Informationssicherheitsleitlinie der Gemeinde Sülzetal (*ISLL*)

Präambel

Die Leitlinie für Informationssicherheit beschreibt die Sicherheitsziele und das angestrebte Sicherheitsniveau der Gemeinde Sülzetal. Hier wird allgemeinverständlich beschrieben, für welche Zwecke, mit welchen Mitteln und mit welchen Strukturen Informationssicherheit innerhalb der Verwaltung erreicht werden soll. Sie beinhaltet außerdem die angestrebte Sicherheitsstrategie.

Versionsübersicht

Version	Bearbeitet durch	Bearbeitung am	Änderungen
1.0	Informationssicherheitsbeauftragter (ISB), Matthias Beck	15.09.2023	

Version	Freigabe durch	Freigabe am	Bemerkungen
1.0	Bürgermeister, Jörg Methner	30.09.2023	

Dokumentenschutz

Dokumentenschutz	
Ablageort	https://t1p.de/2ks3b
Lesezugriff	Alle Beschäftigten
Schreibzugriff	Büro des Bürgermeisters
Vertraulichkeitsstufe	Frei zugänglich
Bearbeitungsstatus	Freigegeben
Freigabeberechtigt	Bürgermeister
Eigentümer	ISB Matthias Beck

Inhaltsverzeichnis

§ 1 *Vorwort* 3
§ 2 Geltungsbereich 3
§ 3 Stellenwert der Informationssicherheit und der zu schützenden Objekte 3
§ 4 Bezug der Informationssicherheit zu den Geschäftszielen und Aufgaben der Gemeinde Sülzetal 4
§ 5 Sicherheitsziele 4
§ 6 Kernelemente der Sicherheitsstrategie 4
§ 7 Verpflichtung zur Umsetzung der Informationssicherheitsleitlinie 5
§ 8 Informationssicherheits-Organisation 6
§ 9 Verpflichtung zur kontinuierlichen Verbesserung 6
§ 10 Sprachliche Gleichstellung 7
§ 11 Inkrafttreten 7
Anlagen 7

§ 1 *Vorwort*

Informationssicherheit in Kommunen ist eng mit deren Aufgabenerfüllung verbunden. Diese ist allerdings nicht auf Dauer festgelegt, sondern entwickelt sich durch wandelnde gesellschaftliche und politische Erwartungen an die öffentliche Verwaltung. Steigende Einwohnerzahlen, höhere Einwohnerdichte, technische Entwicklung, gestiegene Erwartungen an den Umweltschutz, gestiegene Ansprüche durch höheren Lebensstandard führen sowohl der Zahl wie auch dem Umfang und der Intensität nach zu ständig wachsenden Aufgaben der Kommunen.

Unzählige medial verbreitete Sicherheitsvorfälle der letzten Jahre, gleich ob im kommunalen oder privatwirtschaftlichen Sektor, belegen die Dringlichkeit das Thema Informationssicherheit geordnet anzugehen.

Über die letzten Jahrzehnte haben dabei die Anforderungen an die Verfügbarkeit von Informationen stetig zugenommen. Dadurch bedingt hat auch die Sicherheit der Informationstechnik (IT) einen größeren Stellenwert eingenommen. Die Komplexität der Abläufe, der hohe Grad der Vernetzung und die Abhängigkeit der Verwaltung von IT-gestützten Verfahren verlangen nach einer Systematisierung und Organisation der Informationssicherheit – nach einem Informationssicherheits-Managementsystem (ISMS).

Die Grundlage für ein solches System ist ein Bekenntnis der Behördenleitung zur Informationssicherheit. Dieses Bekenntnis wird durch diese Informationssicherheitsleitlinie (ISLL) verbrieft.

Das Ziel dieser Informationssicherheitsleitlinie und der Einführung eines ISMS ist es, ein Grundverständnis und eine Informationssicherheits-Kultur in der Gemeindeverwaltung Sülzetal zu schaffen.

