Gemeindeprüfungsanstalt
Baden-Württemberg

Az. 048.00

18.06.2012

Empfehlungen zur Gestaltung einer Dienstanweisung für die Berechtigungsverwaltung

Sonderheft 1/2012 der GPA-Mitteilungen

Gemeindeprüfungsanstalt Baden-Württemberg
76133 Karlsruhe · Hoffstraße. 1a · Telefon 0721 / 8 50 05 - 0

www.gpabw.de

Vorbemerkungen

1 Ausgangslage

Finanzwirksame Geschäftsprozesse werden überwiegend unter Einsatz von Verfahren der automatisierten Datenverarbeitung (im Folgenden als „Verfahren“ bezeichnet) abgewickelt. Bei Anwendung solcher Verfahren sind geeignete, technische und organisatorische Rahmenbedingen zu schaffen, um ein Höchstmaß an Daten- und Programmsicherheit zu erreichen. Dazu gehören nicht nur programmtechnische Maßnahmen, sondern auch **organisatorische Vorgaben** (Handlungsanweisungen) zum Programmeinsatz und zur Programmanwendung. Es obliegt dem Bürgermeister, die „Sicherung“ der eingesetzten finanzwirksamen Verfahren schriftlich zu regeln (§ 6 GemKVO, § 35 Abs. 6 Satz 1 GemHVO i.V.m. § 28 Abs. 1 GemKVO).

Die GPA hat bereits im Jahr 1993 „Anregungen zur Gestaltung einer Dienstanweisung für die Berechtigungsverwaltung unter dem Online-Steuerungssystem OSSY[1]“ veröffentlicht. Mit Blick auf die zunehmende Heterogenität der Softwarelandschaft, als Folge der Ablösung der Großrechnerverfahren, wurde von Seiten der Kommunen zunehmend der Wunsch geäußert, dass diese (damals verfahrensbezogenen) Anregungen überarbeitet bzw. unter der Maßgabe neu gefasst werden, dass sie **verfahrensunabhängig** angewandt werden können.

2 Trennung der Verantwortungsbereiche

Um die gesetzlich vorgegebene **Trennung von Verantwortungsbereichen** umzusetzen, müssen die einzelnen Verfahrensfunktionen (z.B. „Buchen“, „Zahlen“) den jeweils zuständigen Mitarbeitern bzw. Mitarbeiterinnen[2] über die programmtechnische Zugriffsberechtigungssteuerung zugewiesen werden.

Dabei sind neben den **Bestimmungen zum Datenschutz** und zur **Wahrung des Steuer- und Abgabengeheimnisses** (§ 30 AO) insbesondere die **haushalts- bzw. kassenrechtlichen Vorgaben zur Trennung von Verantwortungsbereichen** zu beachten:

- Trennung von Feststellung und Anordnung (§ 11 Abs. 3 Satz 2 GemKVO).
- Trennung von Anordnung und Vollzug (§ 7 Abs. 2 GemKVO).

---

[1] OSSY ist bzw. war als zentrales Berechtigungs- bzw. Steuerungsmodul (einschließlich einer Programmierumgebung) der Anwendung von „landeseinheitlichen“ Großrechnerverfahren (Dialogverfahren) vorgeschaltet.

[2] Im Folgenden wird wegen der besseren Lesbarkeit nur die männliche Form gewählt - selbstverständlich sind immer auch Mitarbeiterinnen gemeint.

- (Möglichst) Trennung von Buchführung und Zahlungsverkehr (§ 5 Abs. 2 GemKVO; „Sollvorschrift“).

- Ausreichende Trennung der Tätigkeitsbereiche der Verwaltung von Verfahren[1], der fachlichen Sachbearbeitung (Fachamt, Kämmerei) und der Erledigung der Kassenaufgaben (§ 35 Abs. 6 Satz 2 GemHVO).

