Dienstanweisung DA 11 / 09

Fach- und datenschutzgerechter Umgang mit der Informationstechnik

Inhaltsverzeichnis

Vermerke	Erstellt	Management-beauftragter	Geprüft (GF-B)	Freigabe (Geschäftsführung)
Datum	20.06.2010	21.06.2010		8.7.10
Unterschriften	Dr. Reichstein Kietzmann	Dr. Lehmann	Seidler	Lux Dr. Gaudig

Verteiler

- Beauftragtenwesen - GF-BW
- Bereich Systemtechnik - TS
- IT-Consult Halle GmbH - ITC

- weiter Verteilung: über EDV-Ablage

EDV-Ablage

Diese Dienstanweisung ist abgelegt im:

- Outlook (Öffentlicher Ordner → alle öffentlichen Ordner → HWS)

- Xinoah

Änderungsdienst / Aktualisierungen

Revisionsstufe	Änderungen	Datum
0	Original Rot: Änderungen/Ergänzungen gegenüber dem Entwurf	10.06.2010

1. Zweck und Zielstellung

Ziel dieser Dienstanweisung ist die Gewährleistung eines fachgerechten und datenschutzkonformen Umganges der Mitarbeiter mit der Datenverarbeitungs- und der Kommunikationstechnik des Unternehmens bei Ausübung ihrer Tätigkeit um damit die Verfügbarkeit der informationstechnischen Anlagen und der gespeicherten Daten sicherzustellen und Gesetzesverstöße zu vermeiden.

2. Geltungsbereich

Diese Dienstanweisung ist verbindlich für alle Arbeitnehmer und leitende Angestellte der Halleschen Wasser und Stadtwirtschaft GmbH (HWS GmbH) sowie für alle Auszubildenden und Praktikanten, die mit Informationstechnik arbeiten. Ferner gilt die Dienstanweisung für alle Partner der Halleschen Wasser und Stadtwirtschaft GmbH im Rahmen ihrer Tätigkeit.
Die Dienstanweisung gilt für alle Standorte/Objekte der Halleschen Wasser und Stadtwirtschaft GmbH sowie für mobile Informationstechnik auch außerhalb dieser Objekte.

3. Begriffe und Erläuterungen

Bildschirmgerät im Sinne der Bildschirmarbeitsverordnung ist ein Bildschirm zur Darstellung alphanumerischer Zeichen oder zur Grafikdarstellung, ungeachtet des Darstellungsverfahrens.

Bildschirmarbeitsplatz
Ein Bildschirmarbeitsplatz ist gemäß Bildschirmarbeitsverordnung ein Arbeitsplatz mit einem Bildschirmgerät, der ausgestattet sein kann mit:
a) Einrichtungen zur Erfassung von Daten,
b) Software, die den Beschäftigten bei der Ausführung ihrer Arbeitsaufgaben zur Verfügung steht,
c) Zusatzgeräten und Elementen, die zum Betreiben oder Benutzen des Bildschirmgeräts gehören (z.B. Tastatur), oder
d) sonstigen Arbeitsmitteln (z.B. Arbeitstisch, Arbeitsstuhl) sowie die unmittelbare Arbeitsumgebung (z.B. Beleuchtung).

Beschäftigte im Sinne der Bildschirmarbeitsverordnung sind Beschäftigte, die gewöhnlich bei einem nicht unwesentlichen Teil ihrer normalen Arbeit ein Bildschirmgerät benutzen.

Informationstechnik
ist ein Oberbegriff für die Informations- und Datenverarbeitung sowie für die dafür benötigte Hard- und Software. Häufig wird auch die englisch ausgesprochene Abkürzung **IT** verwendet. Dazu gehören:

a) Personalcomputer (PC) mit allen Hardwarekomponenten (z.B. CD-Laufwerk, Floppy) oder Laptop,
b) die gesamte Netzwerktechnik,
c) Peripheriegeräte (z.B. Drucker, Scanner),
d) alle zum Betrieb notwendige Software (Betriebssystem und Anwendungsprogramme) und
e) die Telekommunikationstechnik (Telefonanlage, -apparate, Faxgeräte, Modems, Mobiltelefone)

IT-Sicherheitsmanagement

dient der sicheren Verarbeitung von Informationen durch Sicherstellung eines gewissen Grundschutzes durch geeignete Anwendungen von organisatorischen, personellen, infrastrukturellen, und technischen Sicherheitsmaßnahmen, die für den Schutzbedarf angemessen und ausreichend sind. Mit Hilfe von Informationstechnik realisierte oder unterstützte **Verfahren** (Geschäftsprozesse) sollen systematisch gegen beabsichtigte Angriffe und unbeabsichtigte Ereignisse geschützt werden.

Personalverantwortliche Leiter

sind die Bereichsleiter sowie die Geschäftsführung der HWS GmbH.

Verfahrensverantwortliche

werden vom Informationseigentümer (Geschäftsführung der HWS GmbH) benannt und verantworten den korrekten Einsatz eines entsprechenden Verfahrens bzw. der dafür eingesetzten produktiven Software.
Der Verfahrensverantwortliche prüft die Ihm zugereichten Nutzerrechte und leitet diese an die administrierende Stelle weiter. Dem Verfahrensverantwortlichen obliegt die Ablage der vergebenen Zugangsberechtigungen bzw. die Pflege derselben in einer Datenbank. Der Verfahrensverantwortliche kann für ein Verfahren bzw. der hierfür eingesetzten Software selbst **Modulverantwortlicher** sein oder diese benennen.

