Hand-Out an Dienstleister

Stadtwerke Greifswald GmbH
IT Sicherheitsbeauftragter
Gützkower Landstraße 19-21
17489 Greifswald

Greifswald, Juni 2017

Information zum Betrieb eines Sicherheitssystems für Informationen und Informationstechnik

Sehr geehrte Damen und Herren,

die Stadtwerke Greifswald GmbH (SWG) erfüllt die Anforderungen, die an sie im Kontext ihres Versorgungsauftrages gestellt werden.

Neben den gesetzlichen Anforderungen sind die Anforderungen

- der versorgten Kunden,
- des Gesellschafters mit seinem Aufsichtsgremium, dem Aufsichtsrat
- der Auftraggeber für Dienstleistungserbringungen
- der Dienstleister
- der im Zusammenhang mit dem Versorgungsauftrag agierenden Behörden

zu beachten bzw. zu erfüllen.

Dabei sind insbesondere die Anforderungen an Unternehmen, die im Bereich der öffentlichen Daseinsvorsorge im Bereich der Kritischen Infrastrukturen agieren, hinsichtlich der Aufrechterhaltung und Kontinuität ihres Wirkens stark gestiegen. Um den ständig steigenden Bedrohungen aus dem Umfeld der modernen Informations- und Kommunikationstechnik zu begegnen, sind vom Gesetzgeber eine Vielzahl von Regeln zum Schutz Kritischer Infrastrukturen aufgestellt worden. Der sichere Betrieb der IT-Infrastruktur der Stadtwerke Greifswald gehört dazu.

Ki
28.6.2017

Ein entscheidendes Instrument für eine stabile Versorgung und das Betreiben unserer kommunalen Kritischen Infrastruktur ist die funktionierende Informationstechnik und Datenverarbeitung.

Daher verpflichten wir uns zu folgenden Aussagen:

1. Die gesetzlichen Anforderungen werden mit Hilfe des innerbetrieblichen Compliancemanagements beschrieben, aktuell gehalten und bei der Umsetzung des Versorgungsauftrages beachtet.

2. Die SWG betreibt ein Sicherheitsregime für Informationen und die Informationstechnik in Form eines Informationssicherheitsmanagement-systems nach den gesetzlichen Vorgaben

3. Der Schutz von Unternehmenswerten zur Sicherstellung des Versorgungsauftrages wird als besonderer Schwerpunkt in den Anforderungskatalog aufgenommen.

Aus dem Grundsatz des umfassenden Schutzes der Unternehmenswerte lassen sich die folgenden Ziele für den Umgang mit Informationen und mit Informationstechnik ableiten, deren Umsetzung den o.g. Beteiligten bei der Erfüllung des Versorgungsauftrages zur Kenntnis und zur Beachtung mitgeteilt werden:

- Einhaltung von Vertraulichkeit,
- Sicherstellung der Integrität,
- Erhalt der Verfügbarkeit entsprechend technischer und wirtschaftlicher Möglichkeiten,
- Schutz vor Verlust,
- Nachvollziehbarkeit der Bearbeitung,
- Einhaltung gesetzlicher Vorgaben und
- Einhaltung der Anforderungen interessierter Partner
- Kontinuität der Geschäftsführung.

Li 28.6.2017

Der Umsetzung dieser Ziele dient ein unternehmensweites Risikomanagement, welches im Bereich der IT durch das ISMS untersetzt und fortgeschrieben wird.

Die SWG selbst, der Gesellschafter, Dienstleistungserbringer, Behörden und Kunden werden über unsere Aktivitäten bezüglich der Informationssicherheit informiert und – wenn erforderlich und sinnvoll – in die Sicherheitsmaßnahmen mit einbezogen.

Unsere Informationssicherheitspolitik wird nach innen und außen so kommuniziert, dass alle an der Erfüllung des Versorgungsauftrages Beteiligten in die Implementierung und Ausführung der Informationssicherheit integriert werden.