Soweit Verantwortungsbereiche bei kleineren Kommunen aufgrund einer eingeschränkten Personaldecke nicht getrennt werden können und insoweit auch keine differenzierte Vergabe von Zugriffsberechtigungen in den Verfahren möglich ist, müssen über das **Interne Kontrollsystem** (IKS) andere Maßnahmen ergriffen werden (z.B. nachträgliche Kontrollen).

Es empfiehlt sich, bereits in der Phase zur Pilotierung bzw. Implementierung eines Verfahrens Überlegungen zur späteren Berechtigungsvergabe anzustellen, da die nachträgliche Ausgestaltung von Berechtigungen oft mit erheblichem Mehraufwand verbunden ist.

Die Zugriffsberechtigungen sollten nach Profilen[2] fachlich gebündelt werden. Die Berechtigungsvergabe erfolgt dann durch die Zuordnung des Profils (z.B. „Kasse“) zum Anwender (User) und nicht durch die direkte Zuweisung von Einzelberechtigungen (z.B. „Zahllauf ausführen“). Ergeben sich Änderungen im Verfahren, so müssen nur das jeweilige Profil und nicht die vergebenen Rechte aller in Frage kommenden Anwender angepasst werden.[3]

Berechtigungen sind immer **restriktiv** in Quantität („wer“) und Qualität („darf was“) zu vergeben. D.h. es sind nur so vielen Mitarbeitern wie unbedingt erforderlich Zugriffsberechtigungen zu erteilen. Gleichzeitig darf an diese Mitarbeiter auch nur der Umfang an Berechtigungen vergeben werden, den sie zwingend für die Aufgabenerledigung benötigen. Die Einhaltung dieser Grundsätze ist insbesondere durch ein strukturiertes Verfahren der technischen Ausgestaltung von Zugriffsmöglichkeiten (hierzu gehört z.B. auch die Dokumentation des Berechtigungssystems[4]) und des organisatorischen Ablaufs der Berechtigungsvergabe sicherzustellen.

Damit das IKS seine Wirkung voll entfalten kann, ist es nicht nur erforderlich, dass Regelungen (hier in der Form einer Dienstanweisung) bestehen, sondern auch, dass deren Einhaltung regelmäßig kontrolliert wird (vgl. GoBS Kapitel 4 d). Insbesondere sind systemseitige Auswertun-

---

1 Der „Verfahrensverwalter“ erbringt dv-spezifische Dienstleistungen für die Fachämter, die Kämmerei und die Kasse (z.B. als DV-Administrator, Power-User, Berechtigungsverwalter). Er hat aufgrund seiner Aufgabenstellung i. d. R. weitreichende Zugriffsrechte (z.B. auf Betriebs- und Datenbankebene oder als Berechtigungsverwalter im Verfahren; siehe hierzu auch Abschnitt 3).

2 Andere Bezeichnungen z.B. Rolle, Benutzergruppe, Berechtigungseinheit.

3 Selbstverständlich ist es zulässig, bzw. je nach Verfahren sogar notwendig, Einzelberechtigungen zu vergeben. Es ist allerdings sicherzustellen, dass die Berechtigungsverwaltung übersichtlich und für einen sachverständigen Dritten in angemessener Zeit nachvollziehbar bleibt.

4 Darunter wird in diesem Zusammenhang die Dokumentation der dv-technischen Berechtigung (z.B. Transaktionscode, Berechtigungsprofil) und der damit verbundenen Tätigkeit verstanden (z.B. Transaktion „4711“ = „Ausgaben Buchen“).

gen zur Nutzer-Berechtigungs-Zuordnung (ehemals „Benutzerspiegel“[1]) regelmäßig zu kontrollieren.

