Kreisrechtssammlung Landkreis Osterholz

zuständiges Amt	KRS-Nr.
Hauptamt – Amt 10	**7.28**

Kurzbezeichnung

Informationssicherheitsleitlinie

Informationssicherheitsleitlinie

Dokumentenhistorie

Version	Datum	Status	Bemerkung
0.1	21.03.2019	In Abstimmung	
0.2	04.04.2019	Mit PLG Datenschutz abgestimmt	
1.0	16.05.2019	In Kraft getreten	
1.1	29.08.2019	Redaktionell überarbeitet	Rechtschreibfehler korrigiert

Inhaltsverzeichnis

1 Einleitung

Der Landkreis Osterholz besitzt eine enorme Aufgabenvielfalt, von der Daseinsfürsorge bis zu Dienstleistungen für Bürgerinnen und Bürger, die zusätzlich permanenten Änderungen unterliegt. Eine wirtschaftliche und 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 und weiterer Partner effizient und effektiv zu gestalten.

Beim Einsatz von Informationstechnologie achtet der Landkreis Osterholz darauf, dass der Sensibilität der ihm übertragenen und von ihm 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, die Mitarbeiterinnen und Mitarbeiter sowie alle Geschäftspartner ihr Vertrauen schenken können. Daher stellt sich der Landkreis Osterholz dem Thema Sicherheit in der Informationstechnik in geeigneter Form um die verarbeiteten Informationen geeignet zu schützen.

2 Geltungsbereich

Die Richtlinie Informationssicherheit gilt für die Verwaltung des Landkreises Osterholz. Sie gilt nicht für die Eigenbetriebe, Gesellschaften und Beteiligungen des Landkreises Osterholz, kann aber von diesen übernommen werden.

3 Bezug zu den Leistungen des Landkreises

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 der Landkreis Osterholz 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.

4 Sicherheitsziele

Zur Abbildung des hohen Stellenwertes der Informationssicherheit werden für die Landkreisverwaltung die nachstehenden Sicherheitsziele festgelegt, für die geeignete Sicherheitsniveaus definiert werden:

- **Vertraulichkeit**
  Informationen dürfen ausschließlich einem berechtigten Personenkreis zur Verfügung stehen.

- **Integrität**
  Die physische und logische Unversehrtheit von Systemen, Anwendungen und Daten muss jederzeit gewahrt sein. Dieses umfasst auch die unberechtigte Erstellung oder Änderung von Informationen.

- **Verfügbarkeit**
  Systeme, Anwendungen und Daten müssen den Berechtigten in jeder Situation wie vorgesehen zur Verfügung stehen.

Sie sind im jeweils erforderlichen Maße zu erreichen, d.h. bei der Erreichung dieser Ziele ist eine Verhältnismäßigkeit der eingesetzten Mittel zum Wert der schützenswerten Güter zu beachten.

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 Schutzbedarfskategorien.

Damit ist es ein grundlegendes Ziel der Aufgabenerfüllung, die Schutzbedürfnisse der verarbeiteten Informationen zu wahren. Über geeignete Sicherheitsmaßnahmen ist dafür Sorge zu tragen, dass die Sicherheitsziele 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.

5 Sicherheitsstrategie

Die Informationssicherheitsleitlinie ist ein Rahmenwerk. Der Landkreis Osterholz erlässt nach Bedarf weitere Richtlinien oder Dienstanweisungen zur Aufrechterhaltung der Informationssicherheit. Er führt eine Bedarfsermittlung durch und legt die Mindestsicherheitsstandards für seine eigenen Verfahren fest. Bei ebenenübergreifenden Verfahren sind die entsprechenden Festlegungen des Bundes oder des Landes umzusetzen.

Als zentrale Sicherheitsinstanz ernennt die Behördenleitung eine/n Informationssicherheitsbeauftragte/n und eine/n Stellvertreter/Stellvertreterin, die oder 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 erfüllen zu können.

