SEESTADT BREMERHAVEN

Grundsätze zur Gestaltung der Informationssicherheit beim Magistrat der Stadt Bremerhaven

Richtlinie zur Informationssicherheit für das Magistratsnetz

Versionsstand: 02.12.2016
Magistratsbeschluss vom 00.00.0000

ENTWURF

Zertifikat seit 2007
audit berufundfamilie

Magistrat der Stadt Bremerhaven
Magistratskanzlei - MK 5
Postfach 21 03 60
27524 Bremerhaven

Betrieb für Informationstechnologie
Wirtschaftsbetrieb der
Stadt Bremerhaven
Postfach 21 03 60
27524 Bremerhaven

BREMERHAVEN
MEER ERLEBEN!

ENTWURF

Impressum:
Magistrat der Stadt Bremerhaven
Magistratskanzlei - MK 5
Hinrich-Schmalfeldt-Straße
27576 Bremerhaven
Telefon: 0471-590 3332
E-Mail: uwe.boeye@magistrat.bremerhaven.de

Diese Richtlinie zur Informationssicherheit basiert auf einen Entwurf der Firma

datenschutz nord

Inhaltsverzeichnis

EWUF

N WU F

1. Regelungsgegenstand und Geltungsbereich

Die Verwaltungsabläufe in den Ämtern und Dienststellen des Magistrats sowie den Wirtschafts- und Eigenbetrieben der Stadt Bremerhaven werden mittlerweile weitgehend durch den Einsatz von Informations- und Kommunikationstechnik unterstützt und sind somit hiervon abhängig. Um den Risiken und Gefährdungen, die sich durch die zunehmende Abhängigkeit von Informations- und Kommunikationstechnik ergeben, möglichst frühzeitig begegnen zu können, werden vom Magistrat der Stadt Bremerhaven in dieser IT-Sicherheitsrichtlinie organisatorische und technische Vorgaben formuliert, die beim Betrieb der Informations- und Kommunikationstechnik von allen Beteiligten, d.h. den Fachverantwortlichen, der IT-Administration und von allen Beschäftigten und sonstigen Nutzenden zu beachten sind.

Die IT-Sicherheitsrichtlinie gilt für alle Ämter und Dienststellen des Magistrats sowie für die Wirtschafts- und Eigenbetriebe der Stadt Bremerhaven, soweit sie an das Verwaltungsnetz (Magistratsnetz) angeschlossen sind; sie gilt somit nicht für das pädagogische Netz der Schulen, das Polizeinetz der Ortspolizeibehörde, das Schulungsnetz der Volkshochschule (VHS) sowie das Netz der Integrierten Leitstelle der Feuerwehr Bremerhaven.

Die IT-Sicherheitsrichtlinie orientiert sich an allgemeinen Sicherheitsstandards wie dem IT-Grundschutzkonzept des Bundesamts für Sicherheit in der Informationstechnik (BSI) bzw. der Norm ISO 27001. Soweit sich für einzelne Themenbereiche die Notwendigkeit ergibt, kann diese IT-Sicherheitsrichtlinie um weitergehende Regelungen ergänzt werden.

Die Richtlinie basiert auf der gegenwärtigen technischen Infrastruktur. Sollten aufgrund technischer Änderungen einzelne Vorschriften dieser Richtlinie nicht mehr anwendbar sein, wird die Wirksamkeit der Richtlinie davon nicht berührt. Die unwirksame Vorschrift der Richtlinie ist so zu ergänzen bzw. auszulegen, dass der mit der unwirksamen Vorschrift beabsichtigte Zweck erreicht wird. Die formelle Anpassung soll stets zeitnah unter Mitwirkung der Mitbestimmungsgremien erfolgen.

2. Begriffsdefinitionen

Unter dem Begriff **IT-System** versteht man jegliche Art elektronischer, datenverarbeitender Systeme wie z.B. Personal-Computer, Client- und Serversysteme, Cloud-Computing, Datenbanksysteme, VoIP-Systeme, digitale Anrufbeantworter, Videokonferenzsysteme, mobile Kommunikationssysteme und sonstige Informationssysteme.

Zu den **Anwendungen** gehört neben den Fachanwendungen auf den Serversystemen auch die Software am Arbeitsplatz.

Zu den **Informationen** gehören alle Verkehrs-, Bestands- und Inhaltsdaten.

Zu den **Basisdiensten** gehören die Netzwerkinfrastruktur, die Firewallsysteme, der Virenschutz sowie die Groupware-Dienste, wie z.B. Exchange, Outlook.

Als **Client** wird Soft- oder Hardware bezeichnet, die bestimmte Dienste von einem Server in Anspruch nehmen kann. Häufig steht der Begriff Client für einen Arbeitsplatzrechner, der in einem Netz auf Daten und Programme von Servern zugreift.

Ein **Virtuelles Privates Netz** (VPN) ist ein Netz, das physisch innerhalb eines anderen Netzes (oft des Internet) betrieben wird, jedoch logisch von diesem Netz getrennt wird. In VPNs können unter Zuhilfenahme kryptographischer Verfahren die Integrität und Vertraulichkeit von Daten geschützt und die Kommunikationspartner- und partnerinnen sicher authentisiert werden, auch dann, wenn mehrere Netze oder Rechner über gemietete Leitungen oder öffentliche Netze miteinander verbunden sind.

Ein **sicherheitsrelevanter Vorfall** ist ein Ereignis, das eine Einschränkung oder den Verlust der Vertraulichkeit, Verfügbarkeit oder Integrität von Informationen und IT-Systemen nach sich ziehen kann.