3 Aufgabenbereich Berechtigungsverwaltung

Zur „Verwaltung von Verfahren“ i.S.v. § 35 Abs. 6 Satz 2 GemHVO gehören auch die Tätigkeiten der **Berechtigungsverwaltung.** Demnach ist auf eine ausreichende Trennung dieses Tätigkeitsbereichs von dem der **fachlichen Sachbearbeitung** und dem der **Erledigung der Kassenaufgaben** zu achten. D.h. es ist anzustreben, dass der Berechtigungsverwalter nicht gleichzeitig im Rahmen seiner sonstigen Aufgaben Finanzvorgänge im Verfahren abwickelt. Hintergrund ist, dass verfahrenstechnisch i.d.R. die Notwendigkeit besteht, dass der Berechtigungsverwalter durch seine „besondere Tätigkeit“ bereits schon allumfassende Zugriffsrechte besitzen muss (dies ist oft bei „kleineren“ Verfahren der Fall) bzw. dass er sich selber (ohne weitere programmtechnische Freigabemechanismen) weitere Rechte zuteilen kann.

Oft besteht allerdings die Problematik, dass diese Abtrennung der Berechtigungsverwaltung aus organisatorischen bzw. personellen Gründen nicht bzw. nur sehr schwer umgesetzt werden kann. Dies trifft insbesondere dann zu, wenn die **Berechtigungsverwaltung** aufgrund der Komplexität des eingesetzten Verfahrens und der damit abgewickelten Sachverhalte einen **hohen fachlichen Sachverstand** voraussetzt. Dann kann es angebracht sein, dass die Aufgabe der Berechtigungsverwaltung durch einen **Mitarbeiter der Kämmerei** oder eines anderen Fachamts wahrgenommen wird, gerade weil dieser Mitarbeiter durch seine „Haupttätigkeiten“ den erforderlichen fachlichen Sachverstand für das Verfahren aufgebaut hat. In diesen Fällen sind im Rahmen des IKS **ergänzende Kontrollen** einzurichten (z.B. nachträgliche Stichproben oder flächendeckende Kontrollen; Installation eines „Vier-Augen-Prinzips“ bei Anlegen/Einrichten und Ändern von Berechtigungen - jeweils ausgerichtet auf die individuellen dv-technischen und organisatorischen Rahmenbedingungen bei der Kommune).

Generell ist zu vermeiden, dass die Aufgabe der Berechtigungsverwaltung **von Kassenmitarbeitern**[2] erledigt wird, da sonst die Mechanismen des IKS mit einer hinreichenden Trennung der Verantwortungsbereiche (siehe oben Abschnitt 2) grundsätzlich nicht mehr greifen können.

4 Empfehlungen zur Gestaltung einer Dienstanweisung

Die nachfolgenden **Empfehlungen zur Gestaltung einer Dienstanweisung (DA) zur Berechtigungsverwaltung** berücksichtigen die aus einer Vielzahl von Dienstanweisungen gewonne-

---

[1] Gängiger Begriff aus der „OSSY-Welt“. Die Unterlage muss die Benutzer und die ihnen jeweils zugewiesenen Berechtigungen in „verständlicher“ Form und mit dem notwendigen Detaillierungsgrad ausweisen.

[2] Selbstverständlich kann es sogar geboten sein, dass Mitarbeiter der Kasse (maßgeblich) in konzeptionelle Arbeiten im Bereich der Berechtigungsverwaltung fachlich mit eingebunden sind (z.B. beim Erstellen eines Berechtigungskonzepts).

nen Erfahrungen. Im Übrigen sind Anregungen des Gemeindetags, Landkreistags und des Städtetags sowie der kommunalen Praxis mit in die Empfehlungen eingeflossen.

Den Kommunen bleibt es unbenommen, auf den Erlass einer formalen DA zu verzichten und die Berechtigungsverwaltung anderweitig, etwa durch Einzelanweisungen schriftlich (vgl. § 28 Abs. 1 GemKVO), zu regeln. Allerdings hat sich die Form der DA in der Praxis bewährt, wobei oft der Fokus ausschließlich auf die Buchhaltung gelegt wird und die sonstigen Verfahrensbereiche (Veranlagung, Personalabrechnung usw.) nicht berücksichtigt werden. Die Empfehlungen sind deshalb bewusst so ausgestaltet, dass sie nicht nur für die zentrale DV-Buchführung (vgl. § 35 Abs. 5 GemHVO), sondern auch für nahezu alle sonstigen finanzwirksamen Verfahren bzw. DV-Systeme i.S.v. § 6 GemKVO **(sogen. Fachverfahren)** verwendet werden können.[1] Die Grundüberlegung ist, dass eine **(zentrale) DA** vorliegt und **verfahrensspezifische Besonderheiten** - soweit erforderlich - **ergänzend** in einer **Anlage** geregelt werden.[2]