Durch regelmäßige interne und externe Aktivitäten, wie Beachtung des Standes der Technik, Zusammenarbeit und Umsetzung der Vorgaben fachlich maßgeblicher Stellen (Bundesamt zur Sicherheit in der Informationstechnik-BSI), Betrieb des eigentlichen Managementsystems nach ISO 27001 und 27019, Information, Schulung, Audits, Reviews, Revisionen und die Einbeziehung aller Mitarbeiter, relevanter Dienstleister und Lieferanten halten wir die Maßnahmen zur Informationssicherheit aktuell und erreichen eine kontinuierliche Verbesserung.

Im Anhang möchten wir Ihnen die IT-Sicherheitsleitlinie der Stadtwerke Greifswald zur Kenntnis geben. Sie regelt das „Wie" der Herstellung der Informationssicherheit in der Stadtwerke Greifswald GmbH.

i. A.

Jens Kirsch

IT-Sicherheitsbeauftragter
Stadtwerke Greifswald GmbH

Anlage: IT-Sicherheitsleitlinie

IT-Sicherheits-Leitlinie

für die

Stadtwerke Greifswald GmbH

Erstellt:	Peter Kaufmann	24.05.2017	Das Dokument wurde automatisch erstellt.
Geprüft:	Jens Kirsch	26.05.2017	
Bestätigt:	Hans-Jürgen Schumann, Heike Witt, ...	06.06.2017	
Freigegeben:	Thomas Praße	06.06.2017	

Inhaltsverzeichnis

1 Ziele der IT-Sicherheitsleitlinie 3

1.1 Warum das Unternehmen IT-Sicherheit braucht 3

1.2. Wie die Mitarbeiter zur IT-Sicherheit beitragen können 3

2 Grundsätze der IT-Sicherheit im Unternehmen 4

2.1 Welcher Schutz erreicht werden soll 4

2.2 Wie dieser Schutz erreicht werden soll 4

2.3 Welche Aufgaben der Informationseigentümer hat 4

2.4 Wie Berechtigungen vergeben werden 5

2.5 Wie IT-Sicherheit bei neuen Verfahren berücksichtigt wird 5

3 Verantwortlichkeiten im Rahmen der IT-Sicherheit des Unternehmens 5

3.1 Wofür der Informationseigentümer verantwortlich ist 5

3.2 Wofür der Informationstreuhänder verantwortlich ist 5

3.3 Wofür der Nutzer verantwortlich ist 5

3.4 Wofür der IT-Sicherheitsbeauftragte verantwortlich ist 6

3.5 Wer für die unabhängige Prüfung verantwortlich ist 6

4 Durchsetzung 6

4.1 Was als Verstoß gilt 6

4.2 Wie ein Verstoß geahndet werden kann 7

5 Sicherheitsstandard 7

6 Begriffe 7

Erklärung 8

Die Geschäftsführung trägt die Gesamtverantwortung für die IT-Sicherheit der Stadtwerke Greifswald GmbH (SWG). Diese durch geeignete Regelungen auszugestalten gehört zu ihren Organisationspflichten.

Die folgende IT-Sicherheitsleitlinie beschreibt detailliert die notwendigen Maßnahmen, um die in der Informationssicherheitspolitik der Stadtwerke Greifswald getroffenen Aussagen und Verpflichtungen umsetzen zu können und stellt bei konsequenter Anwendung die Erreichung der in der Informationssicherheitspolitik gesetzten Sicherheitsziele sicher.

Mit Wirkung vom 01.01.2017 setzt die Geschäftsführung der SWG daher folgende IT-Sicherheitsleitlinie in Kraft.

Sie gibt den Rahmen für eine sichere Nutzung aller Komponenten der Informationstechnik des Unternehmens vor. Dazu gehören neben den Computern selbst, zum Beispiel auch Netzkomponenten, Telefontechnik, Fax und alle Einrichtungen, die für deren Betrieb benötigt werden.
Diese Sicherheitsleitlinie ist für jeden, der bei oder für die Stadtwerke Greifswald GmbH arbeitet (also z. B. Angestellte, Vertragspartner, Berater oder Zulieferer), bindend. Ihre Einhaltung wird überprüft.

Die Geschäftsführung verpflichtet jeden Mitarbeiter, diese Leitlinie und die daraus abgeleiteten Standards und Richtlinien zu beachten. Die Verpflichtung der Betroffenen wird durch Unterschrift dokumentiert (siehe Anhang).

