IT-Sicherheitsleitlinie

ITK Harburg

Version 2.0

Stand: 01.03.2018

Inhaltsverzeichnis

1 Zeichnungsebene

Die IT-Sicherheitsleitlinie und die zugehörigen Regelungen gelten für alle Mitarbeiterinnen und Mitarbeiter von

- Landkreis Harburg
- ITK Harburg
- Samtgemeinde Jesteburg
- Gemeinde Rosengarten
- Samtgemeinde Hanstedt
- Samtgemeinde Hollenstedt
- Samtgemeinde Salzhausen
- weitere zu benennende kreisangehörige Kommunen im Rahmen einer gemeinsamen IT-Kooperation

(nachfolgend "die Behörden" genannt).

Die Genehmigung der IT-Sicherheitsleitlinie erfolgt durch die Geschäftsleitungen der Behörden. Alle betroffenen Beschäftigten werden hierüber umgehend informiert.

Eine Überprüfung und bei Bedarf Aktualisierung der IT-Sicherheitsleitlinie ist regelmäßig vorzunehmen.

Zur Umsetzung der IT-Sicherheitsleitlinie werden entsprechende Ressourcen zur Verfügung gestellt, dabei ist auf wirtschaftliche Vorgehensweise zu achten.

Winsen, den 23.01.2018

Landkreis Harburg	gez. Rempe
ITK Harburg	gez. Lidzba
Samtgemeinde Jesteburg	gez. Höper
Gemeinde Rosengarten	gez. Seidler
Samtgemeinde Hanstedt	gez. Muus
Samtgemeinde Hollenstedt	gez. Albers
Samtgemeinde Salzhausen	gez. Krause

2 Einführung

Die Behörden besitzen 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. Beim Einsatz von Informationstechnologie müssen die Behörden 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 müssen sich die Behörden dem Thema Sicherheit in der Informationstechnik in geeigneter Form stellen und die verarbeiteten Informationen geeignet schützen.

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.

3 Etablierung eines IT-Sicherheitsprozesses

Die Durchsetzung und Aufrechterhaltung eines angemessenen und ausreichenden IT-Sicherheitsniveaus kann für einen komplexen IT-Verbund, wie er in den Behörden vorhanden ist, nur durch ein geplantes und organisiertes Vorgehen aller Beteiligten gewährleistet werden.

Aus diesem Grund initiieren die Behördenleitungen einen IT-Sicherheitsprozess, der die Voraussetzungen für die durchdachte Gestaltung sowie sinnvolle Umsetzung von IT-Sicherheitsmaßnahmen gewährleistet. Die Behördenleitungen werden diesen IT-Sicherheitsprozess steuern und kontrollieren und schaffen dafür die notwendigen Rahmenbedingungen.

Die Verantwortung für IT-Sicherheit liegt bei den Behördenleitungen. Die ITK Harburg ist mit der Umsetzung beauftragt und benennt hierzu einen IT-Sicherheitsbeauftragten.

Der oder die IT-Sicherheitsbeauftragte sorgt für die Etablierung eines Informationssicherheits-Managementsystems (ISMS). Jede Leistung, Aufgabe oder Information wird nach einem Schutzbedarf eingestuft. Der Schutzbedarf ist zunächst aus fachlicher Sicht zu erstellen. Anschließend wird der Schutzbedarf auf die Systeme der Informationstechnik und Infrastruktur übertragen.

In regelmäßigen Abständen wird überprüft, ob die ausgewählten Sicherheitsmaßnahmen noch ausreichend sind. Der oder die IT-Sicherheitsbeauftragte entwickelt die notwendigen Maßnahmen fort.

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.

Durch eine regelmäßige Auditierung wird das angestrebte Sicherheitsniveau sichergestellt. Abweichungen werden mit dem Ziel analysiert, den Sicherheitszustand weiter zu verbessern.

4 Regelungen zur IT-Sicherheit

Die IT-Sicherheitsleitlinie definiert das angestrebte IT-Sicherheitsniveau der Behörden. In ihr sind die dafür notwendigen internen Organisationsstrukturen, Regeln und Vorgaben zur Erreichung eines für den Geschäftsbetrieb notwendigen IT-Sicherheitsniveaus festgehalten.