NWR

3. Ziele und Grundsätze der Informationssicherheit

Die Informationssicherheit orientiert sich an folgenden grundlegenden Sicherheitszielen:

- **Vertraulichkeit:** nur befugte Personen erhalten Zugang zu den IT-Systemen, Anwendungen und Informationen.
- **Integrität:** d.h. die Unversehrtheit und Korrektheit von Informationen und die korrekte Funktionsweise von IT-Systemen wird gewährleistet.
- **Verfügbarkeit:** d.h. IT-Systeme, Anwendungen und Informationen sind verfügbar, wenn sie gebraucht werden.

Ziel ist es, die Informationen und IT-Systeme in ihrer Verfügbarkeit so zu sichern, dass evtl. Stillstandzeiten und Datenverluste toleriert werden können. Auch gilt es, die Integrität und Vertraulichkeit von sensiblen Personaldaten und Bürgerdaten im gesetzlich vorgeschriebenen Umfang zu garantieren. Schadensfälle mit finanziellen Auswirkungen und immaterielle Folgen in Form von Imageschäden für den Magistrat müssen verhindert werden.

Die vom Betrieb für Informationstechnologie (BIT), Wirtschaftsbetrieb der Stadt Bremerhaven, zur Verfügung gestellte Netz- und Serverinfrastruktur sowie sämtliche Basisdienste sind so auszulegen, dass eine hohe Vertraulichkeit und Integrität sowie eine hohe Verfügbarkeit der verarbeiteten Daten garantiert werden kann, die der Sensibilität der verarbeiteten Personal- und Bürgerdaten in vollem Umfang entspricht.

Belange der Informationssicherheit sind von Beginn an zu beachten bei

- der Planung und Konzeption von Fachverfahren,
- der Prüfung der Auswirkungen auf die Gestaltung von Organisation und Arbeitsabläufen,
- der Entwicklung und der Einführung von Fachverfahren,
- dem Betrieb und Administration von Fachverfahren,
- der Beschaffung und der Entsorgung von IT-Produkten,
- der Zusammenarbeit mit anderen Behörden einschließlich Nutzung von Diensten Dritter sowie
- der Aus- und Fortbildung von Beschäftigten.

Alle in diesen Leitlinien beschriebenen Maßnahmen dienen ausschließlich der IT-Sicherheit und des Datenschutzes. **Leistungs- und Verhaltenskontrollen von Beschäftigten sind daher auf allen Ebenen (IT-Systeme, Anwendungen, Basisdienste usw.) grundsätzlich ausgeschlossen.** Dies gilt nicht, wenn Tatsachen bekannt werden, die den Verdacht einer erheblichen Verletzung der Dienst- und Arbeitspflichten oder den Verstoß gegen gesetzliche Bestimmungen begründen. Die jeweils zuständigen Mitbestimmungsgremien sowie die örtlich zuständigen Datenschutzbeauftragten sind zu beteiligen.

4. Informationssicherheitsmanagement (ISM)

Informationssicherheit ist kein unveränderbarer Zustand, sondern ein Prozess, der ständigen Veränderungen unterworfen ist. Verwaltungsprozesse und Fachaufgaben können sich ebenso ändern wie gesetzliche Rahmenbedingungen.

In diesem Sinne wird sich nicht nur darauf beschränkt, ein einmalig erstelltes technisch-organisatorisches Sicherheitskonzept adäquat umzusetzen. Nach der Umsetzung ist auch regelmäßig darauf zu achten, ob die dokumentierten Sicherheitsmechanismen überhaupt in dem geplanten Umfang wirksam sind und ob diese unter dem Aspekt der Angemessenheit nicht ggf. noch effektiver gestaltet werden können. Auch gilt es, Überregulierungen zu vermeiden bzw. rückgängig zu machen. Änderungen müssen wiederum geplant und umgesetzt werden. **Insgesamt müssen die Sicherheitsmaßnahmen im Verhältnis zum Wert der**

NWU E

schützenswerten Informationen und IT-Systeme stehen und wirtschaftlich vertretbar sein.

Um das erforderliche Sicherheitsniveau zu erreichen, zu halten und fortzuentwickeln, wird im Zuständigkeitsbereich des Magistrats nachfolgend beschriebene IT-Sicherheitsorganisation mit folgenden Akteuren etabliert.

Magistratskanzlei: Die Magistratskanzlei erarbeitet diese IT-Sicherheitsrichtlinie, die vom Magistrat verabschiedet wird. Durch die IT-Sicherheitsrichtlinie werden Vorgaben zur Umsetzung einer adäquaten IT-Sicherheit definiert und die Magistratskanzlei kontrolliert die Einhaltung der IT-Sicherheitsrichtlinie, z.B. durch Penetrationstests. Im Auftrag der Magistratskanzlei ist der/die IT-Sicherheitsbeauftragte des Magistrats tätig. Die Magistratskanzlei ist auch dafür verantwortlich, dass mit externen Dienstleistern, die im Auftrag des Magistrats tätig werden, Verträge zur Auftragsdatenverarbeitung geschlossen werden, die die externen IT-Dienstleister auf die Einhaltung der Standards dieser Richtlinie verpflichten.