Wichtig hierbei ist, die Informationssicherheit umfasst neben IT-Systemen auch Papierunterlagen in Form von Akten und sonstigen Papierdokumenten und Daten im allgemeinen Sinn. Die Informationssicherheit umfasst die Summe aller organisatorischen, personellen und technischen Maßnahmen. Somit sind alle Beschäftigten für die Informationssicherheit zuständig.

Der sichere Umgang mit den Daten unserer Bürger, unserer ortsansässigen Unternehmen und sonstigen Partner ist uns ein dringliches Anliegen.

§ 2 Geltungsbereich

Diese Leitlinie gilt für die gesamte Verwaltung sowie alle Einrichtungen und Betriebe der Gemeinde Sülzetal. Die Leitlinie und die daraus resultierenden Vorschriften und Maßnahmen sind von allen Mitarbeitern der Gemeinde Sülzetal zu beachten und einzuhalten.

§ 3 Stellenwert der Informationssicherheit und der zu schützenden Objekte

Die Gemeinde Sülzetal besitzt eine enorme Aufgabenvielfalt – von der Daseinsfürsorge bis zu Dienstleistungen für Bürgerinnen und Bürger, die zusätzlich permanenten Änderungen unterliegt. Eine wirtschaftliche, zeitnahe Aufgabenerfüllung stützt sich dabei zunehmend auf die Möglichkeiten der Informationstechnologien.

Aufgaben, Prozesse und die Aufbauorganisation unterliegen einem stetigen Wandel und einer Anpassung der technischen Möglichkeiten.

In Abwägung der zu schützenden Werte, der gesetzlichen Anforderungen, Informationen und der damit verbundenen Risiken wird ein angemessenes Informationssicherheitsniveau geschaffen.

Modernes Verwaltungshandeln erfordert den Einsatz aktueller Informationstechnologien, um die Aufgabenerfüllung der Kommunalverwaltung im Sinne der Bürgerinnen und Bürger, ortsansässiger Unternehmen oder weiterer Partner effizient und effektiv zu gestalten. Dies trifft auch auf die Gemeinde Sülzetal zu. Beim Einsatz von Informationstechnologie muss die Gemeinde Sülzetal darauf achten, dass der Sensibilität der ihr übertragenen und von ihr

verarbeiteten Informationen mit der nötigen Sorgfalt Rechnung getragen wird. Die Informationssicherheit wird in zunehmendem Maße zu einer unverzichtbaren Grundlage für ein Verwaltungshandeln, dem die Bürgerinnen und Bürger, die Unternehmen und alle unsere Partner ihr Vertrauen schenken können. Daher muss sich die Gemeinde Sülzetal dem Thema Sicherheit in der Informationstechnik in geeigneter Form stellen und die verarbeiteten Informationen geeignet schützen.

§ 4 Bezug der Informationssicherheit zu den Geschäftszielen und Aufgaben der Gemeinde Sülzetal

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

Sowohl bei der Erbringung der Pflichtaufgaben als auch der Aufgaben, die die Gemeinde Sülzetal auf freiwilliger Basis übernimmt, werden Informationen erhoben und verarbeitet, deren Vertraulichkeit, Integrität und Verfügbarkeit ein hohes Gut darstellen. Hierbei handelt es sich z. B. um Daten, die entsprechend gesetzlicher Anforderungen geschützt werden müssen, oder auch um wettbewerbsrelevante Informationen ortsansässiger Unternehmen, die Unberechtigten nicht bekannt werden dürfen.

§ 5 Sicherheitsziele

Für den IT-Einsatz sind die Grundwerte der Informationssicherheit - Vertraulichkeit, Integrität und Verfügbarkeit - im jeweils erforderlichen Maße zu erreichen.

Jede Leistung, Aufgabe oder Information wird nach einem Schutzbedarf eingestuft. Die Einstufung gibt die Anforderungen bezüglich der Grundwerte wieder. Die Feststellung des Schutzbedarfes erfolgt gemäß der Anlage 1 Schutzbedarfskategorien.

