Dienstanweisung Nr. 56/2020 zur Informationssicherheit

Stand: März 2024

LANDKREIS TELTOW-FLÄMING
unverkennbar stark - südlich von Berlin

Inhalt

Präambel

Informationsverarbeitung hat eine Schlüsselrolle bei der Aufgabenerfüllung in der Verwaltung inne. Sie unterstützt maßgeblich alle wesentlichen Funktionen und Aufgaben durch Informationstechnik (IT) in miteinander vernetzten Systemen. Somit sind funktionierende und sichere IT-Prozesse eine zentrale Grundlage für die Leistungsfähigkeit der Verwaltung. Dabei kommt der Informationssicherheit eine grundsätzliche Bedeutung zu.
Informationssicherheit (IS) umfasst die Summe aller organisatorischen, personellen und technischen Maßnahmen, um dieses Ziel zu erreichen. Zur Durchsetzung der Informationssicherheit dienen diese Dienstanweisung sowie weitere innerdienstliche Regelungen.

Diese Dienstanweisung beschreibt die allgemeinen Ziele, Strategien und Organisationsstrukturen, die für die Schaffung und Etablierung eines ganzheitlichen Informationssicherheitsprozesses erforderlich sind. Die Dienstanweisung dient der Gewährleistung der Informationssicherheit im Landkreis Teltow-Fläming. Es wird der Aufbau und der Betrieb eines zentral koordinierten, die Geschäftsbereiche übergreifenden **Informationssicherheitsmanagementsystems** (ISMS) beschrieben. Das ISMS soll die **Sicherheitsziele** gewährleisten.

§ 1
Begriffsbestimmungen

(1) **Informationstechnik** (IT) umfasst alle Formen der elektronischen Informationsverarbeitung und Telekommunikation.

(2) Eine **Sicherheitsmaßnahme** ist eine technische oder organisatorische Lösung mit dem Ziel, ein bestehendes Risiko zu minimieren oder zu beherrschen.

(3) Der **Informationssicherheitsprozess** ist ein sich erneut wiederholender Prozess, um die Sicherheit von Informationen auf einem akzeptablen Niveau zu halten.

(4) **Managementprinzipien** sind organisatorische Maßnahmen zur Umsetzung von Führungsstilen und wie diese ausgeübt werden können.

(5) Ein **Sicherheitsvorfall** ist ein Ereignis, welches mindestens eines der drei Gewährleistungsziele der Informationssicherheit verletzen könnte oder einen Bruch der Informationssicherheitsleitlinie darstellt.

(6) Eine **Störung** ist ein kurzzeitiger Ausfall von Prozessen oder Ressourcen mit nur einem geringen Schaden. Die Behandlung ist Teil der üblichen Störungsbehebung.

(7) Ein **Notfall** ist ein länger andauernder Ausfall von Prozessen oder Ressourcen mit einem hohen oder sehr hohen Schaden. Die Behandlung eines Notfalls verlangt eine besondere Notfallorganisation.

(8) Eine **Krise** ist ein Notfall, der die Existenz der Institution oder die Gesundheit oder das Leben einer Person beeinträchtigt. Dabei beeinträchtigt eine Krise im größeren Umfang das öffentliche Leben. Die Krise kann von der Institution selbst behoben werden.

(9) Eine **Katastrophe** ist ein zeitlich nicht begrenztes Großschadensereignis. Dabei handelt es sich um die Steigerung einer Krise, welche nur mithilfe von externen Kräften behoben werden kann.

§ 2
Gegenstand und Geltungsbereich

(1) Diese Dienstanweisung soll sicherstellen, dass Informationswerte und personenbezogene Daten angemessen geschützt werden und die Verfügbarkeit von informationstechnischen bzw. kommunikationstechnischen Verfahren gewährleistet wird.

(2) Die hierfür notwendigen Sicherheitsmaßnahmen sind dem jeweiligen Schutzzweck angemessen am Stand der Technik auszurichten. Dies soll in Abwägung der Werte der zu schützenden Informationen und unter Beachtung des Aufwands an Personal- und Finanzmitteln geschehen.

(3) Diese Dienstanweisung gilt für die Beschäftigten des Landkreises Teltow-Fläming. Sie gilt nicht für die Beschäftigten, die im Jobcenter tätig sind.