Amts- bzw. Betriebsleitung: Die Verantwortung für die ordnungsgemäße und sichere Aufgabenerledigung und damit für die Informationssicherheit der in ihrer Zuständigkeit betriebenen Fachverfahren haben die Leitungen der Ämter bzw. Dienststellen sowie der Wirtschafts- und Eigenbetriebe der Stadt Bremerhaven. Die Leitungen können die Verantwortung an die für die einzelnen Fachverfahren jeweils zuständigen Fachverantwortlichen delegieren. Hierzu gehört die Nutzungsverwaltung einschließlich der Zugriffsrechte auf der Ebene der Fachverfahren. Die Amts- bzw. Betriebsleitungen erteilen in Abstimmung mit dem BIT die Freigabe für jeweilige Fachverfahren und sind auch dafür verantwortlich, dass diese IT-Sicherheitsrichtlinie den Beschäftigten in den Ämtern bzw. Dienststellen sowie in den Wirtschafts- und Eigenbetrieben bekannt gemacht wird. Die Aufgaben und Pflichten des BIT sind in einem Vertrag zur Auftragsdatenverarbeitung detailliert definiert.

Wirtschaftsbetrieb BIT: Der BIT stellt im Auftrag des Magistrats den Ämtern bzw. Dienststellen sowie den Wirtschafts- und Eigenbetrieben der Stadt Bremerhaven eine sichere IT-Infrastruktur zur Verfügung und ist hierfür allein verantwortlich. Eine sichere IT-Infrastruktur umfasst ein sicheres Magistratsnetz, eine sichere IT-Administration der Server und Clients sowie sichere Basisdienste. Sofern noch einige Ämter bzw. Dienststellen sowie Wirtschafts- und Eigenbetriebe die Administration der Server und Clients sowie der Basisdienste in eigener Verantwortung durchführen, sind die Anweisungen der IT-Administration des BIT zu beachten. Eine Übernahme dieser Tätigkeiten durch den BIT ist mittelfristig geplant und notwendig. BIT ergreift alle notwenigen Maßnahmen zur Aufrechterhaltung der technischen Infrastruktur. Die Aufgaben und Pflichten des BIT sind in einem Vertrag zur Auftragsdatenverarbeitung detailliert definiert.

Beschäftigte und sonstige Nutzende: Alle Beschäftigten und sonstige Nutzende sind verpflichtet, verantwortungsvoll mit den von ihnen genutzten IT-Systemen und Informationen umzugehen und die Vorgaben dieser IT-Sicherheitsrichtlinie zu beachten.

Ein Verhalten, das die Sicherheit von Informationen, IT-Systemen oder der Netze gefährdet oder einen Schaden für den Magistrat oder einem Dritten verursacht, kann disziplinar- oder arbeitsrechtlich geahndet, unter Umständen sogar als Ordnungswidrigkeit oder Straftat verfolgt werden. Darüber hinaus können Beschäftigte und sonstige Nutzende zum Schadensersatz herangezogen werden.

5. Aufgaben für IT - Sicherheitsbeauftragte des Magistrats

Durch Magistratsbeschluss wird unter Einbindung der Mitbestimmungsgremien ein IT-Sicherheitsbeauftragter / eine IT-Sicherheitsbeauftragte bestellt, der / die die IT-Sicherheit in den Ämtern und Dienststellen sowie den Wirtschafts- und Eigenbetrieben des Magistrats der Stadt Bremerhaven und insbesondere beim BIT organisieren und überwachen soll. Im Einzelnen handelt es sich hierbei um:

- Planung, Koordination, Steuerung und Dokumentation des Informationssicherheitsprozesses,

Entwurf

- Fortschreibung der Informationssicherheitsrichtlinie,
- Erstellung und Fortschreibung von Sicherheitskonzepten, Notfallvorsorgekonzepten sowie weiterer Richtlinien und Regelungen zur Informationssicherheit,
- Mitwirkung an der IT-Strategie und IT-Architektur des Magistrats,
- Erstellung von Berichten an den Magistrat,
- Untersuchung sicherheitsrelevanter Vorfälle von erheblicher Bedeutung
- Initiierung und Steuerung von Angeboten für Sensibilisierungs- und Schulungsmaßnahmen zur Informationssicherheit,
- Unterstützung der behördlichen Datenschutzbeauftragten bei der Freigabe automatisierter Verfahren zur Verarbeitung personenbezogener Daten,
- Planung, Durchführung, Auswertung sowie Nachbereitung und ggf. Beauftragung von IT-Sicherheitsaudits (Risiko- und Schwachstellenanalyse).
- Mitwirkung beim CERT (Computer Emergency Response Team) der Freien Hansestadt Bremen

6. Vorgaben beim Einsatz von Fachverfahren

Fachverantwortlichen in den Ämtern bzw. Dienststellen sowie den Wirtschafts- und Eigenbetrieben obliegt die Administration der Fachverfahren, die Nutzungsverwaltung der Fachverfahren sowie die Beantragung von Netz- und Server- und Basisdiensten beim BIT; sie sind die Schnittstelle zwischen Anwendenden und dem BIT. Teilaufgaben können dem BIT übertragen werden; hierzu bedarf es einer Leistungsbeschreibung (SLA), in der die übertragenen Leistungen detailliert beschrieben werden; die zuständigen Mitbestimmungsgremien sind durch die Fachämter zu beteiligen. Sofern keine Fachverantwortlichen benannt wurden, obliegen die hier beschriebenen Aufgaben der Amts- bzw. Betriebsleitung.

6.1 Administration der Fachverfahren

Die Administration der Fachverfahren umfasst hauptsächlich das Einspielen von neuen Softwareversionen, sofern diese vom Hersteller des Fachverfahrens zur Verfügung gestellt werden, die Schulung und Unterstützung der Anwender sowie die Kommunikation mit dem BIT.

Sofern externe IT-Dienstleister mit der Administration von Fachverfahren beauftragt werden, sind auch die Vorgaben der Ziffern 7.6 und 7.9 zu beachten. Die Verantwortung hierfür tragen die Fachverantwortlichen in den Ämtern bzw. Dienststellen sowie in den Wirtschafts- und Eigenbetrieben.