Damit ist es ein grundlegendes Ziel der Aufgabenerfüllung, die Schutzbedürfnisse der verarbeiteten Informationen zu wahren. Über geeignete Sicherheitsmaßnahmen muss dafür gesorgt werden, dass die Vertraulichkeit, die Integrität und die Verfügbarkeit der Informationen ihrem Schutzbedarf entsprechend gewährleistet werden können. Hierbei sind rechtliche Bestimmungen zu berücksichtigen. Um dies in einer auch wirtschaftlich angemessenen Form zu tun, ist es unabdingbar, den Schutzbedarf der Informationen zu kennen und dann die zu diesem Schutzbedarf passenden Maßnahmen zu ergreifen.

§ 6 Kernelemente der Sicherheitsstrategie

Die ISLL ist ein Rahmenwerk.

Die Gemeinde Sülzetal erlässt nach Bedarf weitere Richtlinien zur Aufrechterhaltung der Informationssicherheit. Die Kommunalverwaltung führt eine Bedarfsermittlung durch und legt die Mindestsicherheitsstandards für ihre eigenen Verfahren fest. Bei Ebenen übergreifenden Verfahren sind die entsprechenden Festlegungen des Bundes oder des Landes umzusetzen.

Als zentrale Sicherheitsinstanz ernennt der Bürgermeister einen Informationssicherheitsbeauftragten und einen Stellvertreter, der für alle Belange und Fragen der Informationssicherheit zuständig ist.

Der Informationssicherheitsbeauftragte ist unabhängig und weisungsfrei. Er ist der Behördenleitung in dieser Rolle direkt unterstellt. Berichtswege sind festzulegen.

Ein Austausch mit der Leitung der Informationstechnik findet regelmäßig statt.

Dem Informationssicherheitsbeauftragten sind geeignete Qualifizierungsmaßnahmen zu ermöglichen, um seine Verantwortung fachlich und zeitlich zu erfüllen.

Ein Informationssicherheits-Managementsystem (ISMS) ist zu etablieren. In regelmäßigen Abständen ist zu prüfen, ob die ausgewählten Sicherheitsmaßnahmen noch ausreichend

sind. Der Informationssicherheitsbeauftragte leitet das IS-Management-Team und entwickelt die notwendigen Maßnahmen fort.

Bei Gefahr im Verzug ist der Informationssicherheitsbeauftragte oder sein Stellvertreter berechtigt, erforderliche Sicherheitsmaßnahmen auch kurzfristig umzusetzen oder anzuordnen. Das kann bis zur vorübergehenden Sperrung von Anwendungen oder Netzübergängen führen.

Personen und Unternehmen, die nicht zur Gemeinde Sülzetal gehören, für diese aber Leistungen erbringen (Auftragnehmer), haben die Vorgaben des Auftraggebers zur Einhaltung der Informationssicherheitsziele gemäß dieser ISLL einzuhalten. Der Auftraggeber informiert den Auftragnehmer über diese Regeln und verpflichtet ihn in geeigneter Weise zur Einhaltung.

Sicherheitsanforderungen von übergeordnetem Interesse, für deren Umsetzung eine vertragliche oder gesetzliche Verpflichtung besteht, sind zu erfüllen. Entsprechende Vorschriften und Maßnahmen stellen den Mindeststandard bei der Formulierung behördeninterner Vorschriften und Maßnahmen dar. Gemeinsame Basiskomponenten innerhalb der Behörde zur Vereinfachung und Stärkung der Ebenen übergreifenden Verfahren sind zu nutzen.

Die Beschäftigten werden regelmäßig zu Fragen der Informationssicherheit sensibilisiert und qualifiziert.

Die vorliegende ISLL gibt den Rahmen für das Management der Informationssicherheit bei der Gemeinde Sülzetal vor. Die wesentlichen Eckpunkte und Kernelemente der Strategie zur Informationssicherheit sind:

(1) Die Gemeinde Sülzetal etabliert ein Informationssicherheitsmanagementsystem (ISMS) mit einem geeigneten Werkzeug zur Steuerung.
(2) Die Gemeinde Sülzetal verankert das Thema Informationssicherheit in der Organisation über
    a) eine geeignete IS-Organisation, die aktiv das Thema Informationssicherheit betreibt,
    b) klar formulierte Sicherheitsvorgaben, die für alle Beschäftigten verbindlich sind,
    c) die Integration von Sicherheitsaspekten in alle aus Sicht der Informationssicherheit relevanten Prozesse,
    d) kontinuierliche und flächendeckende Sensibilisierungsmaßnahmen für alle Beschäftigten.
(3) Die Gemeinde Sülzetal sorgt sukzessive für eine Absicherung der IT-Infrastruktur durch Umsetzung geeigneter Sicherheitsmaßnahmen auf der Infrastrukturebene.
(4) Die Gemeinde Sülzetal orientiert sich bei allen Aktivitäten zur Informationssicherheit an den aktuellen Standards und Best Practices.

§ 7 Verpflichtung zur Umsetzung der Informationssicherheitsleitlinie

Der Bürgermeister trägt die Gesamtverantwortung für die Informationssicherheit. Es obliegt ihr, für die Umsetzung der Maßnahmen zur Gewährleistung der Informationssicherheit zu sorgen und die dafür benötigten Ressourcen bereitzustellen.

Die Gemeinde Sülzetal orientiert sich für die Umsetzung von Informationssicherheit am IT-Grundschutz.

Der Aufwand für die Bereitstellung von Personal und Finanzmitteln zur Gewährleistung der Informationssicherheit soll für die eingesetzten und geplanten IT-Systeme ein angemessenes Informationssicherheitsniveau schaffen. Zur Umsetzung der Maßnahmen sind erforderliche Ressourcen und Investitionsmittel einzuplanen.

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

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

§ 8 Informationssicherheits-Organisation

Für bereits betriebene und für geplante Informationstechnik sind Sicherheitskonzepte zu erstellen. Der Schutzbedarf ist zunächst aus fachlicher Sicht für die Leistungen und Aufgaben zu erstellen. Anschließend wird der Schutzbedarf auf die Zielobjekte der Informationstechnik und Infrastruktur übertragen (vererbt).

Die Maßnahmen sind auch dann umzusetzen, wenn sich Beeinträchtigungen für die Nutzung ergeben. Bleiben Risiken untragbar, ist an dieser Stelle auf den Einsatz von Informationstechnik zu verzichten.

Die Verantwortlichen haben bei Verstößen und Beeinträchtigungen die zur Aufrechterhaltung des Betriebes und der Informationssicherheit geeigneten und angemessenen Maßnahmen zu ergreifen.

Unabhängig davon, ob und in welcher Weise Teilaufgaben delegiert werden, verbleibt die Gesamtverantwortung für die Gewährleistung der Informationssicherheit immer beim Bürgermeister.

Der Bürgermeister ernennt einen Informationssicherheitsbeauftragten, der alle notwendigen Maßnahmen mit dem Bürgermeister und den Fachbereichsleitern abstimmt und für deren Umsetzung verantwortlich zeichnet. Die Informationssicherheit gehört zu den Dienstpflichten aller Beschäftigten. Nur wenn alle Beschäftigten ihre Verantwortung in der täglichen Arbeit wahrnehmen, kann ein geeignetes Niveau der Informationssicherheit erreicht werden.

§ 9 Verpflichtung zur kontinuierlichen Verbesserung

Der Bürgermeister und die Fachbereichsleiter verpflichten sich, sich an der Optimierung der Informationssicherheit zu beteiligen. Sie sind regelmäßig bzw. im Einzelfall akut über den aktuellen Sicherheitszustand durch den IT-Sicherheitsbeauftragen zu informieren und sind für die Absicherung der Kontinuität des Sicherheitsprozesses verantwortlich.

Die Sicherheitsmaßnahmen sind regelmäßig daraufhin zu untersuchen, ob sie den betroffenen Beschäftigten bekannt, umsetzbar und in den Betriebsablauf integrierbar sind.

Zur Erhaltung und Verbesserung der Informationssicherheit bedient sich der Informationssicherheitsbeauftragte einer Arbeitsgruppe "Informationssicherheit", die aus Vertretern aller Fachbereiche besteht.