§ 3
Grundsätze und Definition der IT-Sicherheit / Informationssicherheit

Informationssicherheit hat den Schutz von Informationen, einschließlich personenbezogener Daten, jeglicher Art und Herkunft zum Ziel. Dabei können Informationen sowohl auf dem Papier, auf Rechnern oder auch in Köpfen gespeichert sein.

Die meisten Informationen werden mit Informationstechnologie (IT) erstellt, gespeichert, transportiert oder weiterverarbeitet. Daher wird als Synonym auch der Begriff „IT-Sicherheit“ verwendet.

Mit dem Ziel der Informationssicherheit im Sinne von Informationssicherheit sind die drei Grundwerte verbunden:

- Vertraulichkeit,
- Integrität,
- Verfügbarkeit von Informationen.

sowie die Schutzziele:

- Authentizität,
- Nichtabstreitbarkeit,
- Verlässlichkeit.

Vertraulichkeit: Gewährleistung des physischen beziehungsweise logischen Zugangs zu Informationen nur für die Zugriffberechtigten,
Integrität: Sicherstellung der Richtigkeit und Vollständigkeit von Informationen und Verarbeitungsmethoden,
Verfügbarkeit: Gewährleistung des bedarfsorientierten Zugangs zu Informationen und zugehörigen Werten für berechtigte Benutzer;
Authentizität: Gewährleistung, dass ein Kommunikationspartner tatsächlich der vorgegebene ist. Informationen sind authentisch, wenn Ihre Quelle verifiziert werden kann.

Nichtabstreitbarkeit: Gewährleistung der Nachweisbarkeit gegenüber Dritten. Ziel ist es zu gewährleisten, dass der Versand von Daten und Informationen nicht in Abrede gestellt werden kann.
Verbindlichkeit: Zusammenfassung der Sicherheitsziele Authentizität und Nichtabstreitbarkeit. Dies bedeutet, dass die Informationsquelle ihre Identität bewiesen hat und der Empfang der Nachricht nicht in Abrede gestellt werden kann.

Risiken, die die Informationssicherheit gefährden, müssen durch geeignete Maßnahmen auf ein notwendiges Mindestmaß reduziert werden. Die Informationssicherheit unterliegt einem kontinuierlichen Verbesserungsprozess, an dem alle mitzuwirken haben. Die Umsetzung der Maßnahmen zur Informationssicherheit kann nicht allein durch das Amt für Digitalisierung und Informationstechnik erfolgen. Es handelt sich um eine interdisziplinäre Aufgabe, bei der alle Bereiche des Hauses mitzuwirken haben.

§ 4
Grundsätze und Definition des Informationssicherheitsmanagementsystems (ISMS)

Das ISMS umfasst alle Regelungen, die für die Steuerung und Lenkung einer Institution sorgen und letztlich das Ziel der Informationssicherheit erreichen. Dies geschieht nachvollziehbar mit Hilfe von definierten Instrumenten und Regelungen. Die grundlegenden Komponenten des ISMS sind:

- Managementprinzipien,
- Ressourcen,
- Beschäftigte
- Sicherheitsprozess.

Sicherheit ist kein unveränderlicher Zustand. Die Verwaltung ist ständigen Änderungen der internen und externen Rahmenbedingungen unterworfen. Daher sind die Sicherheitsmaßnahmen regelmäßig auf ihre Wirksamkeit und Angemessenheit von allen Beschäftigten laufend zu überprüfen. Finden sich Schwachstellen, müssen die Maßnahmen im eigenen Verantwortungsbereich angepasst und verbessert werden.

§ 5
Landrätin und Verantwortungsbereiche

(1) Die Landrätin/der Landrat trägt die Gesamtverantwortung für die Informationssicherheit. Es obliegt ihr/ihm, für die Umsetzung der Maßnahmen zur Gewährleistung der Informationssicherheit zu sorgen und die dafür benötigten Ressourcen bereitzustellen.

(2) Die Amtsleitungen, in deren Zuständigkeitsbereich Verarbeitungstätigkeiten unmittelbar zum Einsatz kommen, tragen die Verantwortung für die:

- Feststellung des Schutzbedarfes von Informationen gemäß § 11,
- Beteiligung der/des Informationssicherheitsbeauftragten, der Leitung des Amtes für Digitalisierung und Informationstechnik, der Leitung des Amtes für zentrale Steuerung, Organisation und Personal und der/des Datenschutzbeauftragten,
- Erstellung von Sicherheitskonzepten nach dem BSI-Standard 200-2,
- Durchführung von Risikoanalysen nach § 12
- Risikoeinschätzung und Behandlung von Risiken § 12 f.
- Umsetzung bzw. das Einfordern der Umsetzung von Sicherheitsmaßnahmen,
- Festlegung von Verantwortlichkeiten im Umgang mit den Informationen (z.B. Zugriffsrechte).