Modulverantwortliche

werden durch die Verfahrensverantwortlichen festgelegt. Ihnen obliegt die Prüfung und Freigabe von Nutzerrechten für den Teilbereich der eingesetzten Software (Modul) für den sie die Modulverantwortung tragen. Die Beantragung erfolgt durch den personalverantwortlichen Leiter beim Verfahrensverantwortlichen unter Einbeziehung der Modulverantwortlichen.

Administrierende Stellen

sind Mitarbeiter der HWS GmbH sowie externe Firmen und Dienstleister, die vertraglich mit der Administration bestimmter bei der HWS GmbH eingesetzter Verfahren (produktive Software) beauftragt sind. Umfang und Art der Administration wird in den entsprechenden Verträgen geregelt. Eine Veränderung der Produktivdaten durch die administrierende Stelle ist generell untersagt.

4. Aufgaben, Zuständigkeiten und Verantwortung

Nr.	Managementschritt	Verantwortlich-keitsgrad	Zuständige Struktureinheit
(1)	Verfahrensbeschaffung / Installation	Verantwortung	Bereichsleiter Systemtechnik
		Mitwirkung	Verfahrensverantwortlicher
		Durchführung	Verfahrensverantwortlicher, administrierende Stellen
		Information	Betriebsrat
		Kontrolle	IT-Sicherheitsbeauftragter Datenschutzbeauftragter
(2)	Verfahrenstestung / Freigabe	Verantwortung	Verfahrensverantwortlicher
		Mitwirkung	Bereichsleiter Systemtechnik
		Durchführung	Verfahrensverantwortlicher Modulverantwortlicher
		Kontrolle	IT-Sicherheitsbeauftragter Datenschutzbeauftragter
(3)	Erstellen der Verfahrensdokumentation	Durchführung	Verfahrensverantwortlicher
		Mitwirkung	Bereichsleiter Systemtechnik
		Information	Datenschutzbeauftragter, Betriebsrat
		Kontrolle	IT-Sicherheitsbeauftragter
(4)	Verfahrens-Nutzerberechtigungen	Durchführung	Verfahrensverantwortlicher, Modulverantwortlicher
		Mitwirkung	zuständiger Bereichsleiter, Bereichsleiter Systemtechnik
		Information	Datenschutzbeauftragter
		Kontrolle	IT-Sicherheitsbeauftragter, Datenschutzbeauftragter
(5)	Verfahrens-Administration	Verantwortung	Bereichsleiter Systemtechnik, Verfahrensverantwortlicher
		Durchführung	administrierende Stellen
		Information	Datenschutzbeauftragter
		Kontrolle	Verfahrensverantwortlicher, IT-Sicherheitsbeauftragter
(6)	Verfahrensdaten-Sicherheit (Backup, Updates...)	Verantwortung	Bereichsleiter Systemtechnik, Verfahrensverantwortlicher
		Durchführung	administrierende Stellen
		Information	Datenschutzbeauftragter
		Kontrolle	Verfahrensverantwortlicher, IT-Sicherheitsbeauftragter

5. Beschreibung

5.1 IT- Sicherheitsleitlinie

5.1.1 Einleitung

Die Informationsverarbeitung spielt in der Halleschen Wasser und Stadtwirtschaft GmbH (HWS GmbH) eine Schlüsselrolle für die Aufgabenerfüllung. Informationen entscheiden über den Erfolg des Unternehmens. Von größter Wichtigkeit ist neben der Genauigkeit und Verfügbarkeit in den meisten Fällen auch die Vertraulichkeit von Informationen. Alle Beschäftigten müssen sich daher der Notwendigkeit der Informationssicherheit bewusst sein und entsprechend handeln.

Diese Maßnahmen sind nicht nur gesetzlich vorgeschrieben sondern auch Teil der Verpflichtung gegenüber Aufsichtsbehörden sowie Kunden und Zulieferern. Jeder Beschäftigte der Halleschen Wasser und Stadtwirtschaft GmbH hat sich daher an diese Sicherheitsrichtlinie und die sich daraus ergebenden Standards und Vorgaben zu halten.

Die Auswahl der zu ergreifenden Sicherheitsmaßnahmen wird durch die Geschäftsleitung festgelegt. Basis dieser Festlegung sind die Gesetzeslage, die Empfehlung der IT-verantwortlichen Mitarbeiter im Unternehmen sowie externer Berater. Die grundlegenden Ziele der IT- Sicherheitsmaßnahmen sind:

- Vermeidung von Gesetzesverstößen sowie die damit verbundene Verhinderung von Rechtsverfahren oder materiellen Verlusten für Mitarbeiter und Unternehmen
- Sicherstellung der Verfügbarkeit informationstechnischer Anlagen und den darauf gespeicherten Daten.