In den Empfehlungen sind deshalb **Alternativen und Ergänzungen als Bausteine** formuliert, um eine möglichst universelle Anwendbarkeit zu erreichen (z.B. bei einer Abwicklung der Berechtigungsverwaltung über das Rechenzentrum). Die Kommune kann sich dadurch ihre DA anhand der Bausteine zusammen stellen. Dennoch konnten bei der Abfassung der Empfehlungen natürlich nur die gängigen Formen, Sachverhalte und Vorgehensweisen abgebildet werden. So kann es durchaus ebenso zweckmäßig sein, weitere nicht (unmittelbar) finanzwirksame Verfahren (z.B. Einwohnerwesen) ebenfalls in der DA mit zu regeln.

Generell gilt der Grundsatz: „Die Berechtigungsverwaltung muss hinreichend sicher, aber dennoch praktikabel und wirtschaftlich sein."

Dem Erlass der DA ist ein **Entscheidungsprozess** vorgeschaltet, in dem die Beteiligungsrechte des Personalrats und ggf. des örtlichen Datenschutzbeauftragten zu beachten sind.[3] Die Kommune muss z.B. abwägen, ob der Berechtigungsverwalter gleichzeitig Sachbearbeiter sein darf (vgl. oben Abschnitt 3) und ob bei einer „Mischtätigkeit" der Berechtigungsverwalter zur Erhöhung der Transparenz seine Sachbearbeitertätigkeiten zwingend über einen eigenen Sachbearbeiter-User abwickeln muss (ggf. mit zusätzlichen Kosten für dessen Bereitstellung). Der Bürgermeister legt mit der DA den Sicherheitsgrad formal fest. Danach richtet sich, welche ergänzenden Kontrollmaßnahmen sich anschließen müssen (vgl. GoBS Kapitel 4.4).

Ferner wird bewusst auf die Möglichkeit hingewiesen, dass sich mehrere Sachbearbeiter eine Zugriffskennung teilen können, wenn z.B. durch klar abgrenzbare Arbeitszeiten und eine Protokollierung der Dateneingaben ein **eindeutiger Personenbezug** hergestellt werden kann. Gene-

---

1 Die Finanzwirksamkeit eines Verfahrens setzt nicht voraus, dass eine maschinelle Schnittstelle zur zentralen DV-Buchführung eingerichtet ist.

2 Beispielsweise kann es zweckmäßig sein, für Programme, bei denen die finanzwirksamen Programmteile von untergeordneter Bedeutung sind (z.B. Hallenverwaltungsprogramme, Programme zur Friedhofsverwaltung), Vereinfachungen zuzulassen.

3 U.U. kann es angebracht sein, in die DA auch entsprechende Regelungen zur Einbindung der Personalvertretung bzw. des örtlichen Datenschutzbeauftragten mit aufzunehmen.

rell muss sich die Kommune bewusst sein, dass solche „Sonderregelungen“[1] überwacht werden müssen (z.B. bei Arbeitszeitänderungen) und damit einen höheren organisatorischen Aufwand verursachen. Zudem muss im Vorfeld geprüft werden, ob die Mehrfachnutzung von Zugriffskennungen überhaupt lizenzrechtlich zulässig ist.

[1] Im Kassenbereich mit z.B. zwei Halbtagskräften (vor- und nachmittags) sollte generell von einer „Teilung“ des Zugriffs abgesehen werden.