(3) Sofern keine Amtsstruktur vorliegt, ist die jeweilige Aufgabe auf Dezernatsebene zu erfüllen. Der Bereich der Landrätin/des Landrats wird insoweit als Dezernat behandelt. Unabhängig davon gilt die Dienstordnung.

§ 6
Informationssicherheits-Managementsystem-Team (ISM-Team)

(1) Das Team besteht aus:

- der/dem Informationssicherheitsbeauftragten,
- der Amtsleitung des Amtes zentralen Steuerung, Organisation und Personal,
- der Amtsleitung des Amtes Digitalisierung und Informationstechnik und
- der/dem Datenschutzbeauftragten.

(2) Die Aufgaben des Teams sind:

- die aufkommenden Risiken, die behandelt werden müssen, zu identifizieren,
- angemessene Maßnahmen nach Bedarf auszuwählen, umzusetzen und zu verbessern,
- die Wirksamkeit der umgesetzten Maßnahmen und Verfahren zu überwachen und
- die Arbeitsberichte zur Informationssicherheit zu erstellen.

(3) Die/der Informationssicherheitsbeauftragte leitet das ISM-Team und ist befugt, weitere Beschäftigte einzuladen.

(4) Die bestehenden Zuständigkeitsbereiche werden durch Entscheidungen des ISM-Teams nicht berührt.

§ 7
Informationssicherheitsbeauftragte*r

(1) Die/der Informationssicherheitsbeauftragte ist dafür verantwortlich:

- den Informationssicherheitsprozess zu steuern und an allen damit zusammenhängenden Aufgaben mitzuwirken,
- die Leitungsebene bei der Erstellung der Leitlinie zur Informationssicherheit zu unterstützen,
- die Erstellung des Sicherheitskonzepts und anderer Teilkonzepte und System-Sicherheitsrichtlinien zu koordinieren sowie weitere Richtlinien und Regelungen zur Informationssicherheit zu erlassen,
- die Umsetzung von Sicherheitsmaßnahmen zu initiieren und zu überprüfen,
- die Leitungsebene über die Informationssicherheit zu unterrichten,
- relevante Informationssicherheitsvorfälle zu untersuchen,
- Sensibilisierungs- und Schulungsmaßnahmen für die Beschäftigten zur Informationssicherheit zu initiieren, zu steuern und durchzuführen.

(2) Die/der Informationssicherheitsbeauftragte hat folgende Befugnisse:

- alle für die Prüfung notwendigen Auskünfte zu erhalten,
- Einsicht in Akten, Schriftstücke oder sonstige Unterlagen zu erhalten und diese auf Verlangen vorgelegt zu bekommen, die die Informationssicherheit betreffen
- Zutritt in alle Bereiche zu erhalten, in denen IT-Technik verwendet wird,
- Zutritt zum Serverraum sowie in weitere für die Gewährleistung der Informationssicherheit relevante Bereiche zu erhalten,
- umgehend die Leserechte für die angeforderten IT-Systeme und Komponenten zu erhalten.

§ 8
Amt für zentrale Steuerung, Organisation und Personal

Das Amt für zentrale Steuerung, Organisation und Personal steuert folgende Aufgaben:

- den Aufbau einer geeigneten Informationssicherheitsorganisation nach dem BSI-Standard 200-2,
- die Erstellung eines zentralen Notfallmanagements (Business-Continuity-Managements) nach dem BSI-Standard 200-4,
- die frühzeitige Einbindung der/des Informationssicherheitsbeauftragten in alle Verarbeitungstätigkeiten.

§ 9
Amt für Digitalisierung und Informationstechnik

Das Amt für Digitalisierung und Informationstechnik ist für folgende Aspekte verantwortlich:

- den sicheren Betrieb der IT und die Umsetzung geeigneter Sicherheitsmechanismen,
- die Umsetzung geeigneter Schutzmaßnahmen in Abstimmung mit der/dem Informationssicherheitsbeauftragten,
- die frühzeitige Einbindung der/ des Informationssicherheitsbeauftragten in alle Verarbeitungstätigkeiten und Projekte.