Alle Maßnahmen werden vor der Anwendung auf ein wirtschaftlich vertretbares Verhältnis zum Wert der schützenswerten Information überprüft. Grundsätzlich sind bei jeder Nutzung von den Geräten und der Verarbeitung von Informationen die einschlägigen Gesetze, wie z.B. Strafgesetzbuch, Handelsgesetzbuch, Sozialgesetzbuch und Bundesdatenschutzgesetz einzuhalten. Negative materielle oder immaterielle Schäden in Folge der Nutzung sind für Beschäftigte und Unternehmen zu vermeiden, Gesetzesverstöße zu unterbinden.

Diese Dienstanweisung zur Nutzung der Informationstechnik ist für jeden Anwender oder Partner im Rahmen seiner Tätigkeit für die HWS GmbH verbindlich. Sie betrifft somit alle Angestellten, Vertragspartner, externe Dienstleistungsunternehmen, Berater, Lieferanten und verbundene Unternehmen, sofern sie IT-Systeme der HWS GmbH nutzen. Ihre Einhaltung wird überprüft.

Diese Dienstanweisung ergänzt die gesetzlichen Regeln für den Umgang mit personenbezogenen Daten, welche von jedem Beschäftigten ebenfalls zu beachten und einzuhalten sind. Daneben finden spezielle Regelungen (Detailbeschreibungen) zur Nutzung ausgewählter Techniken und Dienste ergänzend Anwendung.

5.1.2 IT- Sicherheitsmanagement

Zur Erreichung der IT-Sicherheitsziele wurde in der HWS GmbH eine IT-Sicherheitsorganisation eingerichtet. Es ist ein IT-Sicherheitsbeauftragter sowie entsprechend der gesetzlichen Regelungen ein Datenschutzbeauftragter bestellt. Diese berichten in ihrer Funktion direkt an die Mitglieder der Geschäftsführung.

Der IT-Sicherheitsbeauftragte ist frühzeitig in alle die Informationstechnik tangierenden Projekte einzubinden und somit sind schon in der Planungsphase sicherheitsrelevante Aspekte zu berücksichtigen. Sofern personenbezogene Daten betroffen sein können, gilt gleiches für den Datenschutzbeauftragten.

Sowohl der Datenschutzbeauftragte als auch der IT-Sicherheitsbeauftragte sind in ihrer Eigenschaft neben den organisatorischen Leitern (Bereichs- und Abteilungsleiter) Ansprechstelle für die Beschäftigten und Partner. Weiter legen sie Inhalte für Schulungen und Informationsveranstaltungen fest und entwickeln ein Sicherheitsbewusstsein im Unternehmen.

Die sich entwickelnde Verhaltenskultur ist gekennzeichnet durch:

- die Erkenntnis eines jeden Anwenders, dass effektive Sicherheit ein kritisches und wesentliches Element der Unternehmensphilosophie ist,
- ein stets vorhandenes Sicherheitsbewusstsein bei allen täglich anfallenden Arbeiten und Aktivitäten
- die persönliche Verantwortlichkeit des Einzelnen für proaktive Maßnahmen im Bezug auf sämtliche Risiken für Beschäftigte, Informationen, Vermögenswerte und Fortführung der Geschäftstätigkeit im Notfall.

5.1.3 Qualitätskontrolle

Das Managementsystem der IT-Sicherheit wird regelmäßig auf seine Aktualität und Wirksamkeit geprüft und im Jahresbericht des IT-Sicherheitsbeauftragten dokumentiert. Daneben werden auch die Maßnahmen regelmäßig daraufhin untersucht, ob sie dem betroffenen Beschäftigten bekannt, umsetzbar und in den Betriebsablauf integrierbar sind. Die Unternehmensleitung unterstützt den ständigen Optimierungs- und Verbesserungsprozess des Sicherheitsniveaus. Getrieben wird dieser durch den IT-Sicherheitsbeauftragten und den Datenschutzbeauftragten. Beschäftigte sind angehalten durch Verbesserungsvorschläge sowie durch die Meldung von Schwachstellen an diesem Verbesserungsprozess mitzuwirken.

5.1.4 Kontrolle, Sanktionen und Dokumentationen

Die Kontrolle der Einhaltung der IT-Sicherheitsleitlinie und der daraus folgenden Dokumente wird durch verschiedene Verfahren sichergestellt. Zunächst durch automatisierte Verfahren und Logbücher. Diese werden durch Anwendungen, Sicherheitssoftware und Betriebssysteme automatisch erstellt. Bei Bedarf findet eine Auswertung statt. Weiter obliegt die Kontrolle der Einhaltung den verantwortlichen Leitern der verschiedenen Bereiche der Halleschen Wasser und Stadtwirtschaft GmbH sowie dem Datenschutz- und dem IT-Sicherheitsbeauftragten.

Zusätzlich führt die HWS GmbH regelmäßig Audits durch externe Beratungsunternehmen, wie Wirtschaftsprüfer oder IT- Sicherheitsaudits, durch. Hier wird die Einhaltung bestätigt, der Verbesserungsprozess befördert und Verstöße zu diesen Verhaltensregeln festgestellt.

Verstöße gegen diese Sicherheitsleitlinie bzw. die daraus resultierenden Detailbeschreibungen und Anweisungen zur Anwendung der Informationstechnik und der Verarbeitung der Daten, insbesondere der Umgang mit personenbezogenen Daten, können arbeitsrechtliche und strafrechtliche Konsequenzen haben und werden von der Geschäftsführung geahndet. Sie können Grund für Abmahnungen, eine ordentliche bzw. fristlose Kündigung sein. Weiter werden bei Verstößen gegen geltende Gesetze Ermittlungsverfahren eingeleitet bzw. unterstützt.

