ZKZ 63004

JUSTIZBLATT

RHEINLAND-PFALZ

AMTSBLATT DES MINISTERIUMS DER JUSTIZ

78. Jahrgang **Mainz, den 7. Juni 2024** **Nummer 5**

INHALT

Verwaltungsvorschriften und Rundschreiben

Dienstanweisung zur Authentisierung gegenüber IT-Systemen für den Geschäftsbereich des Ministeriums der Justiz

Rundschreiben des Ministeriums der Justiz vom 8. Mai 2024 (DV5100.1-0026)

1. Allgemeines

1.1. Einleitung

Der Zugang zu schützenswerten Ressourcen einer Institution muss auf berechtigte Benutzer und berechtigte IT-Komponenten beschränkt werden können. Hierzu müssen Benutzer und IT-Komponenten zweifelsfrei identifiziert und authentisiert werden. Der Begriff der Authentisierung bezeichnet in diesem Zusammenhang das Nachweisen einer Identität gegenüber einem IT-System.

Die Verwaltung der dafür notwendigen Informationen wird als Identitätsmanagement bezeichnet. Ein Teilbereich hiervon bildet das Berechtigungsmanagement. Dieses regelt, ob und wie Benutzer oder IT-Komponenten auf Informationen oder Dienste zugreifen dürfen und beschreibt die Prozesse, die für Zuweisung, Entzug und Kontrolle von Zugriffsrechten erforderlich sind.

1.2 Regelungsgegenstand und Geltungsbereich

Die vorliegende Dienstanweisung dient der Umsetzung der Anforderungen des IT-Grundschutz Bausteins ORP.4 (Identitäts- und Berechtigungsmanagement) des IT-Grundschutz-Kompendiums des Bundesamts für Sicherheit in der Informationstechnik. Sie konkretisiert die Umsetzung der Anforderungen und Mindeststandards der durch den IT-Beauftragten der Landesregierung für die Landesverwaltung erlassenen Richtlinie zur Authentisierung für das Ministerium der Justiz sowie für dessen nachgeordnete Geschäftsbereiche.

2. Regelungen für Bedienstete

2.1 Pflicht zur Authentisierung

Nur autorisierte Personen dürfen im Rahmen ihrer jeweiligen Zuständigkeit Zugriff auf bestimmte Informationen oder Systeme haben. Die Authentisierung erfolgt grundsätzlich mittels Benutzernamen und Passwörtern, sofern auf Grund besonderer Anforderungen keine weitergehenden Mechanismen eingesetzt werden.

2.2 Benutzerkennung

Bedienstete müssen grundsätzlich einen eindeutigen Benutzernamen und ein Passwort eingeben, um sich anzumelden. Sie dürfen sich ausschließlich mit der ihnen zugeteilten Benutzerkennung authentisieren. Die gemeinsame Verwendung von Benutzerkennungen ist nur nach Genehmigung der jeweiligen Behördenleitung zulässig. Ausnahmen sind nur bei dienstlichen Bedürfnissen in begründeten Fällen gestattet. Diese müssen von der systemverwaltenden Stelle

dokumentiert werden. Können in Ausnahmefällen nur gemeinsame Kennungen genutzt werden, sollten die Zugriffe protokolliert und regelmäßig kontrolliert werden.

Privilegierte Benutzerkennungen (z. B. Admin-Accounts) dürfen nur zu Zwecken der System- oder Anwendungsverwaltung verwendet werden und sind nur für den Zeitraum des erhöhten Rechtebedarfs zu verwenden.

Ist der PC mit Schadsoftware infiziert oder durch einen Angriff kompromittiert, sorgt diese Maßnahme dafür, dass die Schadsoftware (oder die Angreifenden) im Regelfall nur über gewöhnliche Benutzerberechtigungen verfügt und die Auswirkungen von möglichen Schadensereignissen minimiert werden können.