§ 10
Die Beschäftigten

(1) Die Beschäftigten sind verpflichtet:

- die geltenden Richtlinien und Sicherheitsstandards einzuhalten und
- einen potentiellen Sicherheitsvorfall unverzüglich der IT-Hotline unter der 1740 zu melden.

(2) Die Beschäftigten des Sachgebietes für Informationstechnik haben bei einem potentiellen Sicherheitsvorfall ohne Einhaltung des Dienstweges alle Mitglieder des ISM-Teams zu informieren.

§ 11
Schutzbedarf

(1) Der Schutzbedarf ist unter Berücksichtigung der Bedeutung einer Information/eines Datums festzustellen. Danach sind Sicherheitsmaßnahmen zu treffen.

Es wird nachfolgenden Kategorien unterschieden:

a) **normaler Schutzbedarf**: Die Schadensauswirkungen sind begrenzt und überschaubar.
b) **hoher Schutzbedarf**: Die Schadensauswirkungen können beträchtlich sein. (z.B. bei Verarbeitung personenbezogener Daten besonderer Kategorie.)
c) **sehr hoher Schutzbedarf**: Die Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmaß erreichen.

(2) Die Bestimmung des Schutzbedarfes ist unter Anwendung der nachfolgenden Schutzbedarfskategorien für alle Aufgaben durchzuführen. Die Dokumentation ist im Fachamt zu führen.

Tabelle 1: Zuordnung von Schadensszenario und Schutzbedarfskategorie nach BSI-200-2

Szenario	Schutzbedarfskategorie		
	normal	**hoch**	**sehr hoch**
Beeinträchtigung der persönlichen Unversehrtheit (Leib und Leben)	Keine Beeinträchtigung	Beeinträchtigungen möglich	Gravierende Beeinträchtigungen sind möglich; Gefahr für Leib und Leben droht.
Beeinträchtigung des informationellen Selbstbestimmungsrechts (Datenschutz)	Durch die Verarbeitung personenbezogener Daten könnten Betroffene gesellschaftlich oder wirtschaftlich beeinträchtigt werden; hier nur mit geringfügigen Konsequenzen.	Beeinträchtigungen hätten erhebliche wirtschaftliche oder soziale Konsequenzen und würden nicht toleriert.	Beeinträchtigungen hätten gravierende wirtschaftliche oder soziale Konsequenzen und sind unter keinen Umständen zu tolerieren.
Beeinträchtigung des Ansehens der Behörde	Eine geringe bzw. nur interne Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten.	Eine breite Ansehens- oder Vertrauens-beeinträchtigung ist zu erwarten.	Eine landesweite Ansehens- oder Vertrauensbeeinträchtigung, eventuell sogar existenzgefährdender Art, ist denkbar.
Verstoß gegen Gesetze, Vorschriften und Verträge	Nur geringe Konsequenzen Konventionalstrafen können ohne negative Auswirkungen auf den laufenden Haushalt bestritten werden	Erhebliche Konsequenzen Hohe Konventionalstrafen haben Auswirkungen auf Vorhaben im laufenden Haushalt.	Fundamentale Gesetzesverstöße Ruinöse Haftungsschäden sind mit laufenden Haushalt nicht bestreitbar.
Finanzielle Auswirkungen (finanzrelevante Regressforderungen)	Nur geringe Schäden Regressforderungen können ohne negative Auswirkungen auf den laufenden Haushalt bestritten werden.	Große Schäden haben Auswirkungen auf Vorhaben im laufenden Haushalt.	Sehr große Schäden sind mit laufenden Haushalt nicht bestreitbar.
Beeinträchtigung der Aufgabenerfüllung (intern, extern)	Die Beeinträchtigung würde von den Betroffenen als tolerabel eingeschätzt werden.	Die Beeinträchtigung würde von einzelnen Betroffenen als nicht tolerabel eingeschätzt.	Die Beeinträchtigung würde von allen Betroffenen als nicht tolerabel eingeschätzt werden.