1 Ziele der IT-Sicherheitsleitlinie

1.1 Warum das Unternehmen IT-Sicherheit braucht

Die SWG ist für eine Erfüllung ihrer Aufgaben in erheblichem Umfang auf den Einsatz von Informationstechnik (IT) angewiesen. Dabei hängt nicht nur die wirtschaftliche Erbringung von Dienstleistungen für die Kunden vom korrekten Funktionieren der IT ab. Aufgrund der Qualität der verarbeiteten Daten sind auch gesetzliche Vorgaben hinsichtlich

- des Datenschutzes (Schutz personenbezogener Daten) und
- der Risikoabwehr (Gefährdungshaftung) zu erfüllen.

Ein nicht angemessener Schutz würde unter anderem zur Schadensersatzpflicht des Unternehmens führen.

Des Weiteren zählen Energieversorger zu den zu schützenden bedrohten IT- Infrastrukturen im Sinne der rasant wachsenden Internettechnologien mit realem kriminellem, internationalem Bedrohungspotential.

Ziel dieser Leitlinie ist, den Rahmen für einen angemessenen Schutz festzulegen. Daher ist diese Leitlinie für alle Mitarbeiter verbindlich.
Nach Maßgabe dieser Leitlinie ist jede Organisationseinheit des Unternehmens für die Sicherheit ihrer Informationen und einen angemessenen Schutz der Informationen entsprechend ihres Wertes und Risikos für das betreffende Arbeits- oder technische Umfeld mitverantwortlich.

Diese Anforderungen beinhalten vor allem die Wahrung der Vertraulichkeit, Integrität und Verfügbarkeit der Informationen sowie die Rechenschaftspflicht des Einzelnen hinsichtlich der Nutzung von Informationen.

Die Koordination der Maßnahmen und der Aufbau einer umfassenden IT-Sicherheitskonzeption sind dem IT-Sicherheitsbeauftragten übertragen.

1.2. Wie die Mitarbeiter zur IT-Sicherheit beitragen können

Die Informationssicherheit ist, wie oben dargestellt, ein wichtiger Faktor für die Aufgabenerfüllung des Unternehmens. Daraus folgt, dass das Bewusstsein der Mitarbeiter für IT-Sicherheit ein entscheidender Bestandteil der Dienstleistungen des Unternehmens ist.
Sicherheitsbewusstsein ist durch folgendes Verhalten gekennzeichnet:

- Erkennen, dass IT-Sicherheit ein wesentliches Element der Arbeit für das Unternehmen ist („ Ich weiß, dass IT-Sicherheit wichtig für das Unternehmen ist!")
- Umsetzen dieser Erkenntnis durch entsprechendes Umgehen mit der IT („Ich handle so, dass bei der Arbeit mit IT kein Schaden entsteht!")

- Übernahme von persönlicher Verantwortung für die IT-Sicherheit im eigenen Umfeld. („Ich bin selbst dafür verantwortlich, dass die IT in meinem Arbeitsbereich sicher ist!")
- Umsichtiges Handeln auch über den eigenen Bereich hinaus. („Ich helfe meinen Kollegen, indem ich sie auf Sicherheitslücken hinweise!")

2 Grundsätze der IT-Sicherheit im Unternehmen

2.1 Welcher Schutz erreicht werden soll

Die Daten und Systeme des Unternehmens müssen so geschützt werden, dass

- keine vertraulichen Informationen Unbefugten bekannt werden,
- Informationen nicht bewusst verfälscht werden können,
- sie verfügbar sind, wenn sie gebraucht werden,
- nachvollziehbar bleibt, wer an einem elektronisch bearbeiteten Geschäftsvorgang beteiligt war,
- gesetzliche, vertragliche und aufsichtsrechtliche Verpflichtungen erfüllt werden.

Dabei muss ein angemessenes Verhältnis zwischen dem Wert der Daten und Systeme und dem Aufwand für ihren Schutz gewahrt bleiben.