Ein Informationssicherheitsmanagementsystem (ISMS) ist zu etablieren. In regelmäßigen Abständen ist zu prüfen, ob die ausgewählten Sicherheitsmaßnahmen noch ausreichend sind. Der Informationssicherheitsbeauftragte leitet das ISM-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 zum Landkreis Osterholz gehören, für diesen 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 ebenenübergreifenden 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 beim Landkreis Osterholz vor. Die wesentlichen Eckpunkte und Kernelemente der Strategie zur Informationssicherheit sind:

- Der Landkreis Osterholz etabliert ein Informationssicherheitsmanagementsystem (ISMS) mit einem geeigneten Werkzeug zur Steuerung.
- Der Landkreis Osterholz verankert das Thema Informationssicherheit in der Organisation
  - über eine geeignete ISM-Organisation, die aktiv das Thema Informationssicherheit betreibt,
  - klar formulierte Sicherheitsvorgaben, die für alle Beschäftigten verbindlich sind,
  - die Integration von Sicherheitsaspekten in alle aus Sicht der Informationssicherheit relevanten Prozesse,
  - kontinuierliche und flächendeckende Sensibilisierungsmaßnahmen für alle Beschäftigten.
- Der Landkreis Osterholz sorgt sukzessive für eine Absicherung der IT-Infrastruktur durch Umsetzung geeigneter Sicherheitsmaßnahmen auf der Infrastrukturebene.

6 Pflichten und Berichtswege

Die Behördenleitung 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.

Der Landkreis Osterholz orientiert sich für die Umsetzung von Informationssicherheit am IT-Grundschutz und der Norm ISO/IEC 27001 der „International Organization for Standardization" (ISO), der mindestens dem Standard-Schutzbedarf des BSI entspricht.

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. Die Behördenleitung ist zu informieren, falls notwendige Sicherheitsmaßnahmen aus bestimmten Gründen nicht umgesetzt werden können.

7 Sicherheitsorganisation

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 geeignete und angemessene Maßnahmen zu ergreifen.

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

Die Behördenleitung kann die Verantwortung für die laufenden Angelegenheiten zum Informationssicherheitsmanagement an eine oder mehrere Verantwortliche beim Landkreis Osterholz delegieren. Sie ernennt eine/n für die gesamte Kommunalverwaltung zuständigen Informationssicherheitsbeauftragte/n. Das ISM wird durch ein ISM-Team aufgebaut und betrieben, das die für das Informationssicherheitsmanagement notwendigen Aufgaben und Maßnahmen definiert und koordiniert. Hierzu gehören auch Vorschläge für die weitere Ausgestaltung der ISM-Organisation.

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.

8 Umsetzung

Die Behördenleitung verpflichtet sich, sich an der Optimierung der Informationssicherheit zu beteiligen. Sie ist regelmäßig und bedarfsweise im Einzelfall über den aktuellen Sicherheitszustand durch die/den Informationssicherheitsbeauftrage/n zu informieren und ist 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 „Informationssicherheitsmanagement-Team" (ISM-Team).

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 Informationssicherheitskonzepte ist der Informationssicherheitsbeauftragte, wobei er von den Fachverantwortlichen bestmöglich unterstützt wird. Die Beschäftigten sind angehalten, mögliche Verbesserungen oder Schwachstellen an die entsprechenden Stellen weiterzugeben. Informationssicherheit ist kein unveränderlicher Zustand, sondern hängt von vielen internen und externen Begebenheiten und Einflüssen ab, wie z. B. 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 des Landkreises Osterholz kontinuierlich fortentwickelt.

9 Inkraftsetzung

Diese Leitlinie ist mit Wirkung vom 16.05.2019 in Kraft getreten.

10 Anlage Schutzbedarfsdefinition

10.1 Definition der Schutzbedarfskategorien

Ziel: Auswahl eines dreistufigen Bewertungsmodelles für die Schutzbedarfskategorien in Anlehnung an den IT-Grundschutz nach BSI-Standard 200-2 für die Grundwerte der Informationssicherheit: Vertraulichkeit, Verfügbarkeit und Integrität.