2.3 Umgang mit Authentisierungsinformationen

Beim Umgang mit Authentisierungsinformationen sind die nachfolgenden Regeln zu beachten:

- Passwörter müssen geheim gehalten werden und dürfen nur den Nutzerinnen und Nutzern persönlich bekannt sein. Im Vertretungsfall müssen entsprechende Freigaben und Berechtigungen erteilt werden.
- Ein Passwort darf allenfalls für die Hinterlegung im Notfall handschriftlich fixiert werden. Dies darf nur in Ausnahmefällen bei Anwendungen ohne zentrale Benutzerverwaltung geschehen.
- Bei der physischen Hinterlegung muss das Passwort in einem versiegelten Umschlag sicher und nur für einen engen Personenkreis zugänglich aufbewahrt werden.
- Es sollte ein sicherer Passwortmanager verwendet werden, die Nutzung des justizweit bereitgestellten Passwort-Managers (aktuell „KeePass 2“) wird empfohlen. Dieser kann als Standardsoftware für jede Nutzerin und jeden Nutzer installiert und verfügbar gemacht werden.
- Passwörter dürfen nicht innerhalb von Webbrowsern oder auf programmierbaren Funktionstasten von Tastaturen bzw. Mäusen gespeichert werden.
- Ein Passwort muss gewechselt werden, wenn es unautorisierten Personen bekannt geworden ist oder der Verdacht dazu besteht.
- Passwörter dürfen nicht mehrfach verwendet werden. Für jedes IT-System bzw. jede Anwendung muss ein eigenständiges Passwort verwendet werden. Eine mögliche Verwendung von Single-Sign-On (SSO) Verfahren bleibt hiervon unberührt.
- Wenn technisch möglich, muss die Wiederverwendung der letzten zwölf Passwörter unterbunden werden.
- Passwörter dürfen nur verdeckt eingegeben werden.
- Voreingestellte Passwörter und Kennungen müssen durch individuelle Passwörter und, wenn möglich, Kennungen ersetzt werden.

2.4 Regeln für sichere Passwörter

Es sind ausschließlich sichere Passwörter zu verwenden. Hinsichtlich der Mindestlänge, Komplexität und Änderungsintervalle der Passwörter gelten dabei die Vorgaben des Abschnitts 3.3.5.

Wenn bei IT-Systemen oder Anwendungen das Passwort durch Nutzerinnen und Nutzer nicht eigenständig vergeben oder geändert werden kann, sind die nachfolgenden Regelungen zu beachten:

- Sofern technisch möglich, müssen Passwörter verwendet werden, die den Regelungen zur Passwortqualität (vgl. Abschnitt 3.3.5) entsprechen.
- Passwörter dürfen keine Informationen aus dem persönlichen oder beruflichen Umfeld der Nutzerinnen und Nutzer enthalten wie z. B. Namen, Kfz-Kennzeichen oder das Geburtsdatum. Passwörter oder Passphrasen müssen vollständig und nicht nur in Teilen geändert werden.

3. Regelung für Administrierende und Fachverantwortliche

3.1 Allgemeine Regeln

3.1.1 Pflicht zur Authentisierung

Alle IT-Systeme und Anwendungen sind so zu konfigurieren, dass Nutzerinnen und Nutzer erst nach erfolgreicher Authentisierung Zugang zu dem System oder der Anwendung erhalten. Ausgenommen sind die Frontends von Systemen, die öffentliche Informationen verteilen, wie z. B. öffentlich erreichbare Webseiten. Die Backends solcher Systeme sind hingegen durch Authentisierungsmaßnahmen zu schützen.

3.1.2 Benutzerkennungen

Jede Benutzerkennung muss jeweils einer natürlichen Person zugeordnet werden können. Benutzerkennungen, die nicht für natürliche Personen, sondern für die Ausführung von Anwendungen oder Diensten benötigt werden („Systemkennungen“), müssen einem klaren Verantwortungsbereich unterliegen. Hierzu muss eine Dokumentation erfolgen, aus welcher die Information entnommen werden kann, welche Person die Verantwortung für eine Systemkennung übernimmt. Auch das Einverständnis der Person hierzu muss der Dokumentation beigefügt sein.

Benutzerkennungen, die von mehreren Nutzerinnen und Nutzern gemeinsam verwendet werden, sind nur in Ausnahmefällen zulässig. Es ist zu dokumentieren, wer die Benutzerkennungen nutzt und die Protokolle sind regelmäßig von den Systemverantwortlichen zu prüfen.