Geltende Dienst- und Arbeitsanweisungen, Richtlinien für einzelne Aspekte oder technische Anweisungen werden im Outlook (ab April 2010 in Xinoah) veröffentlicht und tragen damit verbindlichen Charakter.

5.2 Grundsätze

Im Rahmen der Nutzung der Informationstechnik haben Beschäftigte, Vertragspartner oder Berater bei Ihrer Tätigkeit für die HWS GmbH die jeweils geltenden Regelungen, Anweisungen, Gesetze und Vorschriften zur Gewährleistung von Datenschutz und Datensicherheit einzuhalten.

Nutzer, die eine Verletzung der Sicherheitsrichtlinie und damit verbundenen Informationssicherheitsstandards vermuten, Kenntnis davon erlangt haben bzw. annehmen, dass die Information nicht in geeigneter Weise geschützt werden, haben dies unverzüglich ihrem Vorgesetzten, dem IT- Sicherheits- oder dem Datenschutzbeauftragten zu melden

Die im Netzwerk der HWS GmbH sowie die an Einzelarbeitsplätzen installierten Personalcomputer dürfen ausschließlich zu Unternehmenszwecken eingesetzt werden. Die Zugriffsberechtigung auf Daten und Programme erfolgt ausschließlich auf Antrag der jeweils zuständigen Bereichsleiter bzw. der Geschäftsführung. Mit der Zugriffsberechtigung sind Mitarbeiter zu schulen und einzuweisen. Jeder Mitarbeiter ist auf das Datengeheimnis gemäß § 5 Bundesdatenschutzgesetz zu verpflichten (DA 10/09, Anlage 1). Veränderung der Installation am Arbeitsplatz ist untersagt. Das Benutzen von externen Datenträgern (z.B. Disketten, CD-ROM, USB-Sticks, tragbare Massenspeicher) zum Export oder Import von Daten ist nur in Ausnahmen gestattet (siehe Punkt 5.10).

Jedes Gerät ist zur Identifikation mit einem standardisierten Aufkleber mit Inventarnummer zu versehen.

5.3 Zugriffsberechtigung auf Daten und Programme

An- und Abmeldungen von Nutzern sowie deren jeweilige Zugriffsrechte beantragt der zuständige personalverantwortliche Leiter mit dem Antragsformular gemäß **Anlage 1** beim Verfahrensverantwortlichen. Der Bereich Personal/Organisation meldet an die personalverantwortlichen Leiter jeden Mitarbeiter der HWS GmbH, der für das Unternehmen tätig werden soll vor dessen Einstellungsdatum jeden Wechsel des Bereiches und/oder der Stelle sowie jedes Ausscheiden eines Mitarbeiters. Der personalverantwortliche Leiter gibt diese Informationen an die Verfahrensverantwortlichen weiter.

Die Information pro HWS-Mitarbeiter umfasst die Personalnummer, Vornamen, Nachnamen, Bereich und das Datum ab dem die Tätigkeit beginnt bzw. endet.

Bei Anmeldung eines neuen Nutzers darf die Umsetzung durch die administrierende Stelle erst dann erfolgen, wenn der Nachweis über die erfolgte Datenschutzbelehrung gemäß DA 10/09 vorliegt. Dies wird durch Unterschrift des Datenschutzbeauftragten auf dem Antragsformular bestätigt. Bei Änderungen von Berechtigungen eines bestehenden Nutzers (z.B. Umsetzung) sowie einer Abmeldung ist diese Unterschrift nicht notwendig.

Die administrierende Stelle richtet bei Neuanmeldungen einen personengebundenen Zugang (Login-Name, Passwort) ein. Mitarbeiter ohne Einrichtung eines personengebundenen Zuganges sind nicht an PC-Arbeitsplätzen einzusetzen. Nach der Erstanmeldung ist das Passwort zu ändern, es ist vor anderen Mitarbeitern sowie Dritten geheim zu halten. Die Nutzer haben ihr Passwort spätestens aller 90 Tage zu ändern. Das Passwort muss eine Mindestlänge von 6 Zeichen haben und Ziffern oder Sonderzeichen enthalten. Es darf nicht mit den vorher gültigen Passwörtern übereinstimmen. Kann nicht ausgeschlossen werden, dass ein Unbefugter Einblick in das Passwort erhalten hat, ist dieses zu ändern.

Aus Gründen des Datenschutzes sowie zur Wahrung von Betriebsgeheimnissen bzw. zur Verhinderung, dass sich Dritte an dem PC-Arbeitsplatz eines Mitarbeiters Zugang zu dem EDV-System verschaffen, ist generell beim auch nur kurzzeitigen Verlassen des Arbeitsplatzes die Arbeitsstation (PC) zu sperren. Die Entsperrung darf dann nur über die Eingabe des Nutzerpasswortes möglich sein.

Die Nutzung des DV-Netzes ist für alle Mitarbeiter wochentags auf die Zeit von 06.00 Uhr bis 20.00 Uhr beschränkt. Ausnahmen bzw. Sonderregelungen für einzelne Bereiche und/oder Objekte sind gesondert geregelt. Die Möglichkeit des Arbeitens im Netz außerhalb der festgelegten Zeiten ist mindestens 48 Stunden vorher beim Verfahrensverantwortlichen zu beantragen.