Für die Einhaltung und Umsetzung der IT-Sicherheitsleitlinie ist jede Organisationseinheit selbst verantwortlich. Hilfestellung dazu leistet der oder die IT-Sicherheitsbeauftragte.

Alle Beschäftigten der Behörden müssen sich über die Notwendigkeit der Informationssicherheit bewusst sein und entsprechend handeln. Die IT-Sicherheitsleitlinie wird allen Mitarbeiterinnen und Mitarbeitern bekannt gegeben.

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.

Die Behörden orientieren sich für die Umsetzung von IT-Sicherheit an den aktuellen Standards und Best Practises.

Der Aufwand für die Bereitstellung von Personal und Finanzmitteln zur Gewährleistung der IT-Sicherheit soll für die eingesetzten und geplanten IT-Systeme ein angemessenes Sicherheitsniveau 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, wie folgt:

Schutzbedarf	Schadensauswirkung
Normal	Die Schadensauswirkungen sind begrenzt und überschaubar.
Hoch	Die Schadensauswirkungen können beträchtlich sein.
Sehr hoch	Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß erreichen.

4.1 IT-Sicherheitsorganisation

Zur Planung und Umsetzung wurde von den Behördenleitungen eine IT-Sicherheitsorganisation bestehend aus unterschiedlichen Rollen und Gremien eingerichtet, die nachfolgend beschrieben werden.

Bei Verstößen und Beeinträchtigungen haben die nachstehend genannten Verantwortlichen die zur Aufrechterhaltung des Betriebes und der IT-Sicherheit geeigneten und angemessenen Maßnahmen zu ergreifen.

4.1.1 Forum IT-Sicherheit

Das Forum IT-Sicherheit dient der langfristigen Unterstützung des IT-Sicherheitsbeauftragten. Es besteht aus den Behördenleitungen, dem Vorstand der ITK Harburg und dem oder der IT-Sicherheitsbeauftragten (Moderation).

Mindestens ein jährliches Treffen oder ein jährlicher Bericht dient der Priorisierung der IT-Sicherheitsthemen für die Arbeit im folgenden Jahr. Die Termine sollten auf die IT-Jahresplanung abgestimmt sein, um erforderliche Projekte auch rechtzeitig in die Ressourcen- und Kostenplanung der betroffenen Auftraggeber einstellen zu können.

Das Forum hat folgende Aufgaben:

- Beratung und Unterstützung des oder der IT-Sicherheitsbeauftragten durch Entscheidungen.

- Festlegung der Informationen, die auf Vorschlag des oder der IT-Sicherheitsbeauftragten zum Thema IT-Sicherheit die Beschäftigten bzw. die Geschäftspartner und Bürgerinnen und Bürger erreichen sollen.

Das Forum IT-Sicherheit bildet eine Eskalationsstufe bei sicherheitsrelevanten Vorfällen in den Behörden. Bei außerordentlichen Ereignissen, die eine sofortige Behandlung benötigen, finden außerordentliche Treffen des Forums IT-Sicherheit statt.

4.1.2 IT-Sicherheitsbeauftragter

Der oder die IT-Sicherheitsbeauftragte ist für die ganzheitliche Umsetzung des Prozesses IT-Sicherheit zuständig. Zweck der Funktion ist die Steuerung und Weiterentwicklung des IT-Sicherheitsmanagements. Er organisiert den Aufbau, die Durchführung und die Überwachung der IT-Sicherheitsorganisation. In der Ausübung der Aufgaben kann auf interne bzw. externe Unterstützung zurückgegriffen werden. Für die Aufgabenerfüllung werden ausreichende Ressourcen und Zeitbudgets zur Verfügung gestellt.

Die Aufgaben im Einzelnen:

- Die Definition und Fortschreibung der IT-Sicherheitsleitlinie und damit unmittelbar zusammenhängender Dokumente.

- Die Identifizierung von sicherheitsrelevanten Risiken und Strukturierung nach ihrem Risikopotential.

- Regelmäßige Berichterstattung im Rahmen des Forums IT-Sicherheit sowie bei besonderen Vorkommnissen wie z. B. Sicherheitsvorfälle sowie die Moderation des Forums.