Privilegierte Benutzerkennungen (z. B. Admin-Accounts) dürfen nur zu Zwecken der System- oder Anwendungsverwaltung verwendet werden.

3.1.3 Zugriffs- und Zugangssteuerung

Administrative Aufgaben und die hierfür erforderlichen Rollen und Funktionen müssen so strukturiert sein, dass unvereinbare Aufgaben wie operative und kontrollierende Funktionen auf verschiedene Personen verteilt werden. Diese Funktionstrennung muss festgelegt und dokumentiert sein. Auch Vertreterinnen und Vertreter müssen der Funktionstrennung unterliegen. Für Administratorinnen und Administratoren gelten die folgenden Aufgaben als unvereinbar:

- Datenschutzbeauftragter
- Informationssicherheitsbeauftragter
- „Weitere unvereinbare Positionen“

Die Kontrolle der Funktionstrennung obliegt der Geschäftsleitung der jeweiligen Behörde.

Die Erteilung von Zugängen und Berechtigungen zu Systemen oder Anwendungen sollte grundsätzlich rollenbasiert erfolgen.

3.2 Verwaltung der Zugriffs- und Zugangsrechte

Die Vergabe, der Entzug sowie jegliche Änderung von Zugriffs- und Zugangsrechten sind zu dokumentieren, aktuell zu halten und in geeigneter Weise zu sichern. Die Dokumentation ist vor unberechtigtem Zugriff zu schützen. Kommen zur Zugriffs- und Zugangskontrolle Token oder Chipkarten zum Einsatz, so müssen auch deren Vergabe und der Entzug dokumentiert werden. Dieser Prozess sollte durch eine geeignete Software unterstützt und automatisiert werden.

3.2.1 Vergabe von Benutzerkennungen und Berechtigungen

- Berechtigungen müssen nach dem Minimalprinzip (Need-to-know) vergeben werden.
- Bei personellen Veränderungen müssen die Benutzerkennungen und Berechtigungen innerhalb von höchstens einer Arbeitswoche angepasst werden.
- Grundsätzlich richtet sich die Rechtevergabe nach der Zuordnung der Nutzerinnen und Nutzer zu einer Organisationseinheit und der Funktion.
- Der IT-Betrieb erstellt Benutzerkennungen und erteilt Berechtigungen auf Antrag der zuständigen Organisationseinheiten (i.d.R. Personalreferat oder Geschäftsleitung).
- Abweichungen von der Benutzerzuordnung zu einer Organisationseinheit erfolgen nur in Ausnahmefällen auf Antrag der zuständigen Organisationseinheiten (i.d.R. Personalreferat oder Geschäftsleitung).
- Für zeitlich begrenzte Bedienstete (z. B. Praktikanteninnen und Praktikanten, Anwärterinnen und Anwärter) können abteilungs- oder referatsbezogene Sonderkonten eingerichtet werden. Die betroffenen Benutzerkennungen müssen, wenn möglich, mit einer zeitlichen Befristung und anschließender Deaktivierung versehen werden.
- Zugriffsrechte für einzelne Fachverfahren werden nur auf schriftliche (möglichst elektronische) Anforderung der für die jeweiligen Fachverfahren zuständigen Abteilungen/Referate vergeben.
- Externe Bedienstete, die temporär Zugriff auf ein IT-System benötigen, erhalten nur die zur Aufgabenwahrnehmung erforderlichen Rechte. Hierzu sind Sondernutzerkennungen zu verwenden.
- Zugriffsberechtigungen auf Systemverzeichnisse und -dateien sollen beschränkt sein.
- Alle Berechtigungen müssen über separate administrative Rollen eingerichtet werden.

3.2.2 Entzug von Benutzerkennungen und Berechtigungen

Benutzerkennungen von ausgeschiedenen Bediensteten müssen durch den IT-Betrieb umgehend gesperrt und innerhalb einer definierten Zeit vollständig gelöscht werden. Dieser ist hierzu durch die zuständigen Organisationseinheiten (i.d.R. Personalreferat oder Geschäftsleitung) zeitnah zu informieren.