Um Rechte innerhalb eines Fachbereiches kontrolliert vergeben zu können, ist für jeden PC-Arbeitsplatz zu definieren, zu welcher Software und eventuell Teilen derselben der Mitarbeiter an diesem PC-Arbeitsplatz welche Zugriffsberechtigungen erhält. Das Gleiche gilt für nicht mehr erforderliche Softwarezugriffe. Verantwortlich sind die zuständigen Verfahrensverantwortlichen.

Die Beantragung erfolgt durch den personalverantwortlichen Leiter unter Verwendung des Formblattes (**Anlage 1**) bei den Verfahrensverantwortlichen. Auf dem Formular sind durch den personalverantwortlichen Leiter die genauen Bezeichnungen der Zugriffsrechte zu benennen. Sollen verfahrensübergreifend Rechte vergeben werden, ist dies auf **Anlage 1** durch alle betreffenden Verfahrensverantwortlichen per Unterschrift zu bestätigen. Im Falle der Produktivsysteme ist zusätzlich die jeweilige Liste der Aktivitätsgruppen (**Anlage 3 bis 7**) beizufügen und separat durch den Verfahrensverantwortlichen (**Anlage 10**) zu unterzeichnen. Die Unterschrift kann auch durch den Modulverantwortlichen erfolgen, sofern ein solcher benannt ist. In diesem Fall ist durch den Modulverantwortlichen die **Anlage 1** zu paraphieren.

Bei Personalunion von personalverantwortlichem Leiter und Verfahrensverantwortlichem muss auf der **Anlage 1** ein weiterer Verfahrensverantwortlicher unterzeichnen sofern keine Paraphierung durch einen Modulverantwortlichen erfolgt.

In jedem Fall ist die **Anlage 1** abschließend an den Bereichsleiter Systemtechnik zu übergeben. Dies kann mittels Kopie auch nach Einrichtung der Zugänge erfolgen.

Die administrierende Stelle hat die erforderlichen Zugriffe einzurichten bzw. zu löschen. Die vorgenommene Eingabe wird mit Datum und Unterschrift auf den Anträgen dokumentiert.

Nach Einrichtung erfolgt durch die administrierende Stelle eine kurze Mitteilung an die Mitarbeiter (Nutzer) über Zugangsname und Initialpasswort sowie den oder die Verfahrensverantwortlichen.
Um die Berechtigungsprofile der Nutzer nachvollziehbar zu dokumentieren, sind durch den Bereichsleiter Systemtechnik Berechtigungsakten je Mitarbeiter zu führen.

5.4 Zugangsberechtigungen für Externe

Externen Dienstleistern werden nur im Ausnahmefall Zugriffsrechte zum Netzwerk oder Einzelarbeitsplätzen vergeben. Derartige Fälle sind vorab durch den Verfahrensverantwortlichen bei der administrierenden Stelle anzumelden. Wartungen erfolgen nur in Anwesenheit des den Verfahrensverantwortlichen bzw. eines Vertreters der administrierenden Stelle. Über alle ausgeführten Wartungen sind Protokolle anzulegen.
Diese Protokolle müssen folgende Punkte enthalten:

- Auftraggeber (Name und Bereichsangabe)
- Ausführender (Name und Firma)
- Grund der Wartung und Veränderung
- vorgenommene Änderungen
- Datum
- Unterschrift Auftraggeber und Auftragnehmer

Sollten direkte Änderungen des Dateninhaltes notwendig erscheinen, ist dies vorab durch den Verfahrensverantwortlichen zu prüfen. Weiterhin ist vor und nach diesen Änderungen der Dateninhalt abzufragen, und entsprechend zu sichern, da diese Änderungen systemseitig nicht protokolliert werden. Die Änderungen werden auf den Ausdrucken handschriftlich durch den Verfahrensverantwortlichen abgezeichnet und archiviert.

Ist ein dauerhafter Zugriff auf das Netzwerk bzw. eine Ressource der HWS GmbH für einen externen Dritten vorgesehen (z.B. Shared Service, Sichtrechte Umweltamt), so hat die Anmeldung ebenfalls mittels des Formblattes (**Anlage 1**) sowie jeweils weiterer notwendiger Anlagen zu erfolgen, wobei hier jeweils der Verfahrensverantwortliche unterzeichnet. In einem solchen Fall ist das externe Unternehmen auf dem Antrag zu vermerken. Sollte eine Verpflichtung des Externen auf das Datengeheimnis bereits in eigenen Reihen erfolgt sein, so ist dem Datenschutzbeauftragten der HWS GmbH eine Kopie der Verpflichtungserklärung zu übergeben, andernfalls erfolgt die Verpflichtung durch den Datenschutzbeauftragten der HWS GmbH.