Tabelle 2: Beispiele für Schutzbedarfskategorien

Szenario	Schutzbedarfskategorie		
	Normal	**hoch**	**sehr hoch**
Beispiel für die Beeinträchtigung der persönlichen Unversehrtheit (Leib und Leben)	Keine Gefahr	Hunger, leichte Verletzungen,	Gefährdung von Kindeswohl, Tod, dauerhafte Invalidisierung
Beispiele für die Beeinträchtigung des informationellen Selbstbestimmungsrechts (Datenschutz)	Name, Anschrift, Telefonnummer, Geburtsdatum. Berufs-, Dienst-, Amtsbezeichnungen, Titel, Telefonverzeichnisse, branchen- oder Geschäftsbeziehungen, Adressdaten von Funktionsträgern in einer Gemeinde, Daten über Mietverhältnisse, Geschäfts- und Vertragsbeziehungen, verwandtschaftliche Beziehungen, Familienstand, Bekanntenkreis	gesundheitliche Verhältnisse, Patientendaten, Sozialdaten, psychologische Daten, Daten zum Sexualleben, Religion, politische Anschauungen, Steuerdaten, Kontodaten, strafbare Handlungen, Ordnungswidrigkeiten, arbeitsrechtliche Verhältnisse, Personalaktendaten, Gewerkschaftszugehörigkeit, Unterbringung in Anstalten,	Adressen von V-Leuten bei Polizei oder Verfassungsschutz, Adressen von Personen, die dem Zeugenschutzprogramm unterliegen
Beispiele für die Beeinträchtigung des Ansehens der Behörde	Intern: erschwert /verzögerte Aufgabenerfüllung untergräbt Vertrauen in Arbeitgeber. Extern: erschwert/verzögerte Aufgabenerfüllung untergräbt Vertrauen in Behörde, Postings in sozialen Medien, Leserbriefe greifen das Thema auf.	Preisgabe von persönlichen Daten der Antragsteller*innen, Preisgabe von Dienstgeheimnissen führen zu hoher Aufmerksamkeit/Shitstorms in konventionellen und sozialen Medien.	Dauerhafte Arbeitsunfähigkeit der Behörde ohne konkreten Termin für die vollständige Wiederherstellung des Ausgangszustands und die Möglichkeit, die Bürger*innen angemessen zu informieren. Dies verstärkt das mediale Interesse und hat auch politische Auswirkungen.
Beispiele für die Verstöße gegen Gesetze, Vorschriften und Verträge	Die Rückstellungen betragen maximal 25 % oder wenn eine Konventionalstrafe unter 50.000€ droht.	Die Rückstellungen betragen maximal 50 % oder wenn eine Konventionalstrafe unter 200.000€ droht.	Die Rückstellungen betragen über 50 % oder wenn eine Konventionalstrafe über 200.000 € droht.

Szenario	Schutzbedarfskategorie		
	Normal	**hoch**	**sehr hoch**
Beispiele für die Finanzielle Auswirkungen (finanzrelevante Regressforderungen)	weniger als 50.000 €	weniger als 200.000 €	Alle Summen, die 200.000 € übersteigen.
Beispiele für die Beeinträchtigung der Aufgabenerfüllung	Die maximal tolerierbare Ausfallzeit ist größer als 24 Stunden und beträgt maximal 1 Monat.	Die maximal tolerierbare Ausfallzeit liegt zwischen einer und 24 Stunden.	Die maximal tolerierbare Ausfallzeit ist kleiner als eine Stunde.

§ 12
Risikoanalyse

(1) Es ist eine Risikoanalyse nach dem BSI-Standard 200-3 durchzuführen, wenn auf eines der Zielobjekte einer der folgenden Punkte zutrifft:

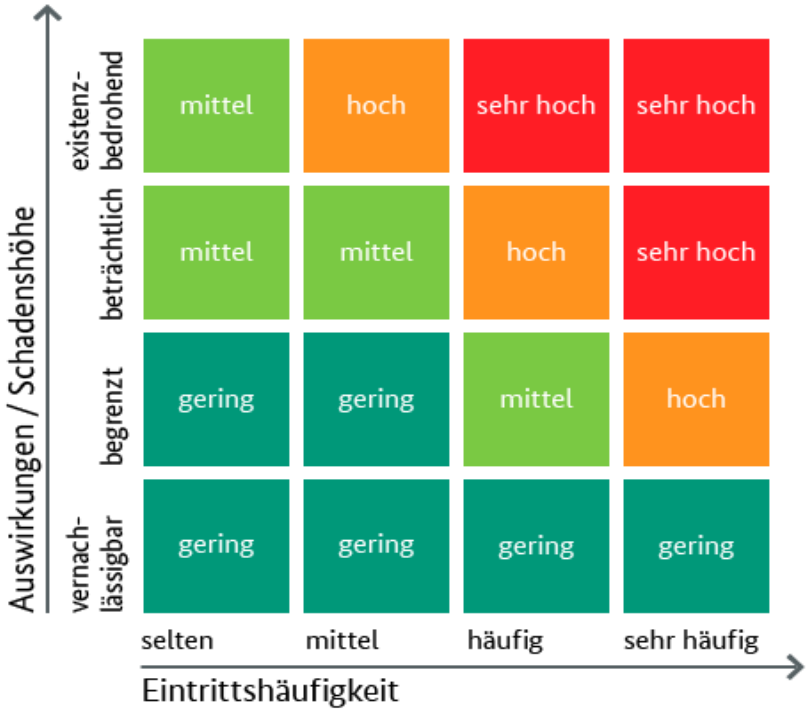
a) einen hohen oder sehr hohen Schutzbedarf in mindestens einen der drei Grundwerte nach § 3
b) nicht mit den Bausteinen des IT-Grundschutzes ausreichend abgebildet werden können
c) in Einsatzszenarien betrieben werden, die nicht im IT-Grundschutz vorgesehen sind

(2) Die anschließende Risikobewertung setzt sich aus der Eintrittshäufigkeit und der Schadenshöhe zusammen, welche für die einzelnen Schadensszenarien betrachtet werden. Die Eintrittshäufigkeit wird in vier Kategorien unterteilt:

a) selten: Ereignis könnte nach heutigem Kenntnisstand höchstens alle fünf Jahre eintreten.
b) mittel: Ereignis tritt einmal alle fünf bis einmal im Jahr ein.
c) häufig: Ereignis tritt einmal im Jahr bis einmal pro Monat ein.
d) sehr häufig: Ereignis tritt mehrmals im Monat ein.

(3) Die zu betrachtende Schadenshöhe ergibt sich aus den oben genannten Schutzbedarfskategorien.

(4) Ausgehend von der Eintrittshäufigkeit und der Schadenshöhe wird für jedes Szenario anhand folgender Matrix das Risiko bewertet:



(5) Die Risikokategorien sind wie folgt definiert:

a) gering: Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen bieten einen ausreichenden Schutz.

b) mittel: Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen reichen möglicherweise nicht aus.

c) hoch: Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen bieten keinen ausreichenden Schutz vor der jeweiligen Gefährdung.

d) sehr hoch: Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen bieten keinen ausreichenden Schutz vor der jeweiligen Gefährdung.

(6) Für die Kategorien mittel, hoch und sehr hoch sind darüber hinaus weitere Sicherheitsmaßnahmen zu treffen. Die Anforderungen hierfür sind in § 11 definiert.

§ 13 Risikobehandlung

(1) Zur Risikobehandlung sind grundsätzlich folgende Optionen möglich:

a) **Reduktion**: Risiken werden reduziert durch die Umsetzung weiterer Maßnahmen.
b) **Akzeptanz**: Restrisiken können von der Amtsleitung akzeptiert werden; hierzu ist es notwendig, dass das Fachamt die Behördenleitung nachweislich fundiert, vollständig, transparent und verständlich über die Restrisiken samt Folgen informiert.
c) **Transfer**: Risiken können transferiert werden, etwa an eine Versicherung oder einen Dienstleister.
d) **Vermeidung**: Risiken können aus dem Geltungsbereich des Informationsverbundes ausgeschlossen werden.

(2) Eine Akzeptanz von Risiken, die aus der Nichterfüllung von Basis-Anforderungen resultieren, ist nicht zulässig.

(3) Maßnahmen, die im Rahmen der Risikobehandlung festgesetzt werden, werden in einer Realisierungsplanung umgesetzt und vom Informationssicherheitsbeauftragten überprüft.

(4) Der Umsetzungsplan enthält mindestens folgende Informationen und ist Bestandteil der IT-Grundschutz-Methodik:

a) Maßnahme/-n
b) zugeordnetes Risiko aus der Risikoanalyse
c) Verantwortlichkeiten
d) Fristen
e) Status

§ 14
Schlussbestimmungen

Die 1. Änderung der Dienstanweisung tritt am Tag nach Veröffentlichung im Intranet in Kraft.

Luckenwalde, den 30. Juli 2024

Wehlan
Landrätin