Schutzbedarf	Schadensauswirkung
Normal	Die Schadensauswirkungen sind begrenzt und überschaubar, d.h. Schäden haben Beeinträchtigungen der Institution zur Folge.
Hoch	Die Schadensauswirkungen können beträchtlich sein, d.h. im Schadensfall tritt Handlungsunfähigkeit zentraler Bereiche der Institution ein. Schäden haben erhebliche Beeinträchtigungen der Institution selbst oder betroffener Dritter zur Folge.
Sehr hoch	Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß erreichen, d.h. der Ausfall der IT oder wesentlicher Geschäftsprozesse oder die Offenlegung bzw. Manipulation von kritischen Informationen führt zum Zusammenbruch der Institution oder hat schwerwiegende Folgen für breite gesellschaftliche oder wirtschaftliche Bereiche.

10.2 Hinweise zur Festlegung

Folgende Schadensszenarien sind zu berücksichtigen. Im Einzelfall wird geprüft, ob ggf. weitere Schadensszenarien möglich sind:

1) Beeinträchtigung von Leib- und Leben (persönliche Unversehrtheit)
2) Verursachung finanzieller Schäden (Grundsatz der Wirtschaftlichkeit und Sparsamkeit)
3) Beeinträchtigung des Ansehens der Behörde
4) Verletzung des Rechts auf informationelle Selbstbestimmung
5) Verletzung von Gesetzen, Vorschriften oder Verträgen
6) Beeinträchtigung der Aufgabenerfüllung (Intern, Extern)

Es können ein oder mehrere Schadensszenarien einzeln oder zur gleichen Zeit auftreten. Verantwortlich für die Festlegung ist der Prozessverantwortliche. Zur Unterstützung bei dieser Abgrenzung ist eine enge Kommunikation mit der Behördenleitung erforderlich. Die Notwendigkeit der Einbindung der 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.)

Schutzbedarfs-kategorien / **Schadens-szenarien**		**Normal**	**Hoch**	**Sehr hoch**
		Die Schadensauswirkungen sind begrenzt und überschaubar.	*Die Schadensauswirkungen können beträchtlich sein.*	*Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß erreichen.*
1	Verstoß gegen Gesetze / Vorschriften / Verträge	• Verstöße gegen Vorschriften und Gesetze mit geringfügigen Konsequenzen • Geringfügige Vertragsverletzungen mit maximal geringen Konventionalstrafen	• Verstöße gegen Vorschriften und Gesetze mit erheblichen Konsequenzen • Vertragsverletzungen mit hohen Konventionalstrafen	• Fundamentaler Verstoß gegen Vorschriften und Gesetze • Vertragsverletzungen, deren Haftungsschäden ruinös sind
2	Beeinträchtigung des informationellen Selbstbestimmungs-rechts	Es handelt sich um personenbezogene Daten, durch deren Verarbeitung der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigt werden kann.	• Verstöße gegen Vorschriften und Gesetze mit erheblichen Konsequenzen • Vertragsverletzungen mit hohen Konventionalstrafen	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	Eine Beeinträchtigung erscheint nicht möglich	Eine Beeinträchtigung der persönlichen Unversehrtheit kann nicht absolut ausgeschlossen werden.	• Gravierende Beeinträchtigungen der persönlichen Unversehrtheit sind möglich. • Gefahr für Leib und Leben
4	Beeinträchtigung der Aufgabenerfüllung	• Die Beeinträchtigung würde von den Betroffenen als tolerabel eingeschätzt werden. • Die maximal tolerierbare Ausfallzeit ist größer als 24 Stunden.	• Die Beeinträchtigung würde von einzelnen Betroffenen als nicht tolerabel eingeschätzt. • Die maximal tolerierbare Ausfallzeit liegt zwischen einer und 24 Stunden.	• 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 geringe bzw. nur interne Ansehens- oder Vertrauens-beeinträchtigung ist zu erwarten.	Eine breite Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten.	Eine landesweite Ansehens- oder Vertrauensbeeinträchtigung, eventuell sogar existenzgefährdender Art, ist denkbar.
6	Finanzielle Auswirkungen	Der finanzielle Schaden bleibt für die Institution tolerabel.	Der Schaden bewirkt beachtliche finanzielle Verluste, ist jedoch nicht existenzbedrohend.	Der finanzielle Schaden ist für die Institution existenzbedrohend.
Schlussfolgerungen		Standard-Sicherheitsmaßnahmen nach IT-Grundschutz sind im Allgemeinen ausreichend und angemessen.	Standard-Sicherheitsmaßnahmen nach IT-Grundschutz bilden einen Basisschutz, sind aber unter Umständen alleine nicht ausreichend. Weitergehende Maßnahmen können durch eine Risikoanalyse ermittelt werden.	Standard-Sicherheitsmaßnahmen nach IT-Grundschutz bilden einen Basisschutz, sind aber alleine im Allgemeinen nicht ausreichend. Die erforderlichen zusätzlichen Sicherheitsmaßnahmen müssen individuell durch eine Risikoanalyse ermittelt werden.