Sofern Fachverfahren der Freien Hansestadt Bremen oder anderer Bundesländer oder des Bundes eingesetzt werden, haben die Fachverantwortlichen sicherzustellen, dass die Vorgaben des Bundes bzw. der Länder zum Betrieb der Fachverfahren umgesetzt werden. Ggf. sind die einzuleitenden Maßnahmen auf Client- oder Netzwerkebene mit der Magistratskanzlei und / oder dem BIT abzustimmen.

6.2 Nutzungsverwaltung der Fachverfahren

Die Nutzungsverwaltung beinhaltet im Wesentlichen die Verwaltung der Zugangskennungen, der Zugriffsrechte und Rollen sowie das Zuweisen von Initialpasswörtern. Neue Zugangskennungen dürfen nur dann angelegt und geändert werden, wenn dies unter Nennung der Zugriffsrechte beauftragt wurde. Ausgeschiedene Beschäftigte sind von den Fachabteilungen unverzüglich den Fachverantwortlichen zu benennen. Das entsprechende Konto wird dann deaktiviert.

Zugriffsberechtigungen sind nur in dem Maße einzurichten, wie es zur Aufgabenerfüllung erforderlich ist. Es werden nach Möglichkeit Rollen definiert, denen Zugriffsberechtigungen

E-L-R

zugeordnet werden; diese sind im Datenschutz- und Datensicherheitskonzept zu beschreiben.

Darüber hinaus vergibt der/die Fachverantwortliche neue Initialpasswörter für Beschäftigte, die das Passwort vergessen haben und vergewissert sich vorab von der Identität des Beschäftigten. Initialpasswörter sollten in der Regel an eine im Fachverfahren hinterlegte Mailadresse versendet werden; das Offenbaren von neuen Initialpasswörtern per Telefon ist nur zulässig, sofern die Identität des Anrufenden zweifelsfrei bekannt ist.

6.3 Beantragung von Netz-, Server- und Basisdiensten

Die Fachverantwortlichen beantragen für neue Beschäftigte in den Ämtern und Dienststellen sowie Wirtschafts- und Eigenbetrieben beim BIT die Bereitstellung von Basisdiensten. Darüber hinaus beantragen sie für neue Fachverfahren oder bei entsprechenden Änderungen beim BIT die Bereitstellung sicherer Netz- und Serverdienste. Die Beantragung erfolgt per E - Mail.

Sofern für einzelne Organisationseinheiten zentrale Postfächer eingerichtet werden, haben die Leitungen der Ämter und Dienststellen sowie der Wirtschafts- und Eigenbetriebe die Behandlung der E - Mail-Eingänge zu regeln.

7. Vorgaben für die IT-Administration des BIT

Die IT-Administration des BIT besitzen im Hinblick auf die IT-Sicherheit eine besondere Verantwortung: Die Administration der Server und Clients wird mit Ausnahme einiger Ämter und Dienststellen von ihnen durchgeführt. Sie können und müssen Sicherheitseinstellungen an den Komponenten vornehmen, Systeme neu aufsetzen und Software installieren. Gleiches gilt für die Einrichtung, Änderung und Überwachung von Kommunikationsverbindungen. Im Folgenden werden daher Grundsätze beschrieben, nach denen die IT-Administration erfolgen soll.

7.1 Server – Administration

Die Administration des Magistratsnetzes sowie die Administration von Betriebssystemen und Datenbanken erfordern einen privilegierten Zugriff auf die jeweiligen Systeme. Privilegierte Zugriffsmöglichkeiten sollten daher nur den Administratoren / Administratorinnen bekannt und unter größter Sorgfalt verwendet werden. Die Administration der Server wird mit Hilfe von Individualkennungen durchgeführt.

Die Serveradministration ist möglichst so zu erledigen, dass hierbei durch die Administratoren / Administratorinnen nicht auf Personal- oder Bürgerdaten zugegriffen wird; dies gilt insbesondere für die Administration der Mail-Server. Im Rahmen der Serveradministration bekannt gewordene Daten dürfen anderen Personen nicht offenbart werden.

Die Anbindung des Magistratsnetzes an das Internet wird durch geeignete Netzwerkkomponenten gesichert. Diese werden so konfiguriert, dass die IT-Systeme der Ämter und Dienststellen sowie der Wirtschafts- und Eigenbetriebe in geeigneter Weise gegenüber externen Attacken abgesichert und nur gesicherte Dienste internetweit verfügbar sind. Die Konfiguration wird vom BIT dokumentiert und regelmäßig überprüft.

Basisdienste werden allen Beschäftigten in den Ämtern und Dienststellen sowie Wirtschafts- und Eigenbetrieben auf Antrag durch die Leitungen der Ämter und Dienststellen sowie der Wirtschafts- und Eigenbetriebe bereitgestellt. Zum Versenden und zum Empfang sensibler Daten werden geeignete Verschlüsselungsverfahren zur Verfügung gestellt.

Die Verwaltung der Zugangskennungen im Active Directory obliegt ebenfalls dem BIT. Neu anzulegende oder zu löschende Nutzungskonten werden dem BIT von den Leitungen der Ämter und Dienststellen sowie der Wirtschafts- und Eigenbetriebe bzw. den Fachverantwortlichen mitgeteilt. Initialpasswörter werden per Telefon nur mitgeteilt, sofern die Identität des

NWL F

Anrufenden / der Anrufenden zweifelsfrei bekannt ist. Ansonsten werden die Initialpasswörter an die E - Mail-Adresse des / der jeweiligen Vorgesetzten verschickt.