- Vorschlag von Maßnahmen zur Vermeidung, Begrenzung und/oder Identifizierung von Risiken

- Bereitstellen von Informationen bzgl. gesetzlichen Regelungen und Rahmenbedingungen zur IT-Sicherheit. Hierzu ist er angehalten, sich angemessen weiterzubilden.

- Zuständigkeit für die Planung, Priorisierung und Realisierung von IT-Sicherheitsmaßnahmen.

- Zentrale Stelle der Behörden in Fragen der IT-Sicherheit.

- Zuständigkeit für die organisatorische und technische Umsetzung der Sicherheitsanforderungen.

- Sensibilisierung der Beschäftigten in Fragen zur IT-Sicherheit.

4.1.3 Vorstand ITK Harburg

Der Vorstand der ITK Harburg ist bezüglich der gesamten IT verantwortlich für die Gestaltung, Beschaffung, Disposition und den rationellen Einsatz der personellen, sachlichen und technischen Mittel.

Er ist zusätzlich verantwortlich für:

- die Sicherstellung des Produktionsbetriebs und die Bereitstellung der Anwendungen gemäß den festgelegten Service-Level-Vereinbarungen,

- die Umsetzung der im IT-Management bzw. von den Behördenleitungen beschlossenen IT-Maßnahmen,

- IT-Ressourcenplanung,

- direkte Kontrolle von Umsetzungsmaßnahmen,

- Einbeziehung des oder der IT-Sicherheitsbeauftragten bei relevanten Änderungen.

4.1.4 IT-Sicherheits-Board

Der oder die IT-Sicherheitsbeauftragte wird bei der operativen Arbeit durch das IT-Sicherheits-Board unterstützt. Es tagt mindestens sechs mal im Jahr. Dem IT-Sicherheits-Board gehören neben dem oder der IT-Sicherheitsbeauftragten (Moderation), der Leiter Systembetrieb und der Vorstand der ITK Harburg an. Bei Bedarf können weitere Personen hinzugezogen werden.

4.1.5 Verpflichtung User

Die Beschäftigten und die Geschäftspartner sind bei der Erstellung, Nutzung und Verwaltung von Informationen verpflichtet, die IT-Sicherheitsleitlinie und die damit verbundenen arbeitsordnenden Regelungen und Richtlinien der Behörden einzuhalten. Die User sind für sämtliche Maßnahmen verantwortlich, die sie bei der Nutzung von Informationen und der damit verbundenen Systeme ergreifen.

Sie müssen verstehen, wann und warum Informationen, die in den Behörden zur Durchführung ihrer Geschäfte verwendet werden, durch angemessene Kontrollen zu schützen sind. Um diese Kontrollen durchführen zu können, sind sie verpflichtet, bei Bedarf adäquate Unterstützung einzuholen. Es werden entsprechende Schulungen und Beratungen über IT-Sicherheit angeboten.

User, die eine Verletzung der IT-Sicherheitsleitlinie und der damit verbundenen Sicherheitsstandards vermuten oder Kenntnis davon erlangt haben bzw. annehmen, dass Infor-

mationen nicht in geeigneter Weise geschützt sind, müssen dies unverzüglich ihrem Vorgesetzten und/ oder dem oder der IT-Sicherheitsbeauftragten melden.

4.2 Durchsetzung der IT-Sicherheitsleitlinie

Die IT-Sicherheitsleitlinie wird allen Beschäftigen zur Verfügung gestellt. Als Verstöße gegen die IT-Sicherheitsleitlinie gelten vorsätzliche oder grob fahrlässige Handlungen, die

- gegen bestehende Gesetze, Verordnungen oder arbeitsordnende Regelungen bzw. Richtlinien verstoßen,
- den Behörden oder den Bürgerinnen und Bürgern einen tatsächlichen oder potentiellen Vermögensschaden zufügen,
- den Ruf der Behörden, von Beschäftigten oder Bürgerinnen und Bürgern schädigen,
- den unberechtigten Zugriff auf Daten oder Systeme und deren Missbrauch ermöglichen.

Verstöße gegen die IT-Sicherheitsleitlinie und die entsprechenden Detailregelungen können zu arbeitsrechtlichen Konsequenzen führen. Bei schweren Verstößen sind zivilrechtliche oder sogar strafrechtliche Folgen möglich. Hierbei sind der Personalrat und die Gleichstellungsbeauftragte mit einzubeziehen.