5.5 Jährlich wiederkehrende Überprüfung der IT-Berechtigungen

Um eine Kontrolle der im Netzwerk der HWS GmbH vergebenen Rechte fortwährend sicherzustellen, erfolgt durch den IT-Sicherheitsbeauftragten in Zusammenarbeit mit dem Datenschutzbeauftragten einmal jährlich eine stichprobenartige Kontrolle der vergebenen IT-Berechtigungen. Dazu werden in Abstimmung mit den Verfahrensverantwortlichen zufällig mindestens 10 % aller Mitarbeiterzugriffsrechte geprüft, wobei alle Bereiche vertreten sein müssen. Grundlage bildet die jeweils aktuelle EDV-seitige Abbildung der Organisationsstruktur. Die Verfahrensverantwortlichen stellen hierzu eine stichtagsbezogene Übersicht der vergebenen Rechte je Mitarbeiter zur Verfügung. Darin sind die folgenden Daten enthalten:

- Name, Vorname
- Team und/oder Bereich
- Email-Adresse
- Datum der letzten Anmeldung im HWS-Netzwerk
- Ggf. Enddatum bei befristeter Anmeldung
- Gruppenmitgliedschaften (Zugang zu Programmen und Rechte auf Server)
- Datum der letzten Anmeldung in den Produktivsystemen
- Gruppenzugehörigkeit des Nutzers in diesen Produktivsystemen (Rechte)

Der IT-Sicherheitsbeauftragte prüft die ihm übergebene Auswertung entsprechend der IT-Sicherheitsleitlinie, der Datenschutzbeauftragte beurteilt diese aus datenschutzrechtlicher Sicht. Es erfolgt eine Prüfung hinsichtlich der im Unternehmen integrierten Berechtigungskonzepte auf Umsetzung und Aktualität bezogen auf die einzelnen Nutzer. Besteht Handlungsbedarf hinsichtlich der vergebenen Berechtigungen, werden die jeweiligen Bereichsleiter vom IT-Sicherheitsbeauftragten darauf hingewiesen. Sind Änderungen erforderlich, werden diese durch die Bereichsleiter veranlasst. Ggf. notwendige Ausnahmeregelungen werden im Rahmen der Prüfung in Abstimmung mit den Bereichsleitern dokumentiert.

Nach Abschluss der Prüfung unterzeichnen der IT-Sicherheitsbeauftragte und der Datenschutzbeauftragte je Mitarbeiter sowie der Bereichsleiter für die jeweils geprüfte Abteilung / den Bereich.

Die geprüften und unterzeichneten Berechtigungen sowie die damit in Zusammenhang stehenden Dokumentationen werden durch den IT-Sicherheitsbeauftragten abgelegt und mindestens 5 Jahre ab dem Zeitpunkt der Überprüfung aufbewahrt.

Mit dem neuen Jahr beginnt der stichprobenartige Kontrolldurchlauf der in der HWS GmbH vergebenen IT-Berechtigungen erneut.

Unabhängig von der jährlich wiederkehrenden Überprüfung können sowohl der IT-Sicherheitsbeauftragte als auch der Datenschutzbeauftragte stets eine solche Auswertung für von den Verfahrensverantwortlichen abfordern.

5.6 Zugang zu Altdaten

Nicht mehr benötigte Programmsysteme werden offline gesetzt und der Zugang allen Nutzern entzogen. In solchen Fällen müssen die Programme jedoch weiterhin vorgehalten werden. Gegebenenfalls kann es jedoch zu Prüfungs- oder Recherchezwecken nötig werden, auf die entsprechenden Altdaten zuzugreifen.

Wenn es nicht möglich ist, für ein solches Programm ausschließlich lesende Zugriffsrechte zu administrieren, ist hier mittels des Formulars in **Anlage 8** der Zugang zu beantragen. Dabei ist so vorzugehen, wie auf dem Formular beschrieben.

5.7 Protokollierung von Zugriffen auf Daten und Programme

Die HWS GmbH setzt physische Zugangskontrollen sowie Loginverfahren für sämtliche von ihr betriebenen Informationssysteme ein. Zugriff auf Informationen darf den Nutzern nur für definierte Geschäftsbedarfe gewährt werden. Diese werden im entsprechenden Berechtigungsbeantragungsverfahren erteilt. Der Zugriff, insbesondere die Veränderung von Daten, sind entsprechend des verfahrensspezifischen Sicherheitskonzeptes zu protokollieren.
Die Protokolle werden gespeichert und entsprechend der gesetzlichen Regelfristen archiviert. Bei Bedarf muss eine Auswertung möglich sein. Die Protokolldateien dienen den Zwecken der Datenschutzkontrolle, der Datensicherung, der Missbrauchsaufsicht sowie der Sicherstellung eines ordnungsgemäßen Betriebes und werden nicht zur Leistungskontrolle verwendet.

5.8 Beschaffung von Hardware

Die Bereichsleiter beauftragen den Bereich Systemtechnik zur Bereitstellung von Hardware für die Mitarbeiter unter Angabe des Umfanges der Ausstattung (**Anlage 9**).

Die administrierenden Stellen sind verantwortlich für die Bereitstellung und Passfähigkeit der Hardware gemäß Investitionsplan. Nach Aufstellung der Hardware bei den Nutzern erfolgt eine kostenstellengemäße Umverteilung zu Lasten der betreffenden Bereiche. Die Nutzung privater Geräte ist unzulässig.

5.9 Einführung neuer Verfahren

Vor der Einführung neuer Verfahren automatisierter Verarbeitung wird durch den Verfahrensverantwortlichen eine Übersicht gemäß § 4e Bundesdatenschutzgesetz erstellt und an den Datenschutzbeauftragten übergeben. Mit einem neuen Verfahren ist dabei nicht ausschließlich eine neue Softwarelösung gemeint sondern jede automatisierte oder gleichgestellte Verarbeitung von Daten.