Dienstanweisung für die Berechtigungsverwaltung

1 Allgemeine Bestimmungen

1.1 Geltungsbereich, Grundsatz

Diese Dienstanweisung gilt für die Einrichtung und Pflege von Zugriffsberechtigungen (Berechtigungsverwaltung) der in der **Anlage** aufgeführten Verfahren.

Es dürfen nur die Berechtigungen an den Anwender (Sachbearbeiter) vergeben werden, die zur Aufgabenerledigung notwendig sind.

1.2 Zuständigkeit Berechtigungsverwalter; Sachbearbeiterfunktionen

Der Bürgermeister bestimmt den [die] Berechtigungsverwalter und dessen [deren] Stellvertreter.[1]

Für die Berechtigungsverwaltung ist <$_{Amt}$>[2] zuständig.

Baustein[3]: Für die Berechtigungsverwaltung sind die in der **Anlage** angegebenen Organisationseinheiten zuständig.

Baustein: Für die in der **Anlage** angegebenen Verfahren wird die Berechtigungsverwaltung vom Rechenzentrum durchgeführt.

Baustein: Kontaktstelle zum Rechenzentrum [Softwareanbieter] ist <$_{Amt}$>.[4]

Der Berechtigungsverwalter [Stellvertreter] darf gleichzeitig [keine] Sachbearbeiterfunktionen in den jeweiligen Verfahren wahrnehmen.[5]

Baustein: Werden vom Berechtigungsverwalter [Stellvertreter] selbst Sachbearbeiterfunktionen im Verfahren wahrgenommen, sind diese mit einem eigenen Sachbearbeiter-User abzuwickeln. Dessen Einrichtung erfolgt jeweils durch den Berechtigungsverwalter bzw. dessen Stellvertreter gegenseitig. Unter der Anmeldung als Berechtigungsverwalter [Stellvertreter] darf nur die Einrichtung und Pflege von Zugriffsberechtigungen vorgenommen werden.

---

1 Nachfolgend wird aus Vereinfachungsgründen grundsätzlich von einem Berechtigungsverwalter und einem Stellvertreter für alle Verfahren ausgegangen.

2 Amt steht hier stellvertretend für eine Organisationseinheit.

3 Baustein kann nachfolgend für eine Ergänzung oder eine Alternative stehen.

4 Es kann auch bei einer Inhouse-Verarbeitung angebracht sein, die Kontaktstelle zu einem (privaten) Softwareanbieter in der DA mit aufzunehmen, wenn der Anbieter z. B. Berechtigungsprofile erstellt und diese eingesetzt werden (vgl. Ziffer 2.1).

5 Zur Abtrennung der Berechtigungsverwaltung von der fachlichen Sachbearbeitung und der Erledigung der Kassenaufgaben siehe Vorbemerkungen Abschnitt 3.

1.3 Informationsaustausch

Die für die Berechtigungsverwaltung zuständige[n] Stelle[n] und die Fachämter informieren sich gegenseitig über Veränderungen bei den einzelnen Verfahren, bei Personalwechseln und Veränderungen der Aufgabengebiete der Sachbearbeiter.

2 Berechtigungsprofile

2.1 Bildung von Berechtigungsprofilen

Soweit das Verfahren die Bündelung von einzelnen Berechtigungen zu Berechtigungsprofilen[1] ermöglicht, sind diese aufgabenbezogen zu erstellen. Es sind sprechende Berechtigungsprofilbezeichnungen zu wählen. Die Profile sind ausreichend zu dokumentieren.

Baustein: Der Berechtigungsverwalter darf selbst keine Profile erstellen und pflegen. Dies erfolgt ausschließlich durch das Rechenzentrum [den Softwareanbieter].

Baustein: Das vom Rechenzentrum [Softwareanbieter] erstellte Berechtigungskonzept mit den zur Verfügung gestellten Profilen ist [grundsätzlich][2] unverändert einzusetzen.

2.2 Vorrang der Vergabe von Berechtigungsprofilen

Soweit Berechtigungsprofile eingerichtet sind, dürfen aus Gründen der Transparenz Einzelberechtigungen nur in begründeten Ausnahmefällen vergeben werden.