Der Informationssicherheitsbeauftragte ist bei allen organisatorisch-technischen Neuerungen oder Änderungen, die Auswirkungen auf die Informationssicherheit haben können, frühzeitig einzubinden. Er hat ein Vetorecht.

Durch eine kontinuierliche Betrachtung der Regelungen und deren Einhaltung wird das angestrebte Sicherheitsniveau sichergestellt. Abweichungen werden mit dem Ziel analysiert, die Informationssicherheit zu verbessern und ständig auf dem aktuellen Stand zu halten.

Verantwortlich für die Weiterentwicklung der ISLL und der IT-Sicherheitskonzepte ist der Informationssicherheitsbeauftragte, wobei er von den Beschäftigten bestmöglich unterstützt

wird. Die Beschäftigten sind angehalten, mögliche Verbesserungen oder Schwachstellen an den Informationssicherheitsbeauftragten weiterzugeben.

Informationssicherheit ist kein unveränderlicher Zustand, sondern hängt von vielen internen und externen Begebenheiten und Einflüssen ab, wie z. B. von neuen Bedrohungen, neuen Gesetzen oder auch der Entwicklung neuer technischer Lösungen. Diesen Entwicklungen müssen sich die Ansätze zum Management der Informationssicherheit anpassen. Aus diesem Grund muss dafür Sorge getragen werden, dass sich die Sicherheitsstrategie der Gemeinde Sülzetal kontinuierlich fortentwickelt.

§ 10 Sprachliche Gleichstellung

Personen- und Funktionsbezeichnungen gelten jeweils für Personen mit männlichem, weiblichem und diversem Geschlecht sowie für Personen ohne Geschlechtsangabe.

§ 11 Inkrafttreten

Diese Leitlinie tritt *am Tag nach der Bekanntgabe an die Beschäftigten* in Kraft.

Sülzetal, ...

Jörg Methner
Bürgermeister

Dienstsiegel

Gemeinde Sülzetal
1
Landkreis Börde

Anlagen

1 Schutzbedarfskategorien

Anlage 1

Informationssicherheitsleitlinie der Gemeinde Sülzetal
Schutzbedarfskategorien

Definition der Schutzbedarfskategorien

Da der Schutzbedarf meist nicht quantifizierbar ist, beschränkt sich der IT-Grundschutz somit auf eine qualitative Aussage, indem der Schutzbedarf in drei Kategorien unterteilt wird:

Schutzbedarfskategorien	
„normal“	Die Schadensauswirkungen sind begrenzt und überschaubar.
„hoch“	Die Schadensauswirkungen können beträchtlich sein.
„sehr hoch“	Die Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmaß erreichen.

Tabelle 1: Schutzbedarfskategorien

Hinweise zur Festlegung

Die Schäden, die bei dem Verlust der Vertraulichkeit, Integrität, oder Verfügbarkeit für einen Geschäftsprozess bzw. eine Anwendung einschließlich ihrer Daten entstehen können, lassen sich typischerweise folgenden Schadensszenarien zuordnen:

(1) Verstoß gegen Gesetze/ Vorschriften/ Verträge
(2) Beeinträchtigung des informationellen Selbstbestimmungsrechts
(3) Beeinträchtigung der persönlichen Unversehrtheit
(4) Beeinträchtigung der Aufgabenerfüllung
(5) Negative Innen- oder Außenwirkung
(6) Finanzielle Auswirkungen

Häufig treffen dabei für einen Schaden mehrere Schadensszenarien zu. So kann beispielsweise der Ausfall einer Anwendung die Aufgabenerfüllung beeinträchtigen, was direkte finanzielle Einbußen nach sich zieht und gleichzeitig auch zu einem Imageverlust führt.

Verantwortlich für die Abgrenzung der Schutzbedarfskategorien in „normal“, „hoch“ und „sehr hoch“ ist der Prozessverantwortliche. Hier bietet es sich an, die Grenzen für einzelne Schadensszenarien zu bestimmen. Außerdem ist eine enge Kommunikation mit der Behördenleitung unabdingbar. Die Notwendigkeit der Einbindung des IT-Leiters, des Informationssicherheitsbeauftragten oder des Datenschutzbeauftragten ist zu empfehlen.