Bei Bedarf müssen Zugangsberechtigungen von berechtigten Personen vorübergehend gesperrt werden (z. B. bei längeren Abwesenheiten). Dies gilt auch bei Personen mit privilegierten Berechtigungen.

Kompromittierte Zugangsmittel (z. B. Chipkarten, Schlüssel) müssen umgehend erneuert werden. Der weitergehende Gebrauch ist unzulässig.

3.2.3 Ersteinrichtung und Entsperrung von Benutzerkennungen

IT-Systeme und Anwendungen, die eine passwortbasierte Authentisierung verwenden, sollen so konfiguriert werden, dass sich neu berechtigte Nutzerinnen und Nutzer mit einem Initialpasswort anmelden können, dessen Änderung sofort nach der ersten Anmeldung erzwungen wird. Ist das nicht möglich, muss die Nutzerin oder der Nutzer bei der Passwortübergabe in Textform (z. B. per E-Mail) angewiesen werden, das Initialpasswort unverzüglich zu ändern.

Alle Systeme und Anwendungen müssen so konfiguriert werden, dass der IT-Betrieb bei der Neuanlage oder Entsperrung von Benutzerkonten nicht mit geheimen Authentisierungsinformationen, wie z. B. Passwörtern, in Berührung kommt. Alternativ müssen sie so konfiguriert werden, dass Nutzerinnen und Nutzer ihre eigenen gesperrten Benutzerkonten selbst zurücksetzen oder ändern können bzw. ein Initialpasswort vergeben wird, das die Nutzerin oder der Nutzer unverzüglich ändern muss.

Bei der Vergabe eines Initialpassworts oder bei der Rücksetzung eines Passworts durch den IT-Betrieb, muss vor der Übermittlung der Authentisierungsdaten sichergestellt werden, dass die Identität der Nutzerin oder des Nutzers verifiziert wurde. Bestehen Zweifel an der Identität der Nutzerin oder des Nutzers soll von der Vergabe eines Initialpassworts oder der Rücksetzung eines Passworts abgesehen werden.

3.2.4 Überprüfung der Berechtigungen und Benutzerkennungen

Erteilte Berechtigungen und eingerichtete Benutzerkennungen müssen stets aktuell gehalten werden. Personalveränderungen müssen zeitgerecht eingearbeitet und bei Bedarf überprüft werden.

- Nicht mehr benötigte Konten müssen deaktiviert werden und nach einer Wartezeit von maximal 30 Tagen gelöscht werden.
- Berechtigungen müssen nach dem Need-to-know-Prinzip angepasst werden.

3.3 Verfahren

3.3.1 Grundlegende Anforderungen

IT-Systeme und Anwendungen müssen nach Empfehlung des Informationssicherheitsbeauftragten und der Zustimmung der Behördenleitung so konfiguriert sein, dass die Benutzeranmeldung folgenden Kriterien genügt:

- Es sollen keine System- und Anwendungsinformationen bei der Anmeldung angezeigt werden, bis der Authentifizierungsprozess abgeschlossen ist.
- Während der Anmeldung dürfen keine Hilfetexte angezeigt werden, die nähere Informationen über das System oder die Anwendung liefern.
- Bei der Anmeldung soll die Benutzerkennung nicht vorausgefüllt sein.
- Die Anmeldedaten dürfen erst nach vollständiger Eingabe aller Bestandteile geprüft werden. Bei einer negativen Prüfung darf das System oder die Anwendung keinen Hinweis darauf geben, welcher Teil der Anmeldedaten fehlerhaft war.
- Die Systeme oder Anwendungen müssen geeignete Maßnahmen zum Schutz vor Brute-Force-Angriffe implementieren (z. B.: Sperrung nach mehrmaliger Falscheingabe).