Gibt es keinen Verfahrensverantwortlichen dem ein neues Verfahren zugeordnet werden kann, ernennt die Geschäftsführung einen neuen Verfahrensverantwortlichen.
Soll neue Software eingeführt werden, informieren die Bereiche den Bereich Systemtechnik, die Verfahrensverantwortlichen sowie die administrierenden Stellen rechtzeitig über ihren Bedarf. Die administrierenden Stellen beraten die Nutzer und prüfen die Kompatibilität zur Hardwarekonfiguration sowie zu vorhandenen Anwendungen.

Es ist ausschließlich lizenzierte und möglichst testierte Software einzusetzen. Der nutzende Bereich ist verantwortlich für die sachliche Prüfung von Software und die Nutzung im Unternehmen. Software ist ausschließlich durch die Bereiche Systemtechnik und Abteilung Einkauf/Materialwirtschaft zu beschaffen. Die Nutzung selbstbeschaffter Software ist unzulässig.

5.10 Externe Datenträger

Über die Verwendung externer Datenträger (insbesondere Disketten, CD-/DVD-ROMs, USB-Sticks, tragbare Massenspeicher u.a.) zum Datenaustausch mit Dritten (Stadtverwaltung, Banken, Großkunden usw.) entscheidet der jeweilige Verfahrensverantwortliche. Dieser kann die administrierenden Stellen zum Transfer von Daten auf oder von externen Datenträgern beauftragen. Diese stellen sicher, dass in diesem Fall jeder Datenträger bei jedem Im- und Export aus dem Netzwerk mit einem aktuellen Virenprüfprogramm untersucht wird.

Die Arbeit mit externen Datenträgern an einem Arbeitsplatz eines Mitarbeiters erfolgt im Ausnahmefall. Die administrierende Stelle sichert, dass ein aktuelles Virenprüfprogramm auf dem PC installiert ist. Alle Mitarbeiter erhalten eine gesonderte Sicherheitsbelehrung (**Anlage 2**). Entsprechend dieser sind alle externen Datenträger vor deren Verwendung durch den Nutzer selbst auf Viren und Schadprogramme zu untersuchen.

Die Nutzung von externen Datenträgern an einem Arbeitsplatz wird durch den zuständigen personalverantwortlichen Leiter mit dem Antragsformular (**Anlage 1**) beantragt und durch den Verfahrensverantwortlichen für die IT-Grundrechte (Bereichleiter Systemtechnik) bestätigt. Die Nutzung externer Datenträger an den Arbeitsstationen eines Bereiches ist bedarfsorientiert gering zu halten.

5.11 Nutzung von mobilen Geräten

Die durch die HWS GmbH zur Verfügung gestellten mobilen Geräte sind ausschließlich für tätigkeitsbezogene Arbeiten im Rahmen des Arbeitsverhältnisses einzusetzen. Diese Geräte dienen der Bearbeitung unternehmungsspezifischer Daten sowie in Absprache mit den Verfahrensverantwortlichen der Kommunikation mit Lieferanten, Kunden und dem Unternehmenszweck dienlichen Kommunikationspartnern. Unternehmensrelevante Daten sind nach Möglichkeit täglich, jedoch mindestens einmal pro Woche auf die zentralen Speichersysteme zu übertragen. Beim Einsatz von mobilen Geräten ist der Gerätebenutzer für das regelmäßige Update der Signaturen und der aktuellen Virenpattern selbst zuständig. Dies gilt insbesondere dann, wenn mit dem Gerät eine Einwahl in das Unternehmensnetzwerk realisiert wird.

5.12 Nutzung von Internet und Email

Die Beschäftigten der HWS GmbH dürfen Internet und Email ausschließlich zu geschäftlichen Zwecken zur Erledigung ihrer Aufgaben im Rahmen des Arbeitsverhältnisses nutzen. Die Nutzung des Internets oder Emails zu privaten Zwecken ist untersagt. Die genaue Beschreibung der Nutzungsrichtlinie ist in der Detailbeschreibung in der Dienstanweisung DA 12/09 sowie deren Anlage 1 (Benutzerrichtlinie) festgelegt.

5.13 Nutzung von VPN (Virtuelles Privates Netzwerk)

Das VPN stellt keinen generellen Zugang zum lokalen Netzwerk dar. Es wird daher nur ausgewählten Personen zur Verfügung gestellt, die aufgrund ihrer spezifischen Aufgabenstellung externen Zugang zu Dateien und Servern der HWS GmbH benötigen. Im Betriebsfall dürfen nicht gleichzeitig Schnittstellen zu einem anderen Internetserviceprovider genutzt werden.

5.14 Sicherung der Datenunverlierbarkeit

Zur Gewährleistung der Datenunverlierbarkeit werden regelmäßige Sicherungen des Datenbestandes durchgeführt, um bei Systemstörungen auf der Sicherungsbasis einen geordneten Wiederanlauf durchführen zu können. Die Verfahrensverantwortlichen können sich hierbei der administrierenden Stellen bedienen bzw. auf die Gestaltung der entsprechenden Dienstleistungsverträge hinwirken.