7.2 Client – Administration (Endgeräte)

Die Administration der dienstlichen Endgeräte (Clients) erfolgt mit wenigen Ausnahmen ausschließlich durch die IT-Administration des BIT; Ziel ist die ausschließliche Zuständigkeit des BIT. Welche Endgeräte zum Einsatz kommen wird im Einvernehmen mit den Mitbestimmungsgremien unter Einbeziehung der Arbeitssicherheit sowie des Betriebsärztlichen Dienstes festgelegt.

Für den Zugriff auf interne Serverdienste sind als Clients nur dienstliche Endgeräte zugelassen. Für den ausschließlichen Zugriff auf Groupware-Dienste können unter den Voraussetzungen gemäß Ziffer 8.5 auch private Endgeräte zugelassen werden.

Sofern auf dienstlichen mobilen Endgeräten (z.B. Laptops, Smartphones, Tabletts) Personal- oder Bürgerdaten gespeichert werden, sind diese Daten verschlüsselt zu speichern. In einem solchen Fall erfolgt auf den dienstlichen mobilen Endgeräten entweder eine Festplattenverschlüsselung oder es werden hierfür verschlüsselte Speicherbereiche zur Verfügung gestellt.

Die Administration von mobilen dienstlichen Endgeräten (z.B. Laptops, Smartphones, Tabletts) sowie von privaten mobilen Endgeräten, sofern sie im Sinne der Ziffer 8.5 verwendet werden sollen, wird mittelfristig über ein Mobile Device Management System erfolgen. Diese Software ermöglicht, dass neue Geräte zentral angemeldet, konfiguriert und im Bedarfsfall auch gelöscht oder gesperrt und Einstellungen überwacht werden können. Nur über diesen Weg kann die Einhaltung der definierten Sicherheitsrichtlinien gewährleistet und ein sicherer Zugang zum Magistratsnetz garantiert werden.

7.3 Change – Management

Die IT-Administration installiert und deinstalliert Basisdienste und Systemsoftware auf Client-Geräten und Servern und ist ebenso verantwortlich für den Aus- und Einbau von Hardware jeglicher Art. Grundsätzlich werden sämtliche nicht benötigte Dienste deaktiviert. Vom Hersteller aus Sicherheitsgründen empfohlene Software-Updates / Upgrades werden zeitnah installiert, sofern hiermit keine Risiken anderer Art verbunden sind. Sofern durch ein Update / Upgrade der bisherige Funktionsumfang der Software ausgeweitet wird, sind die Mitbestimmungsgremien zu beteiligen.

Es werden nur Basisdienste und Systemsoftware installiert, die von der Magistratskanzlei im Einvernehmen mit dem BIT, und soweit erforderlich unter Einbeziehung der Mitbestimmungsgremien, zentral freigegeben worden sind. Die Installation erfolgt im Rahmen der Lizenzbedingungen der einzelnen Softwareprodukte.

Änderungen an IT-Systemen erfolgen im Rahmen des Change-Managements und werden außerhalb des Systems mit Datum und Uhrzeit der Änderung, dem Grund der Änderung, der durchgeführten Tätigkeit sowie dem Namen des jeweiligen Administrators / der jeweiligen Administratorin dokumentiert.

Sicherheitskritische Änderungen durch die IT-Administration sind möglichst vorab in einer Testumgebung zu überprüfen. Erst nach abschließender Bewertung der Testergebnisse sind Änderungen an den Produktivsystemen vorzunehmen. Testsysteme sind wie Produktivsysteme zu behandeln, d. h. nur die zuständigen Administratoren / Administratorinnen haben Zugriff auf die Testsysteme und damit auf die dort gespeicherten Daten.

Regelmäßige operative Tätigkeiten, die nicht sicherheitskritisch sind, bedürfen keiner zentralen Freigabe.

ENTWURF

7.4 Virenschutz

Viren-Schutzprogramme werden auf allen IT-Systemen installiert und eingesetzt. Alle Schutzprogramme werden so konfiguriert und administriert, dass sie einen effektiven Schutz darstellen und Manipulationen verhindert werden.

Auf dem zentralen Mail-Server werden zusätzliche SPAM-Filter installiert, die den Empfang von Werbe - Mails automatisch prüfen.

7.5 Administration durch Fernwartung (Remote – Zugriff)

Der Remote-Zugriff auf dienstliche Endgeräte (Clients) ist ausschließlich der IT-Administration vom BIT und der Fachadministration vorbehalten. Der Zugriff ist durch eine Software zu realisieren, der eine Mitwirkung der davon betroffenen Beschäftigten erfordert. Ein Zugriff auf Clientsysteme ohne Kenntnis der Betroffenen ist nur zulässig, soweit es Maßnahmen der IT-Sicherheit zwingend erfordern; die betroffenen Beschäftigten sind unverzüglich darüber zu informieren.

Bei einem Remote-Zugriff durch externes Dienstleistungsunternehmen gilt zusätzlich:

- Die Verbindung zu den Systemen erfolgt ausschließlich über eine VPN-Verbindung.
- Die Remote-Verbindung wird nur durch die Fachadministration oder die IT-Administration des BIT aufgebaut; Externe können sich nicht selbstständig auf Systeme per Remote-Zugriff aufschalten.
- Nach Beendigung der externen Administratorentätigkeit wird die Remote-Verbindung wieder deaktiviert.
- Die Aktivitäten während des externen Zugriffs werden protokolliert.

Über ein Monitoring können die Tätigkeiten während des externen Zugriffs bei Bedarf jederzeit mitverfolgt werden.