- Die Systeme oder Anwendungen müssen soweit technisch möglich erfolglose und erfolgreiche Anmeldeversuche protokollieren.
- Nach erfolgreicher Anmeldung sollen Datum und Uhrzeit der letzten erfolgreichen Anmeldung angezeigt werden sowie Details zu allen erfolglosen Anmeldeversuchen, die in der Zwischenzeit stattgefunden haben.
- Das eingegebene Passwort darf nicht im Klartext angezeigt werden und es darf nicht im Klartext über das Netzwerk übertragen werden.
- Inaktive Sitzungen müssen nach einer angemessenen Zeitspanne von maximal 30 Minuten beendet oder gesperrt werden (Abmeldung oder Bildschirmsperre).

Können o. a. notwendige („muss“) Forderungen nicht erfüllt werden, sind diese zu begründen und zu dokumentieren.[1]

3.3.2 Kryptografische Anforderungen an die Speicherung und Übertragung von Authentisierungsinformationen

Systeme und Anwendungen sollen so konfiguriert werden, dass sie durch kryptographische Authentisierung nach dem aktuellen Stand der Technik geschützt werden. Das betrifft z. B. Passwörter, PINs, private Schlüssel für Zertifikate und vergleichbare Informationen. Maßgeblich hierfür sind die technischen Richtlinien des BSI zu kryptographischen Verfahren.

3.3.3 Protokollierung

Es sollen alle Ereignisse, welche die Nutzung und Verwaltung von Zugangsberechtigungen betreffen, unter Beachtung der gesetzlichen Bestimmungen und Wahrung der richterlichen Unabhängigkeit, aufgezeichnet und archiviert werden. Dazu zählen die Erteilung, die Änderung und der Entzug von Zugangsberechtigungen, die An- und Abmeldung von Nutzerinnen und Nutzern an Systemen oder Anwendungen sowie erfolglose Anmeldeversuche. Näheres ist in einer eigenen Richtlinie für die Protokollierung zu regeln.

3.3.4 Zentrales Verzeichnis

Alle unter einer Benutzerkennung gewährten Rechte sollen in einem zentralen Verzeichnis (z. B. Active Directory) verwaltet werden. Wenn das für bestimmte Systeme oder Anwendungen nicht möglich ist bzw. es dort keine Möglichkeit gibt, sich einen system- bzw. anwendungsweiten Überblick über die vergebenen Berechtigungen zu verschaffen, sind die System-, Anwendungs- oder Verfahrensverantwortlichen für eine stets aktuelle Dokumentation der autorisierten Benutzerkennungen und deren Berechtigungen verantwortlich.

[1] Als begründete Ausnahme kann bspw. die IT-Nutzung im Sitzungsbetrieb gelten.

3.3.5 Regelungen zur Passwortqualität

IT-Systeme oder Anwendungen, die Passwörter zur Authentisierung verwenden, müssen so konfiguriert werden, dass sichere Passwörter verwendet werden, die dem Stand der Technik entsprechen.

Folgende Kriterien müssen mindestens beachtet werden:

Änderungsintervalle
Auf regelmäßige Intervalle für den Passwortwechsel soll verzichtet werden. In diesem Fall müssen technische Maßnahmen ergriffen werden, die eine mögliche Kompromittierung des Passwortes erkennen. Wenn keine zusätzlichen technischen Maßnahmen zur Erkennung einer Kompromittierung möglich sind, muss ein Passwortwechsel spätestens nach drei Monaten erzwungen werden. System- und Servicekonten können hiervon ausgenommen werden. Alternativ kann für System- und Dienstekonten durch systemimmanente Tools (z. B. Managed ServiceAccounts) eine automatisierte und sichere Kennwortänderung konfiguriert werden.

- Die Sperrung der Benutzerkennung muss spätestens nach 5-maliger Fehleingabe erfolgen.
- Dauer der Kontosperrung: mind. 30 Minuten oder bis zur Aufhebung durch den IT-Betrieb.
- Passwortchronik: mind. 12 gespeicherte Passwörter.
- Passwortlänge und Komplexität für Benutzerkonten

Bei einem guten Passwort müssen die Länge und die Anzahl der verwendeten Zeichenarten wie Großbuchstaben, Kleinbuchstaben, Sonderzeichen und Zahlen in sinnvoller Kombination und in Abhängigkeit des verwendeten Verfahrens gewählt werden.