Wann welche Datenbestände/Datenpfade (z.B. auf Grund von Periodenabschlüssen) außerhalb der täglichen Sicherungen separat zu sichern sind und wie lange diese archiviert werden müssen, wird durch die jeweils Verfahrensverantwortlichen festgelegt und mit der administrierenden Stelle abgestimmt. Um die Zuverlässigkeit und Sicherheit der Anwendungssysteme zu gewährleisten, sind regelmäßige Kontrollen (Datendiagnose, Datenintegritätsprüfung) durch die betroffenen Fachbereiche zu veranlassen.

5.15 Sonstige Verhaltenspflichten

Alle sicherheitsrelevanten Ereignisse (unerklärliches Systemverhalten, Verlust von Daten oder Programmen, Verdacht auf Missbrauch der Benutzerkennung usw.) sind sofort dem IT-Sicherheitsbeauftragten, dem Datenschutzbeauftragten oder dem Verfahrensverantwortlichen zu melden.

Es ist unzulässig, Dateien auf Datenträger zu überspielen und diese mit nach Hause zu nehmen, sofern dies nicht anders geregelt ist. Dies gilt sowohl für firmenbezogene Daten, als auch für lizenzierte Software. Dateien dürfen nur zu Sicherheitszwecken kopiert werden.

Scheiden Beschäftigte aus dem Unternehmen aus, so sind alle für das Unternehmen relevanten Daten an die Verfahrensverantwortlichen bzw. Vorgesetzten zu übergeben. Es ist strikt untersagt, Programmdateien, Systemdateien oder relevante Datenbestände von entsprechenden Programm- oder Serververzeichnissen zu löschen oder Festplatten zu formatieren.

Unbefugten ist jeder Zugriff auf den PC und das lokale Netzwerk und den darin gespeicherten Daten zu verwehren. Das Ausprobieren, das Ausforschen und die Benutzung fremder Zugriffsberechtigungen und sonstiger Authentifizierungsmittel sind unzulässig und werden geahndet.

Die Weitergabe und das zur Verfügung stellen von eigenen Benutzerkennungen und sonstiger Authentifizierungsmittel für die Benutzung durch Dritte sind unzulässig. Ausdrücklich wird darauf hingewiesen dass in einem derartigen Fall aus Protokolldateien die Identität der Beschäftigten hervorgeht. Jegliche Aktivität durch diesen kann auf den Beschäftigten zurückgeführt und ihm angelastet werden. Passwörter müssen den entsprechenden Sicherheitsstandards genügen. Die Festlegungen hierzu werden in den entsprechenden Detailbeschreibungen getroffen. Bei Fragen hierzu steht der Verfahrensverantwortliche oder der IT-Sicherheitsverantwortliche und Datenschutzbeauftragte zur Verfügung.

6. Nachweisdokumentation

Aufzeichnung	Aufbewahrungsort	Aufbewahrungsdauer
Berechtigungsakte (Antrag Nutzerzugang + Folgedokumente)	Bereich Systemtechnik	mind. 10 a nach Beendigung der Beschäftigung
Sicherheitsbelehrung über externe Datenträger	DSB, Berechtigungsakte	10 a
Antrag auf Altdatenzugang	Verfahrensverantwortliche	10 a ab Systemabschaltung
Antrag PC/Peripherie	Bereich Systemtechnik	10 a
Dokumentation der jährlichen IT-Berechtigungsprüfung	IT-Sicherheitsbeauftragter	5 a
Übersicht der Verfahrens- und Modulverantwortlichen	Bereich Systemtechnik, administrierende Stellen	10 a bei nicht mehr gültigen Versionen

7. Mitgeltende Unterlagen / Regelungen, verbindliche Anschlussdokumente

- Bundesdatenschutzgesetz (BDSG) in der jeweils aktuellen Fassung
- Aktuelle Rahmenvereinbarung und Einzelverträge zwischen der Halleschen Wasser und Stadtwirtschaft GmbH und der IT-Consult Halle GmbH
- DA 10/09 Datenschutz
- DA 03/09 Kreditorische Zahlungen im bargeldlosen maschinellen Zahlungsverkehr (Zahlungsverkehr und Buchführung)
- DA 01/10 IT-Sicherheitsbeauftragter
- DA 01/09 Arbeitsorganisatorische Grundsätze
- DA 02/09 Zahlungsverkehr, Prüf- und Zeichnungsbefugnisse
- DA 12/09 Internet- und E-Mailnutzung
- DA 07/11 Archivordnung

8. Anlagenverzeichnis

Anlage 1 – Antrag auf Einrichtung eines Nutzerzuganges
Anlage 2 – Sicherheitsbelehrung über den Gebrauch Externer Datenträger
Anlage 3 – Zugriffsberechtigungen SAP R/3
Anlage 4 – Zugriffsberechtigungen opti.abfallwirtschaft (AWI)
Anlage 5 – Zugriffsberechtigungen opti.gebührenabrechnung (GA)
Anlage 6 – Zugriffsberechtigungen Schleupen
Anlage 7 – Zugriffsberechtigungen SMALLWORLD
Anlage 8 – Antrag auf Zugang zu Altdaten
Anlage 9 – Antrag auf Bereitstellung/Umsetzung von PC und Peripherie
Anlage 10 – Übersicht der Verfahrens- und Modulverantwortlichen