---

1 Andere Bezeichnungen z.B. Rolle, Benutzergruppe, Berechtigungseinheit.

2 Werden Änderungen vorgenommen, so sind diese zu dokumentieren (vgl. hierzu Ziffer 5.1 sowie Anlage zur DA, Spalte Bemerkungen).

3 Antragsverfahren

3.1 Berechtigung Berechtigungsverwalter/Stellvertreter

Dem Berechtigungsverwalter/Stellvertreter werden die Berechtigungen für [die Erstellung und Pflege der Profile,] das Anlegen der Sachbearbeiter als Benutzer sowie die Vergabe der Berechtigungen an die Sachbearbeiter zugeordnet.[1]

Berechtigungsverwalter und Stellvertreter nehmen gegenseitig die notwendigen Änderungen an den Berechtigungen des anderen vor. Soweit technisch machbar, ist die Möglichkeit zur Änderung der eigenen Berechtigungen verfahrensgestützt zu unterbinden.

Baustein: Die Berechtigungen des Berechtigungsverwalters/Stellvertreters werden durch das Rechenzentrum auf schriftlichen Antrag [E-Mail, Fax] eingerichtet.

3.2 Erstmalige Berechtigung Sachbearbeiter

Die Berechtigung des Sachbearbeiters (Zulassung) erfolgt nur auf schriftlichen Antrag [E-Mail, Fax].

Der Umfang der Zugriffsberechtigung hat sich unter Berücksichtigung der Bestimmungen zum Datenschutz, zur Wahrung des Steuer- und Abgabengeheimnisses und der haushalts- und kassenrechtlich vorgegebenen Trennung von Verantwortungsbereichen[2] am jeweiligen Aufgabengebiet auszurichten. Dabei sind der Aufbau und die organisatorischen Abläufe in der Verwaltung zu berücksichtigen. Insbesondere sind Vertretungen innerhalb der Organisationseinheiten zu beachten.

Der Antrag ist nach fachlicher Prüfung durch den Amtsleiter[3] [zu unterzeichnen und] dem Berechtigungsverwalter zuzuleiten (Trennung von fachlicher Entscheidung über die Berechtigungsvergabe und ihrer dv-technischen Umsetzung).

Der Berechtigungsverwalter ordnet dem Sachbearbeiter die erforderlichen technischen Berechtigungsobjekte zu. Bei der Vergabe von Berechtigungsprofilen schränkt er diese dem konkreten Aufgabenbereich des Sachbearbeiters entsprechend ein.[4]

Baustein: Der Antrag ist nach fachlicher Prüfung durch den Amtsleiter [zu unterzeichnen und] der Kontaktstelle zuzuleiten. Diese leitet den Antrag dem Rechenzentrum weiter.

---

1 Je nach Verfahren ist auch eine personelle Trennung zwischen dem Anlegen von Benutzern und der Vergabe der Berechtigungen an die (angelegten) Benutzer möglich. Wird von dieser Trennung Gebrauch gemacht, muss die DA entsprechend angepasst werden.

2 Siehe Vorbemerkungen Abschnitt 2.

3 Amtsleiter steht hier stellvertretend für einen Vorgesetzten.

4 Beschränkung des Zugriffs auf eine „Teilmenge“ der Daten (Buchungskreis, bestimmte Einnahmearten usw.). Teilweise wird auch der Begriff des „Ausprägens“ verwendet.

3.3 Passwort

Das Verfahren wird vor unbefugtem Zugriff durch ein Passwort geschützt.

Der Berechtigungsverwalter teilt dem Sachbearbeiter bei der erstmaligen Zulassung das von ihm vergebene vorläufige Passwort mit. Dieses ist vom Sachbearbeiter unverzüglich zu ändern.

Soweit verfahrenstechnisch vorgesehen, ist das Passwort so einzurichten, dass es spätestens nach drei Monaten seine Gültigkeit verliert und durch den Sachbearbeiter neu vergeben werden muss. Ansonsten hat der Sachbearbeiter dafür Sorge zu tragen, dass er sein Passwort regelmäßig ändert.