2.2 Wie dieser Schutz erreicht werden soll

Um den genannten Schutz in einem wirtschaftlich angemessenen Rahmen zu erreichen gelten die folgenden Grundsätze:

- Für alle Informationen wird ein „Informationseigentümer" benannt, der festlegt, welcher Schutz für diese Informationen erforderlich ist.
  Mit „Informationen" sind dabei nicht nur die Dateien im IT-Netz gemeint, sondern zum Beispiel auch Mess- und Verbrauchsdaten oder Steuerinformationen in der Prozessrechnertechnik.
  Die Geschäftsführung legt Kategorien fest, nach denen der Schutzbedarf eingestuft werden kann.
- Anhand dieses Schutzbedarfes wird bewertet, welche Schutzmaßnahmen für die Informationen angemessen sind. Da sich diese Maßnahmen im Einzelnen ergänzen oder ausschließen können, wird für das Unternehmen ein Gesamtkonzept zur IT-Sicherheit erarbeitet. Dies ist Aufgabe des IT-Sicherheitsbeauftragten. Die endgültige Entscheidung über die Umsetzung des Konzeptes (und damit auch die Angemessenheit der Maßnahmen) trifft die Geschäftsführung.
- Jeder Mitarbeiter ist für die bestimmungsgerechte Nutzung der Informationen in seinem Zugriff verantwortlich. Der IT-Sicherheitsbeauftragte unterstützt die Mitarbeiter durch Schulungen und als Ansprechpartner bei Problemen und für Lösungen.
- Durch Einsatz von Protokollierung und ggf. durch zusätzliche Verfahren soll die Nachvollziehbarkeit sämtlicher IT-gestützten Geschäftsvorgänge gewährleistet werden. Die Mitbestimmungsrechte des Betriebsrates werden durch eine enge Beteiligung gewahrt.
- Zur unabhängigen Überprüfung, ob die genannten Ziele erreicht wurden, wird eine Revision der IT-Sicherheit durchgeführt.

2.3 Welche Aufgaben der Informationseigentümer hat

Für alle Gattungen von Informationen wird es einen benannten „Eigentümer" geben. Dies gilt auch für „technische" Anwendungen, die zum Beispiel zur Prozesssteuerung oder Anlagenüberwachung dienen. Die Rolle des Informationseigentümers nehmen die Leiter der Organisationseinheiten wahr.

Der Informationseigentümer hat dafür zu sorgen, dass

- alle für die Einschätzung des Schutzbedarfes erforderlichen Grundlagen, (z. B. gesetzliche oder vertragliche Verpflichtungen) berücksichtigt werden,

- der Schutzbedarf „seiner" Informationen richtig den unternehmensweit geltenden Kategorien zugeordnet wird,
- der IT-Sicherheitsbeauftragte diese Informationen rechtzeitig für die Erstellung oder Fortschreibung des IT-Sicherheitskonzeptes erhält,
- die mitgeteilte Einschätzung korrigiert wird, wenn dies (z. B. aufgrund einer veränderten Ausgangssituation) erforderlich wird.

2.4 Wie Berechtigungen vergeben werden

Der Zugriff auf Informationen darf Nutzern nur zur Erfüllung ihrer Aufgaben im Unternehmen gewährt werden. Die Verantwortung für die Freigabe von Zugriffsrechten liegt vom Grundsatz bei den Informationseigentümern. Für die praktische Durchführung können standardisierte Verfahren eingeführt werden.
Die Einhaltung der Berechtigungen wird durch Protokollierung überwacht. Für die Rahmenbedingungen hierzu werden mit dem Betriebsrat entsprechende Betriebsvereinbarungen getroffen.

2.5 Wie IT-Sicherheit bei neuen Verfahren berücksichtigt wird

Werden neue Verfahren, Anwendungen oder IT-Systeme geplant, ist der IT-Sicherheitsbeauftragte zu beteiligen. In Zusammenarbeit mit ihm ist das neue Verfahren in das IT-Sicherheitskonzept zu integrieren.

3 Verantwortlichkeiten im Rahmen der IT-Sicherheit des Unternehmens

3.1 Wofür der Informationseigentümer verantwortlich ist

Der Informationseigentümer ist verantwortlich dafür, dass er seine unter 2.3 geschilderten Aufgaben erfüllt.

