnen Wahlvorschläge der nachfolgenden Parteien und sonstigen politischen Vereinigungen:	
1. Alternative für Deutschland (AfD)	380 717
2. Christlich Demokratische Union Deutschlands (CDU)	253 937
3. Sozialdemokratische Partei Deutschlands (SPD)	181 697
4. DIE LINKE (DIE LINKE)	61 520
5. BÜNDNIS 90/DIE GRÜNEN (GRÜNE)	82 672
6. Freie Demokratische Partei (FDP)	44 764
7. Partei für Arbeit, Rechtsstaat, Tierschutz, Elitenförderung und basisdemokratische Initiative (Die PARTEI)	31 806
8. FREIE WÄHLER (FREIE WÄHLER)	29 349
9. PARTEI MENSCH UMWELT TIERSCHUTZ (Tierschutzpartei)	23 200
10. Familien-Partei Deutschlands (FAMILIE)	16 914
11. Die Heimat (HEIMAT)	3 826
12. Piratenpartei Deutschland (PIRATEN)	5 360
13. Aktion Partei für Tierschutz (TIERSCHUTZ hier!)	9 340
14. Volt Deutschland (Volt)	22 096
15. Partei für schulmedizinische Verjüngungsforschung	894
16. Ökologisch-Demokratische Partei (ÖDP)	4 514
17. MERA25 - Gemeinsam für Europäische Unabhängigkeit (MERA25)	2 402
18. Deutsche Kommunistische Partei (DKP)	1 085
19. Partei der Humanisten (PdH)	2 170
20. Menschliche Welt – für das Wohl und Glücklichein aller (MENSCHLICHE WELT)	2 781
21. Bündnis C - Christen für Deutschland (Bündnis C)	1 483
22. Marxistisch-Leninistische Partei Deutschlands (MLPD)	547
23. Bündnis für Innovation & Gerechtigkeit (BIG)	728
24. Sozialistische Gleichheitspartei, Vierte Internationale (SGP)	309
25. Aktion Bürger für Gerechtigkeit (ABG)	1 504

26. Basisdemokratische Partei Deutschland (dieBasis)	2 870
27. BÜNDNIS DEUTSCHLAND (BÜNDNIS DEUTSCHLAND)	7 237
28. Bündnis Sahra Wagenknecht - Vernunft und Gerechtigkeit (BSW)	191 290
29. Demokratische Allianz für Vielfalt und Aufbruch (DAVA)	720
30. Klimaliste Deutschland (KLIMALISTE)	1 134
31. Parlament aufmischen – Stimme der Letzten Generation (LETZTE GENERATION)	4 012
32. Partei der Vernunft (PDV)	1 363
33. Partei des Fortschritts (PdF)	7 538
34. V-Partei ³ - Partei für Veränderung, Vegetarier und Veganer (V-Partei ³)	1 731

Die endgültige Verteilung der Sitze auf die Wahlvorschläge und die Namen der danach gewählten Bewerbenden wurden vom Bundeswahlausschuss festgestellt und von der Bundeswahlleiterin im Bundesanzeiger bekannt gemacht.

BEKANNTMACHUNGEN DER LANDESBETRIEBE

Verfügung zur (Teil-)Umstufung der Landesstraße (L) 215 in der Gemeinde Templin im Landkreis Uckermark

Bekanntmachung
des Landesbetriebes Straßenwesen Brandenburg,
Betriebssitz Hoppegarten
Vom 14. Juni 2024

Mit Wirkung zum 1. Oktober 2024 wird auf der Grundlage des § 7 des Brandenburgischen Straßengesetzes (BbgStrG) in der Fassung der Bekanntmachung vom 28. Juli 2009 (GVBl. I S. 358), das zuletzt durch Artikel 5 Absatz 6 des Gesetzes vom 5. März 2024 (GVBl. I Nr. 10 S. 79) geändert worden ist, die nachstehende Umstufung vorgenommen:

Die Landesstraße (L) 215 Abschnitt 010 wird von Netzknoten (NK) 2947 004 bis NK 2946 010 über eine Länge von 7,075 km, einschließlich der Nebenanlagen, zur Kreisstraße gemäß § 3 BbgStrG abgestuft.