Das Verfahren ist so zu konfigurieren, dass spätestens nach fünfmaliger Falscheingabe der Zugang gesperrt wird.[1] Die Sperre ist nur durch den Berechtigungsverwalter aufhebbar.

Das Passwort muss folgende Voraussetzungen erfüllen.

- Mindestlänge sechs Zeichen;
- Kombination aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen;
- keine Trivialpasswörter.[2]

Soweit verfahrensseitig diese Mindestvoraussetzungen unterstützt werden, sind diese Verfahrensfunktionen zu aktivieren. Ansonsten hat der Sachbearbeiter die Vorgaben bei der Passwortwahl zu beachten.

Der Sachbearbeiter hat sein Passwort geheim zu halten. Hat der Sachbearbeiter Grund zu der Annahme, dass sein Passwort bekannt geworden ist, muss er es unverzüglich ändern.

Die gemeinsame Nutzung eines Login- Namens mit Passwort durch mehrere Sachbearbeiter ist nicht gestattet.

Baustein: Die gemeinsame Nutzung eines Login- Namens mit Passwort durch mehrere Sachbearbeiter ist ausnahmsweise dann gestattet, wenn der jeweils zugreifende Sachbearbeiter dennoch eindeutig bestimmbar ist. Die Gründe sowie die technischen und organisatorischen Rahmenbedingungen der gemeinsamen Nutzung (z.B. systemtechnische Protokollierung der Zugriffe, eindeutig abgrenzbare Arbeitszeiten) sind vom Amtsleiter auf dem Zulassungsantrag darzulegen.

---

1 Es wird hier unterstellt, dass jedes finanzwirksame Verfahren diese Funktionalität beinhaltet.

2 Vgl. auch Maßnahmenkatalog M 2.11 (Regelung des Passwortgebrauchs) des Bundesamts für Sicherheit in der Informationstechnik (BSI).

4 Pflege der Berechtigungen

4.1 Änderung von Berechtigungsprofilen

Bei Änderungen an bestehenden Berechtigungsprofilen gilt Ziffer 2.1 entsprechend. Soweit sich Auswirkungen auf den Berechtigungsumfang der Sachbearbeiter ergeben können, werden die zuständigen Amtsleiter informiert. Diese überprüfen die Auswirkungen auf die Berechtigungen ihrer Mitarbeiter. Im Übrigen gilt das weitere Verfahren nach Ziffer 3.2.

Baustein: Werden die Berechtigungsprofile vom Rechenzentrum [Softwareanbieter] gepflegt, so sind die zuständigen Amtsleiter von der Kontaktstelle über die Änderungen zu informieren.

4.2 Personalwechsel, Aufgabenänderung

Bei Personalwechseln oder Änderungen im Aufgabenumfang des Sachbearbeiters gilt das Verfahren nach Ziffer 3.2 entsprechend. Beim Ausscheiden eines Mitarbeiters sind diesem die Berechtigungen unverzüglich zu entziehen.

Beim Wechsel des Berechtigungsverwalters übergibt dieser seine bisherigen Berechtigungen seinem Nachfolger. Dieser entzieht dem bisherigen Berechtigungsverwalter sodann die Zugriffsmöglichkeit durch Änderung des Passworts.

Baustein: Bei Wechsel des Berechtigungsverwalters wird das Rechenzentrum schriftlich informiert. Dieses veranlasst die Änderungen.

5 Dokumentation, Protokollierung, Auswertungen

5.1 Dokumentation des Berechtigungssystems

Der Aufbau des Berechtigungssystems ist zu dokumentieren. Dabei ist insbesondere zu beschreiben

- welche dv-technischen (Einzel-)Berechtigungen das Verfahren bietet und welche auszuführenden Tätigkeiten (Aufgaben) damit verbunden sind;
- ob Berechtigungsprofile eingerichtet sind und welche (Einzel-)Berechtigungen in welchen Profilen gebündelt werden (siehe auch Ziffer 2.1);
- ob und ggf. welche Konflikte bei der Vergabe von Zugriffsrechten (z. B. aus technischen oder organisatorischen Gründen) aufgetreten sind.