7.6 Protokollierung

Eine Protokollierung von Systemaktivitäten erfolgt auf Systemen, auf denen Internet- und Mailing-Dienste installiert sind sowie auf der zentralen Firewall zum Schutz des Magistratsnetzes. Eine Auswertung der Protokolle erfolgt ausschließlich zur Analyse und Korrektur technischer Fehler, zur Gewährleistung der Systemsicherheit und zur Optimierung des Netzes sowie zur Kontrolle einer rechtmäßigen Internet- und E - Mail-Nutzung. Sofern dabei ein konkreter Personenbezug hergestellt werden kann, sind die Mitbestimmungsgremien zu beteiligen.

Auf dem Proxy-Server, über den der ausgehende Internetverkehr realisiert wird, werden die Adressen (URL) der aufgerufenen Seiten, sowie Datum und Uhrzeit protokolliert.

Die IP-Adresse des aufrufenden Clients wird nicht protokolliert; Ausnahmen sind im Einzelfall im Rahmen der Ziffer 3 möglich. Auf dem Mail-Server werden die IP-Adresse des Empfängers und des Absenders, Datum und Uhrzeit des Empfangs gespeichert.

Die Protokolldateien werden nach 1 Monat gelöscht.

7.7 Datensicherung

Um die Verfügbarkeit der Unternehmensdaten und -systeme sicherzustellen, werden folgende Vorgaben umgesetzt:

- Alle auf zentralen Systemen gespeicherten Daten sowie die Daten von Fachverfahren werden regelmäßig gesichert.
- Die definierten Sicherungszeiträume und Wiederherstellungsfristen sind einzuhalten.

E-Mail

7.8 Notfallplanung

Der BIT verfügt über ein Notfallkonzept zur Vermeidung und Behebung von Notfällen. Im Rahmen dieses Konzeptes werden mögliche Notfälle identifiziert und die einzuleitenden Maßnahmen zur Vermeidung und Behebung dieser Notfälle geplant. Dabei werden folgende Grundsätze beachtet:

- Alle wichtigen Systeme sind redundant ausgelegt.
- Es werden ausreichend Ersatzsysteme und -hardware bereitgehalten, um bei Ausfall einzelner Komponenten schnellstmöglich den Betrieb wieder aufnehmen zu können.
- Soweit möglich, werden Serviceverträge geschlossen, um bei Ausfall von Systemen und System-Komponenten schnellstmöglich den Betrieb wieder aufnehmen zu können.

7.9 Externe Dienstleistung

Beim BIT erfolgen Administration, Betrieb und Wartung der IT-Infrastruktur grundsätzlich durch eigene Beschäftigte. Nur in Einzelfällen wird ein externes Dienstleistungsunternehmen beauftragt. Dieses wird nicht eigenverantwortlich, sondern nur nach Aufforderung aktiv. Es sind vorab Ansprechpersonen zu benennen, die auf die Systeme beim BIT zugreifen dürfen. Die ausgeführten Tätigkeiten sind zu dokumentieren und werden im Anschluss durch eine sachkundige Person des BIT abgenommen. Die Zugriffsberechtigungen werden auf die Systeme begrenzt, die für die aktuelle Tätigkeit benötigt werden.

Wird ein externes Dienstleistungsunternehmen in Anspruch genommen, ist ein Vertrag zur Auftragsdatenverarbeitung abzuschließen; Auftraggeber ist der BIT. Bei der Vertragsgestaltung ist darauf zu achten, dass neben einer genauen Beschreibung der Tätigkeiten auch die benötigten Fristen für Reaktions- und, sofern angebracht, Wiederherstellungszeiten definiert sind.

Wenn im Rahmen der Auftragsdatenverarbeitung personenbezogene Daten zur Kenntnis gelangen können, ist im Vertrag eine Regelung aufzunehmen, durch die das externe Dienstleistungsunternehmen verpflichtet wird, seine Beschäftigten vor Aufnahme ihrer Tätigkeit auf Verschwiegenheit und auf die Einhaltung des Datengeheimnisses zu verpflichten.

8. Rechte / Pflichten / Hinweise für die Beschäftigten

Die Beschäftigten in den Ämtern bzw. Dienststellen sowie den Wirtschafts- und Eigenbetrieben haben eine hohe Verantwortung für die IT-Sicherheit und insbesondere eine hohe Verantwortung für die Vertraulichkeit der Daten. Sie sind es, die in der täglichen Verwaltungspraxis die organisatorischen und technischen Vorgaben umsetzen müssen.

8.1 Umgang mit Passwörtern

Um die Gefahr zu reduzieren, dass Passwörter erraten werden, werden an Passwörter folgende Anforderungen gestellt:

- Die Mindestlänge beträgt 8 Zeichen, darunter mindestens eine Zahl und ein Sonderzeichen; es dürfen keine Trivialpasswörter verwendet werden.
- die Höchstgültigkeitsdauer beträgt 90 Tage; anschließend müssen neue Passwörter verwendet werden, die sich von den drei vorherigen unterscheiden.

Die Eingabe von mindestens achtstelligen Passwörtern sowie das regelmäßige Ändern der Passwörter werden automatisch vorgegeben.

Die von den Beschäftigten benutzten Passwörter müssen geheim gehalten werden und dürfen nicht an andere Personen weitergegeben werden. Besonders dürfen Passwörter nicht

öffentlich zugänglich notiert werden. Sofern der Verdacht besteht, dass Passwörter auch anderen Personen bekannt geworden sind, müssen diese geändert werden.