Schutzbedarfsfeststellung und Schlussfolgerungen nach BSI-Standard 200-2 „IT-Grundschutz-Vorgehensweise“

(Für jedes der Schutzziele **„Vertraulichkeit“**, **„Integrität“** und **„Verfügbarkeit“** gesondert anzuwenden.)

Schutzbedarfskategorie „normal“	
1. Verstoß gegen Gesetze/ Vorschriften/Verträge	• Verstöße gegen Vorschriften und Gesetze mit geringfügigen Konsequenzen • Geringfügige Vertragsverletzungen mit maximal geringen Konventionalstrafen
2. Beeinträchtigung des informationellen Selbstbestimmungsrechts	• Es handelt sich um personenbezogene Daten, durch deren Verarbeitung der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigt werden kann
3. Beeinträchtigung der persönlichen Unversehrtheit	• Eine Beeinträchtigung erscheint nicht möglich.
4. Beeinträchtigung der Aufgabenerfüllung	• Die Beeinträchtigung würde von den Betroffenen als tolerabel eingeschätzt werden. • Die maximal tolerierbare Ausfallzeit liegt zwischen 24 und 72 Stunden.
5. Negative Innen- oder Außenwirkung	• Eine geringe bzw. nur interne Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten.
6. Finanzielle Auswirkungen	• Der finanzielle Schaden bleibt für die Institution tolerabel.

Tabelle 2: Schutzbedarfskategorie „normal“

Schutzbedarfskategorie „hoch“	
1. Verstoß gegen Gesetze/ Vorschriften/Verträge	• Verstöße gegen Vorschriften und Gesetze mit erheblichen Konsequenzen • Vertragsverletzungen mit hohen Konventionalstrafen
2. Beeinträchtigung des informationellen Selbstbestimmungsrechts	• Es handelt sich um personenbezogene Daten, bei deren Verarbeitung der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigt werden kann.
3. Beeinträchtigung der persönlichen Unversehrtheit	• Eine Beeinträchtigung der persönlichen Unversehrtheit kann nicht absolut ausgeschlossen werden.
4. Beeinträchtigung der Aufgabenerfüllung	• Die Beeinträchtigung würde von einzelnen Betroffenen als nicht tolerabel eingeschätzt • Die maximal tolerierbare Ausfallzeit liegt zwischen einer und 24 Stunden.
5. Negative Innen- oder Außenwirkung	• Eine breite Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten.

6. Finanzielle Auswirkungen	• Der Schaden bewirkt beachtliche finanzielle Verluste, ist jedoch nicht existenzbedrohend.

Tabelle 3: Schutzbedarfskategorie „hoch“

Schutzbedarfskategorie „sehr hoch“	
1. Verstoß gegen Gesetze/ Vorschriften/Verträge	• Fundamentaler Verstoß gegen Vorschriften und Gesetze • Vertragsverletzungen, deren Haftungsschäden ruinös sind
2. Beeinträchtigung des informationellen Selbstbestimmungsrechts	• Es handelt sich um personenbezogene Daten, bei deren Verarbeitung eine Gefahr für Leib und Leben oder die persönliche Freiheit des Betroffenen gegeben ist.
3. Beeinträchtigung der persönlichen Unversehrtheit	• Gravierende Beeinträchtigungen der persönlichen Unversehrtheit sind möglich. • Gefahr für Leib und Leben
4. Beeinträchtigung der Aufgabenerfüllung	• Die Beeinträchtigung würde von allen Betroffenen als nicht tolerabel eingeschätzt werden. • Die maximal tolerierbare Ausfallzeit ist kleiner als eine Stunde.
5. Negative Innen- oder Außenwirkung	• Eine landesweite Ansehens- oder Vertrauensbeeinträchtigung, eventuell sogar existenzgefährdender Art, ist denkbar.
6. Finanzielle Auswirkungen	• Der finanzielle Schaden ist für die Institution existenzbedrohend.

Tabelle 4: Schutzbedarfskategorie „sehr hoch“