3.2 Wofür der Informationstreuhänder verantwortlich ist

„Informationstreuhänder" ist, wer für einen Informationseigentümer Daten weiterverarbeitet. Dies ist zum Beispiel die IT-Abteilung, aber auch Mitarbeiter anderer Abteilungen, die Informationen aus anderen Bereichen weiter verarbeiten. Der Informationstreuhänder muss den Schutz gewährleisten, der dem vom Informationseigentümer festgelegten Schutzbedarf angemessen ist. Dabei ist das IT-Sicherheitskonzept der Maßstab.
Der Informationstreuhänder ist verpflichtet, den Informationseigentümer über Risiken zu informieren, die sich aufgrund der Weiterverarbeitung ergeben können. Er informiert den Informationseigentümer, wenn sich aufgrund der Weiterverarbeitung ein höherer Schutzbedarf für die Daten ergibt.

3.3 Wofür der Nutzer verantwortlich ist

Nutzer (Mitarbeiter, Vertragspartner, Berater) sind bei der Erstellung, Nutzung und Verwaltung von Informationen verpflichtet, die Sicherheitsleitlinie und die damit verbundenen Informationssicherheitsstandards sowie die Richtlinien des Unternehmens einzuhalten. Die einzelnen Nutzer sind für sämtliche Maßnahmen verantwortlich, die sie bei der Nutzung von Informationen und der dafür notwendigen Systeme ergreifen.
Die Nutzer müssen verstehen, wann und warum Informationen, die vom Unternehmen zur Erfüllung ihrer Aufgaben verwendet werden, durch angemessene Kontrollen geschützt werden sollten. Um diese Kontrollen durchführen zu können, sind sie verpflichtet, adäquate Unterstützung zu leisten. Das Unternehmen bietet den Nutzern entsprechende Schulungen und Beratung über Informationssicherheit an.

Nutzer, die eine bewusste Verletzung der Sicherheitsleitlinie und der damit verbundenen Informationssicherheitsstandards vermuten oder erkennen bzw. annehmen, dass Informationen aufgrund fehlender Richtlinien nicht in geeigneter Weise geschützt sind, müssen dies unverzüglich ihrem Vorgesetzten und/oder dem IT-Sicherheitsbeauftragten melden.

3.4 Wofür der IT-Sicherheitsbeauftragte verantwortlich ist

Die Geschäftsführung hat einen IT-Sicherheitsbeauftragten benannt. Seine Aufgaben und Befugnisse sind in einer Arbeitsanweisung festgehalten, die (vor allem in Bezug auf die eingeräumten Kompetenzen) für alle Mitarbeiter verbindlich ist.
Der IT-Sicherheitsbeauftragte ist für die Konzeption der erforderlichen Maßnahmen zum Schutz der Informationstechnik verantwortlich und beauftragt ihre Umsetzung.
Er stellt die Entwicklung der Sicherheitsleitlinie und der damit verbundenen Standards, ihre ständige Fortschreibung und Veröffentlichung sicher. Er ist sowohl für die Einführung von Sicherheitsprogrammen entsprechend den Sicherheitsbedürfnissen sowie für die Bereitstellung unternehmensweiter Sicherheitsdienstleistungen zum Schutz der IT des Unternehmens verantwortlich. Dazu gehören auch die Sensibilisierung der Mitarbeiter, die Sicherheitsanalyse und - wenn erforderlich - die technische Überwachung.
Der IT-Sicherheitsbeauftragte versichert sich ständig über die Einhaltung dieser Leitlinie durch geeignete Managementinstrumente (interne wie externe Audits), die vom Managementsystembeauftragten durchgeführt bzw. organisiert werden.
Er wird bei der Geschäftsführung Maßnahmen veranlassen, wenn der notwendige IT-Sicherheitsstandard gefährdet ist.
Für diese Aufgaben steht dem IT-Sicherheitsbeauftragten ein festgelegtes jährliches Budget zusätzlich zu projektbezogenen Ausgabenbewilligungen zur Verfügung.