Der Arbeitsplatz-Client ist beim Verlassen des Raumes zu sperren; dies gilt insbesondere dann, wenn Unbefugte (z. B. Bürgerinnen und Bürger, Beschäftigte anderer Ämter) Zugang zum System haben könnten. Eine Deaktivierung erfolgt nur nach erfolgreicher Authentisierung per Passwort.

8.2 Internet – Nutzung

Beschäftigten, die IT-Systeme nutzen, steht ein Internetzugang am Arbeitsplatz zur Verfügung. Die Nutzung des Internet ist vorbehaltlich der nachfolgenden Regelungen grundsätzlich nur für dienstliche Zwecke gestattet.

Voraussetzung für eine private Nutzung des dienstlichen Internetzuganges ist eine individuelle Einwilligung (siehe Anlage 1). Mit dieser Einwilligung wird zur Kenntnis genommen,

- dass die Internetnutzung in der in dieser Richtlinie beschriebenen Weise zur Datenschutzkontrolle und zur Gewährleistung der technischen Sicherheit der Systeme protokolliert wird,
- dass die private Nutzung auf das Abrufen von Inhalten sowie auf das Nutzen von externen Webmail-Diensten beschränkt ist,
- dass kein Anspruch auf die private Nutzung besteht und der Magistrat die Nutzung von externen Webmail-Diensten zeitweise oder dauerhaft jederzeit untersagen und / oder den Abruf von Inhalten zentral sperren kann.
- dass die Verfolgung kommerzieller Zwecke im Rahmen der Privatnutzung untersagt ist.

Aufruf, Nutzung und Speicherung rechtswidriger Angebote und Inhalte ist ausdrücklich untersagt und wird strafrechtlich verfolgt. Dies gilt auch für die Nutzung und Speicherung von Angeboten und Inhalten, die gegen datenschutzrechtliche, persönlichkeitsrechtliche, urheberrechtliche oder strafrechtliche Bestimmungen verstoßen sowie z.B. für beleidigende, verleumderische, verfassungsfeindliche, rassistische, sexistische oder pornografische Äußerungen und Abbildungen oder von kostenpflichtigen Seiten. Der Magistrat behält sich vor, rechtswidrige Inhalte und Inhalte, die auf eine private Nutzung schließen lassen, zentral zu sperren.

Inhalte dürfen nur dann auf einem Server oder dem eigenen Arbeitsplatz-PC gespeichert werden, wenn dies für berufliche Belange erforderlich ist und nicht gegen rechtliche Vorgaben verstößt. Nicht mehr benötigte Inhalte sind zu löschen. Das Downloaden von ausführbaren Programmen ist für Anwender und Anwenderinnen unzulässig.

Die lokal zur Verfügung gestellten Browser werden vom BIT vorkonfiguriert. Die sicherheitsrelevanten Browser-Einstellungen dürfen nicht verändert werden.

8.3 E - Mail – Nutzung

Beschäftigten, die IT-Systeme nutzen, werden am Arbeitsplatz über einen zentralen Mail-Server E-Mail-Dienste zur Verfügung gestellt. Diese E - Mail-Dienste dürfen nur für dienstliche Zwecke genutzt werden. Weitere Details werden in einer besonderen E-Mail-Richtlinie festgelegt.

Zulässig ist die Nutzung von Webmailern für private Zwecke, sofern hierdurch keine dienstlichen Belange beeinträchtigt werden (siehe Ziffer 8.2).

Der lokal zur Verfügung gestellte E - Mail-Client wird vom BIT vorkonfiguriert. Die sicherheitsrelevanten Client-Einstellungen dürfen nicht verändert werden.

NWO F

8.4 Software – und Hardware – Nutzung

Die zentral zur Verfügung gestellte Hardware und Software ist ausschließlich sachgemäß, mit angemessener Sorgfalt zu verwenden. Eine private Nutzung ist grundsätzlich nicht zulässig, eine Ausnahme bildet die Internet- und E - Mailnutzung (siehe Ziffer 8.2 und 8.3).

Die Nutzung der Software muss im Rahmen der Lizenzbedingungen der einzelnen Softwareprodukte erfolgen; hierfür ist in aller Regel der Fachverantwortliche oder der BIT zuständig. Es ist untersagt, dienstliche Software auf Rechnern zu installieren, die nicht im Besitz des Magistrats sind, oder an Dritte weiterzugeben.

Die Installation lokaler Software durch die Beschäftigten ist grundsätzlich unzulässig; hierzu sind nur die IT-Administration befugt.

Auf allen Systemen werden Anti-Viren-Programme eingesetzt. Diese dürfen weder deaktiviert noch darf ihre Konfiguration geändert werden. Bei Verdacht auf eine Virusinfektion ist unverzüglich die IT-Administration des BIT zu informieren.

8.5 Fernzugriff auf interne Systeme (Remote – Zugriff)

Beschäftigten kann der Zugriff auf zentrale Serverdienste mit dienstlichen Endgeräten über eine VPN-Verbindung oder eine andere zertifikatbasierte Verbindung gestattet werden; die zuständigen Mitbestimmungsgremien sind zu beteiligen.

Beschäftigten kann der ausschließliche Zugriff auf Groupware-Dienste auch über private Endgeräte über eine zertifikatsbasierte Verbindung gestattet werden; die zuständigen Mitbestimmungsgremien sind zu beteiligen.

Die entsprechenden Zugriffe werden auf Antrag der jeweiligen Organisationseinheit vom BIT eingerichtet. Die Beteiligung der jeweils zuständigen Mitbestimmungsgremien ist nachzuweisen.