Künftiger Träger der Straßenbaulast wird der Landkreis Uckermark.

Der Verwaltungsakt und seine Begründung können im Landesbetrieb Straßenwesen Brandenburg, Betriebssitz Hoppegarten, Lindenallee 51, 15366 Hoppegarten zu den üblichen Dienstzeiten eingesehen werden.

Die Verfügung gilt einen Tag nach der Veröffentlichung als bekannt gegeben.

Rechtsbehelfsbelehrung

Gegen diese Verfügung kann innerhalb eines Monats nach Bekanntgabe Widerspruch beim Landesbetrieb Straßenwesen Brandenburg, Betriebssitz Hoppegarten, Lindenallee 51 in 15366 Hoppegarten erhoben werden.

Im Auftrag

Mike Koehler
Abteilungsleiter Fachdienste

SONSTIGE BEKANNTMACHUNGEN

Ungültigkeitserklärung von Dienstausweisen

Polizeipräsidium Land Brandenburg

Der durch Verlust/Diebstahl abhandengekommene Dienstausweis von Frau **Olivia Weise**, Dienstausweisnummer **205963**, Kartennummer 2399, Farbe grau, ausgestellt am 07.03.2023 durch den Zentraldienst der Polizei des Landes Brandenburg, wird hiermit für ungültig erklärt.

Ministerium für Infrastruktur und Landesplanung

Der durch Verlust abhandengekommene Dienstausweis von Herrn **Simon Kirner**, Dienstausweisnummer **220185**, ausgestellt am 22.06.2021, gültig bis 21.06.2031, wird hiermit für ungültig erklärt.

STELLENAUSSCHREIBUNGEN

Stadt Ludwigsfelde

In der Stadt Ludwigsfelde ist zum 1. Januar 2025 die Stelle der/des Ersten Beigeordneten (m/w/d) zu besetzen.

Beschäftigungsverhältnis: Vollzeit

Beginn: 1. Januar 2025

Befristung: befristet auf acht Jahre

Besoldung: A 16 BbgBesO

Bewerbungsfrist: 18. August 2024

Der/Dem Ersten Beigeordneten soll der Fachbereich Zentrale Steuerung, Ordnung und Sicherheit mit den Fachdiensten Personal, Finanzen, Ordnungsamt und Bürgerservice sowie den Stabstellen Organisation und Controlling zugeordnet werden. Eine spätere Änderung der Geschäftsverteilung bleibt vorbehalten.

Die Stadt Ludwigsfelde mit circa 30 000 Einwohnerinnen und Einwohnern sucht für die aktive Gestaltung ihrer weiteren Entwicklung eine zielstrebige, verantwortungsbewusste und teamfähige Persönlichkeit, die in der Lage ist, die Verwaltung im Sinne eines modernen Dienstleistungsunternehmens bürger-nah und zukunftsorientiert zu gestalten. Für die Nutzung der besonderen Möglichkeiten und Potenziale der Stadt werden hohe Kreativität, Entscheidungsfreude, Verantwortungs- und Kostenbewusstsein und die Fähigkeit, Mitarbeiterinnen und Mitarbeiter zu motivieren und zu führen, erwartet.

Die Bewerberinnen und Bewerber müssen die Qualifikationsanforderungen der Kommunalverfassung des Landes Brandenburg an Wahlbeamte in kreisangehörigen Gemeinden unter 40 000 Einwohnerinnen und Einwohnern erfüllen. Dies bedeutet insbesondere, über die Befähigung zum gehobenen Verwaltungsdienst oder eine vergleichbare Qualifikation zu verfügen und die persönlichen Voraussetzungen für die Berufung in das Beamtenverhältnis auf Zeit zu erfüllen.

Es besteht die Chance, die Stadtentwicklung und eine bürgerorientierte Verwaltung in vertrauensvoller Zusammenarbeit mit

dem Bürgermeister, den Mitarbeiterinnen und Mitarbeitern und den politischen Gremien aktiv mitzugestalten.