Baustein: Soweit das Berechtigungskonzept des Rechenzentrums [des Softwareanbieters] eingesetzt wird, ist von der Kontaktstelle darauf hinzuwirken, dass die jeweils aktuellen Dokumentationsunterlagen verfügbar sind.

5.2 Protokollierung

Die Vergabe der Berechtigungen muss [grundsätzlich] durch eine systemseitige Protokollierung dokumentiert sein.

Baustein: Soweit keine systemseitige Protokollierung der Berechtigungsvergabe erfolgt, sind vom Berechtigungsverwalter sonstige geeignete historisch lückenlos nachvollziehbare Nachweise (z.B. Bildschirmausdrucke) anzufertigen.

5.3 Auswertungen

Durch Auswertungen muss jederzeit feststellbar sein, welche Berechtigungen (Profile) dem einzelnen Sachbearbeiter zugeordnet sind („Nutzer-Berechtigungs-Zuordnung“).

Die Vergabe der Berechtigungen ist vom Berechtigungsverwalter regelmäßig (mindestens jährlich) auszuwerten und zu kontrollieren.

Baustein: Mindestens einmal jährlich wird die Auswertung „Nutzer-Berechtigungs-Zuordnung“ den zuständigen Amtsleitern zur Kontrolle zugeleitet. Diese bestätigen deren Richtigkeit bzw. veranlassen bei notwendigen Änderungen das weitere Verfahren nach Ziffer 3.2.

6 Aufbewahrung von Unterlagen

Die Dokumentation des Aufbaus des Berechtigungssystems (Ziffer 5.1) ist dauernd aufzubewahren.

Die Systemprotokolle [bzw. die sonstigen Nachweise] zur Berechtigungsvergabe (Ziffer 5.2) sowie die Auswertungen nach Ziffer 5.3 sind mindestens bis zum Abschluss der überörtlichen Prüfung aufzubewahren.

Der Antrag auf erstmalige Zulassung sowie der Antrag zur Berechtigungsänderung sind nach Ausscheiden des Mitarbeiters ebenfalls mindestens bis zum Abschluss der überörtlichen Prüfung aufzubewahren.

Baustein: Der Antrag auf erstmalige Zulassung sowie der Antrag zur Berechtigungsänderung sind dauernd aufzubewahren.

7 In-Kraft-Treten

Diese Dienstanweisung tritt zum …… in Kraft.

Ort, Datum

Unterschrift des Bürgermeisters

Anlage zur Dienstanweisung für die Berechtigungsverwaltung (beispielhaft)

Verfahrensbezeichnung; Finanzbereich	**Zuständigkeit Berechtigungsverwaltung (DA Ziffer 1.2)**	**Berechtigungsverwalter mit Sachbearbeiterfunktion (DA Ziffer 1.2)**	**Verwendung Berechtigungsprofile (DA Ziffer 2.1)**	**Verwendung Konzept des RZ / Softwareanbieters (DA Ziffer 2.1)**	**Maschinelle Protokollierung Berechtigungsvergabe (DA Ziffer 5.2)**	**Bemerkungen**
Verfahren A, Finanzbuchhaltung; einschl. Veranlagung	Rechenzentrum (RZ)	Entfällt	Ja	Ja (unverändert)	Ja	
Verfahren B, Personalwesen	IuK-Abteilung	Nein	Ja	Ja (mit Änderungen)	Ja	Änderungen zum Konzept sind manuell zu dokumentieren.
Verfahren C, Friedhofwesen	Friedhofsamt	Ja	Nein (Funktionalität fehlt)	Nein	Nein	Es sind folgende organisatorische Kontrollen einzurichten: <$_{\text{Maßnahmen}}$>.