8.6 Nutzung dienstlicher mobiler Endgeräte und mobiler Datenträger

Im Rahmen der Nutzung **dienstlicher** mobiler Endgeräte (z.B. Laptops, Smartphones, Tabletts) sind durch die Beschäftigten folgende Dinge zu berücksichtigen:

- Die Endgeräte sind gegen Diebstahl zu schützen. Die Geräte sollten daher nicht unbeaufsichtigt aufbewahrt werden, insbesondere in Fahrzeugen. Dies gilt auch innerhalb der verwaltungseigenen Räume und insbesondere, wenn sich diese Räume in Gebäudebereichen mit Besucherverkehr befinden.
- Beim Verlust von mobilen Endgeräten ist die Leitung des Amtes oder der Dienststelle bzw. der/die jeweilige Fachverantwortliche sowie der BIT unverzüglich zu benachrichtigen.
- Die Beschäftigten haben Sorge zu tragen, dass der VPN-Client nicht von Dritten genutzt werden kann; dies gilt auch für Familienangehörige. Insbesondere muss sichergestellt sein, dass bei geöffneter VPN-Verbindung keine weiteren Internetverbindungen möglich sind.
- Auf den mobilen Endgeräten sollten keine Bürger- oder Beschäftigtendaten gespeichert werden. Ansonsten sind die Beschäftigten verpflichtet, die Fachverantwortlichen in den Ämtern und Dienststellen hierüber zu informieren, so dass entsprechende Verschlüsselungsmaßnahmen durch den BIT zur Verfügung gestellt werden.

EFL

- Dienstliche Smartphones dürfen auch zu privaten Zwecken[1] genutzt werden. Beim Laden von Apps haben die Nutzenden darauf zu achten, dass nur solche Applikationen auf das Smartphone geladen werden, die als verlässlich und sicher gelten. Auch haben sie darauf zu achten, dass die Betriebssysteme regelmäßig durch sie aktualisiert werden.

Die Nutzung mobiler externer Datenträger ist nur in Ausnahmefällen zulässig.

9. Inkrafttreten

Die IT-Sicherheitsrichtlinie tritt am Tage Ihrer Veröffentlichung in Kraft.

Die IT-Sicherheitsrichtlinie wird fortlaufend weiterentwickelt und entweder anlassbezogen oder mindestens alle 2 Jahre einer überprüfenden Revision unterzogen. Für die redaktionelle und inhaltliche Pflege und Weiterentwicklung der Richtlinie ist der / die IT-Sicherheitsbeauftragte zuständig.

E T R

[1] Gemäß § 3 Nr. 45 Einkommensteuergesetz sind die Vorteile des Arbeitnehmers aus der privaten Nutzung von betrieblichen Datenverarbeitungsgeräten und Telekommunikationsgeräten sowie deren Zubehör, aus zur privaten Nutzung überlassenen System- und Anwendungsprogrammen, die der Arbeitgeber auch in seinem Betrieb einsetzt, und aus den im Zusammenhang mit diesen Zuwendungen erbrachten Dienstleistungen steuerfrei (kein geldwerter Vorteil).

Anlage 1 (datenschutzrechtliche Einwilligungserklärung)
zur Richtlinie zur Informationssicherheit für das Magistratsnetz

Datenschutzrechtliche Einwilligungserklärung

Der Magistrat der Stadt Bremerhaven stellt allen Beschäftigten, die IT-Systeme nutzen, einen Internetzugang am Arbeitsplatz grundsätzlich nur zur Erfüllung von dienstlichen Aufgaben zur Verfügung. Gemäß Ziffer 8.2 der Richtlinie zur Informationssicherheit wird die private Nutzung gestattet, sofern eine individuelle Einwilligungserklärung vorliegt. Die private Nutzung ist in jedem Fall auf das Aufrufen von Inhalten sowie auf das Nutzen von externen Webmail-Diensten beschränkt. Ein Anspruch auf private Nutzung besteht nicht.

Nutzung des dienstlichen Internetzuganges für private Zwecke gemäß Ziffer 8.2 der Richtlinie zur Informationssicherheit für das Magistratsnetz	
☐	**Ich möchte den dienstlichen Internetzugang auch für private Zwecke nutzen.** **Mit dieser Einwilligung habe ich zur Kenntnis genommen**, • dass die Internetnutzung in der in der Richtlinie zur Informationssicherheit beschriebenen Weise zur Datenschutzkontrolle und zur Gewährleistung der technischen Sicherheit der Systeme protokolliert wird, • dass die private Nutzung auf das Abrufen von Inhalten sowie auf das Nutzen von externen Webmail-Diensten beschränkt ist, • dass kein Anspruch auf die private Nutzung besteht und der Magistrat die Nutzung von externen Webmail-Diensten zeitweise oder dauerhaft jederzeit widerrufen und / oder den Abruf von Inhalten zentral sperren kann. • dass die Verfolgung kommerzieller Zwecke im Rahmen der Privatnutzung untersagt ist.

Diese datenschutzrechtliche Einwilligungserklärung kann ich jederzeit ganz oder teilweise mit Wirkung für die Zukunft widerrufen. **Mir ist bekannt**, dass ich in diesem Fall den Internetzugang nur noch ausschließlich zu dienstlichen Zwecken verwenden darf. Eine Privatnutzung ist dann verboten.

(Hinweis: Zu einem späteren Zeitpunkt wird ein entsprechendes Formular zur Abgabe der individuellen Einwilligung gestaltet. Lediglich die Gestaltung dieses Formulars wird von der obigen Darstellung abweichen. Auch bei einer anderen Gestaltung wird es keine inhaltlichen Abweichungen zur obigen Darstellung geben).

N WUF