Die/Der Erste Beigeordnete wird für die Dauer von acht Jahren als Beamtin/Beamter auf Zeit auf Vorschlag des Bürgermeisters durch die Stadtverordnetenversammlung gewählt. Die/Der Erste Beigeordnete ist gleichzeitig allgemeine Vertreterin/allgemeiner Vertreter des Bürgermeisters.

Die Besoldung der/des Ersten Beigeordneten erfolgt nach der Besoldungsgruppe A 16. Daneben wird eine Aufwandsentschädigung nach den Vorschriften der Kommunaldienstaufwandsentschädigungsverordnung des Landes Brandenburg gewährt.

Zur Prüfung der Verfassungstreue findet vorbehaltlich möglicher Änderungen des Landesbeamtengesetzes (LBG) vor der Berufung eine Regelanfrage bei der Verfassungsschutzbehörde Brandenburg statt.

Es wird darauf hingewiesen, dass Kosten, die im Zusammenhang mit der Bewerbung entstehen, nicht erstattet werden.

Bewerbungen mit den üblichen Unterlagen (insbesondere beglaubigte Zeugnisabschriften, lückenlose Qualifikations- und Tätigkeitsnachweise, Referenzen, erweitertes Führungszeugnis) sind digital über unsere Bewerberplattform auf unserer Internetseite hochzuladen oder sind in einem verschlossenen Umschlag mit dem Kennwort „Bewerbung Erste Beigeordnete/Erster Beigeordneter“ bis zum 18. August 2024 an:

Stadt Ludwigsfelde

An den Bürgermeister

- persönlich -

„Bewerbung Erste Beigeordnete/Erster Beigeordneter“

Rathausstraße 3

14974 Ludwigsfelde

zu senden.

Als Ansprechpartner steht zur Verfügung:

Frau Hentze
Fachdienst Personal
Telefon: 03378 827-128
Rathausstraße 3
14974 Ludwigsfelde.

Hinweis zum Datenschutz:

Ihre persönlichen Daten werden im Rahmen dieses Bewerbungsverfahrens auf der Grundlage des § 26 Absatz 1 des Brandenburgischen Datenschutzgesetzes (BbgDSG) von der Stadt Ludwigsfelde, Fachdienst Personal gespeichert. Für die ordnungsgemäße Durchführung des Verfahrens erhalten die beteiligten Personen und Gremien (Personalvertretung, Gleichstellungsbeauftragte und Schwerbehindertenvertretung) Einsicht. Weitere Informationen zum Datenschutz sind unter www.Ludwigsfelde.de/datenschutz zu finden.

Herausgeber: Ministerium der Justiz des Landes Brandenburg,

Anschrift: 14473 Potsdam, Heinrich-Mann-Allee 107, Telefon: 0331 866-0.

Der Bezugspreis beträgt jährlich 75,00 EUR (zzgl. Versandkosten + Portokosten). Die Einweisung kann jederzeit erfolgen.

Die Berechnung erfolgt im Namen und für Rechnung des Ministeriums der Justiz des Landes Brandenburg.

Die Kündigung ist nur zum Ende eines Bezugsjahres zulässig; sie muss bis spätestens 3 Monate vor Ablauf des Bezugsjahres dem Verlag zugegangen sein.

Die Lieferung dieses Blattes erfolgt durch die Post. Reklamationen bei Nichtzustellung, Neu- bzw. Abbestellungen, Änderungswünsche und sonstige Anforderungen sind an die Wolters Kluwer Deutschland GmbH zu richten.

Herstellung, Verlag und Vertrieb: Wolters Kluwer Deutschland GmbH, Wolters-Kluwer-Straße 1, 50354 Hürth, www.wolterskluwer.de,

Kundenservice: Telefon 02233 3760 7201, Fax 02233 3760 7202, E-Mail: info-wkd@wolterskluwer.com.

Das Amtsblatt für Brandenburg ist im Internet abrufbar unter www.landesrecht.brandenburg.de (Veröffentlichungsblätter [ab 1998]),
seit 1. Januar 2007 auch mit sämtlichen Bekanntmachungen (außer Insolvenzsachen) und Ausschreibungen.