3.5 Wer für die unabhängige Prüfung verantwortlich ist

Die Wirksamkeit und Effizienz von IT-Sicherheitsmaßnahmen muss regelmäßig von unabhängiger Seite überprüft werden. Bei dieser Prüfung muss die Verhältnismäßigkeit und die Wirksamkeit der Umsetzung überprüft werden. Die Prüfung kann intern durch eine Revision (Audit mit Korrekturvorschlägen) erfolgen, soll aber zusätzlich regelmäßig für spezielle Fälle durch Externe durchgeführt werden.
Die Ergebnisse führen zu einer Aktualisierung dieser Leitlinie und der darauf aufbauenden Strukturen und Regelungen.
Verantwortlich für das Veranlassen der Prüfung und die Umsetzung der daraus resultierenden Erkenntnisse ist die Geschäftsführung.

4 Durchsetzung

Zur Durchsetzung dieser Leitlinie wird das Unternehmen Verstöße gegen die Regelungen zur IT-Sicherheit angemessen ahnden.

4.1 Was als Verstoß gilt

Als Verstöße gelten beabsichtigte oder grob fahrlässige Handlungen[1], die

- das Ansehen des Unternehmens in der Öffentlichkeit beeinträchtigen
- die Sicherheit der Mitarbeiter, Vertragspartner, Kunden oder unbeteiligter Dritter oder des Vermögens des Unternehmens beeinträchtigen,
- dem Unternehmen tatsächlichen oder potentiellen finanziellen Schaden einbringen
- den unberechtigten Zugriff auf Informationen, deren Preisgabe und/oder Änderung beinhalten,

[1] Beabsichtigt oder grob fahrlässig ist insbesondere eine Handlung, die trotz dokumentierter Belehrung über die Unzulässigkeit durchgeführt wird.

- die Nutzung von unternehmensinterner Informationen für illegale Zwecke beinhalten.

4.2 Wie ein Verstoß geahndet werden kann

Die Ahndung eines Verstoßes muss angemessen sein. Je nach Schwere des Verstoßes können die Reaktionen des Unternehmens auch arbeitsrechtliche Maßnahmen, Schadensersatzklagen, die Entlassung oder eine Strafanzeige umfassen.

5 Sicherheitsstandard

Die SWG werden in einem IT-Sicherheitsprozess interne Regelungen und Verfahren überarbeiten neu strukturieren und ergänzen.

Ziel ist das Erreichen eines Sicherheitsniveaus, das bei entsprechender Dokumentation eine Zertifizierung nach ISO 27001 auf Basis von IT-Grundschutz zulässt.

Die aktuelle Version des Grundschutzhandbuchs des Bundesamts für Sicherheit in der Informationstechnik (BSI) gilt solange als gültiger Sicherheitsstandard, bis konkretisierte unternehmensinterne Standards vorliegen.

6 Begriffe

Informationen	Daten, die gespeichert oder anders verarbeitet werden. Umfasst z. B. auch Steuer- oder Abrechnungsinformationen
Sicherheit	Schutz von Informationen vor unberechtigten Änderungen, Zerstörungen oder Preisgabe - unabhängig davon, ob sie absichtlich oder unabsichtlich erfolgten.
Vertraulichkeit	Information darf nur den Berechtigten bekannt sein.
Integrität	Information darf nur von Berechtigten verändert werden.
Verfügbarkeit	Information steht dem Berechtigten zur Verfügung, wenn er sie braucht.
Authentizität	Information wurde so vom Berechtigten selbst erstellt (und von keinem anderen)

Greifswald, den 01.01.2017

Praße
Geschäftsführer SWG

Erklärung

Ich habe die IT-Sicherheitsleitlinie der Stadtwerke Greifswald GmbH ausgehändigt bekommen und zur Kenntnis genommen.
Mir ist bekannt und bewusst, dass die Inhalte der Leitlinie und der darauf aufbauenden Regelungen zur IT-Sicherheit für meine Arbeit bindend und einzuhalten sind und Verstöße dagegen geahndet werden.
Die Bedeutung meines eigenen Verhaltens, wie es in Abschnitt 1.2 der IT-Sicherheits-Leitlinie beschrieben wird, ist mir deutlich geworden.

Name der Mitarbeiterin /
des Mitarbeiters

Ort, Datum

Unterschrift