Beispielhafte Schutzbedarfsfeststellung einer fiktiven Firma aus dem BSI-Standard 200-2

A.2 Schutzbedarfsfeststellung der RECPLAST GmbH

Bezeichnung	Beschreibung des Zielobjektes / der Gruppe der Zielobjekte	Plattform / Baustein	Verantwortlich / Administrator	Vertraulichkeit	Begründung für die Vertraulichkeit	Integrität	Begründung für die Integrität	Verfügbarkeit	Begründung für die Verfügbarkeit
A003	Textverarbeitung, Tabellenkalkulation	Office-Produkt 2010	IT-Betrieb	normal	Die Anwendung selbst enthält keine Informationen.	normal	Die Anwendung selbst enthält keine Informationen	normal	Die Anwendung wird lokal installiert. Die Lizenzen sind entsprechend aufgehoben, so dass eine Neuinstallation schnell ermöglicht werden kann. Eine Ausfallzeit von mehr als 24 Stunden ist tolerierbar.
A007	Lotus Notes	Lotus Notes	IT-Betrieb	hoch	Über das E-Mailsystem werden viele, teilweise vertrauliche Informationen versendet. Durch die Anwendung werden alle E-Mails verschlüsselt.	normal	Durch eine Signatur kann die Integrität einer E-Mail festgestellt werden.	sehr hoch	Das Mailsystem sollte auch dann zur Verfügung stehen, falls andere Kommunikationsmittel ausfallen (z.B. Faxserver)
C002	Laptop Verwaltung	Client unter Windows 10	IT-Betrieb	normal	Maximumprinzip Auf dem Arbeitsplatzrechner werden keine Informationen gespeichert	normal	Maximumprinzip Auf dem Arbeitsplatzrechner werden keine Informationen gespeichert	normal	Es ist ein Ausfall von höchstens 4 Stunden tolerierbar.
G003	Vertrieb Berlin	Gebäude	-	hoch	Maximumprinzip In dem Gebäude werden grundsätzlich alle Informationen verarbeitet	hoch	Maximumprinzip In dem Gebäude werden grundsätzlich alle Informationen verarbeitet	hoch	Maximumprinzip In dem Gebäude werden grundsätzlich alle Informationen verarbeitet
K001	Internet – Bonn BG	-	IT-Betrieb	hoch	Maximumprinzip	hoch	Maximumprinzip	hoch	Maximumprinzip
R003	Häuslicher Arbeitsplatz	Telearbeit	IT-Betrieb	hoch	Maximumprinzip	hoch	Maximumprinzip	hoch	Maximumprinzip
N001	Router Internetanbindung	Router und Switches	IT-Betrieb	hoch	Der Router stellt den Anschluss zwischen dem Internet und dem Produktionsnetz dar.	normal	Zutritt, Zugang und Zugriff nur für autorisierte Personen möglich	normal	Ersatzgerät liegt auf Lager und kann schnell durch den IT-Betrieb ausgetauscht werden