Die technische Umsetzung der vorgenannten Regelungen hängt von verschiedenen Faktoren ab, einschließlich der Art der Anwendung, in der das Passwort verwendet wird, sowie den Anforderungen an die Sicherheit, die von der Anwendung gestellt werden.

Ein hinreichend sicheres Passwort ist mindestens zwölf Zeichen lang, beinhaltet Klein- und Großbuchstaben, Zahlen und Sonderzeichen und lässt sich nicht aus personenbezogenen Angaben wie Namen, Geburtstag oder Wohnort herleiten. Auf Standardkombinationen wie „12345", „admin" oder der Name des Netzwerks sollte unbedingt verzichtet werden. Es sollten in einem Passwort auch keine Informationen verwendet werden, die der Benutzer über sich selbst in sozialen Netzwerken veröffentlicht hat, wie z.B: Name eines Haustiers, Name der Lieblingsband, eines Films oder eines Buches.

3.3.6 Zwei-Faktor-Authentisierung (2FA)

Bei privilegierten Konten (Benutzerkennungen mit weitreichenden Berechtigungen) ist eine Zwei-Faktor-Authentisierung zu nutzen. Sofern dies nicht erfolgt, ist dies zu dokumentieren.

Zwei-Faktor-Authentisierung soll immer dann verwendet werden, wenn Nutzerinnen oder Nutzer von außerhalb der Behördennetze auf dienstliche Systeme oder Anwendungen zugreifen. Gleiches gilt für die Verwendung von IT-Systemen oder Anwendungen mit erhöhtem Schutzbedarf.

4. Beachtung bestehender Vorschriften

Die in diesem Zusammenhang maßgeblichen Bestimmungen in ihrer jeweils geltenden Fassung sind zu beachten.

5. Inkrafttreten, Überprüfung

Diese Dienstanweisung tritt mit Veröffentlichung im Justizblatt in Kraft.
Diese Dienstanweisung wird bei Anpassung bzw. Aktualisierung der zu Grunde liegenden Richtlinie der Landesverwaltung überprüft.

314

Geschäftsführung der Gerichtsvollzieherinnen und Gerichtsvollzieher

Verwaltungsvorschrift des Ministeriums der Justiz vom 14. Mai 2024 (2344-0012) *)

1 Die Verwaltungsvorschrift des Ministeriums der Justiz vom 1. August 2012 (2344-3-48) - JBl. S. 360; 2022 S. 122 -, zuletzt geändert durch Verwaltungsvorschrift vom 19. März 2024 (2344-0012) - JBl. S. 75 -, wird wie folgt geändert:

1.1 In Nummer 3.1 Satz 1 wird der Kammerzusatz „(vgl. Nr. 3 und 5 RdSchr. JM vom 25. Mai 1988 -2344-1-24/88-, JBl. S. 117)“ durch den Klammerzusatz „(vgl. Nr. 3 RdSchr. JM vom 26. Juli 2023 -2344-0001-, JBl. S. 86, geändert durch RdSchr. JM vom 22. Februar 2024 -2344-0001-, JBl. S. 73)“ ersetzt.

1.2 In Nummer 4 Satz 2 wird nach der Angabe „GV 1 bis GV 8“ die Angabe „und GV 11“ eingefügt.

1.3 Anlage 2 Vordruck GV 11 erhält die aus der Anlage zu dieser Verwaltungsvorschrift ersichtliche Fassung.

2 Die Verwaltungsvorschrift tritt mit Ausnahme der Nummer 1.1 mit Wirkung vom 1. Januar 2024 in Kraft. Nummer 1.1 tritt am Tage nach der Veröffentlichung dieser Verwaltungsvorschrift in Kraft.

*) Die Änderungen werden in die konsolidierte Fassung im Landesrecht Rheinland-Pfalz eingearbeitet

Anlage
(zu Nummer 1.3)

Oberlandesgerichtsbezirk
Landgerichtsbezirk
Amtsgericht

Übersicht über die Diensteinnahmen
der Vollstreckungsbeamten (Gerichtsvollzieher und Vollziehungsbeamten der Justiz) für das Jahr

Vordruck GV 11
Stand 01.01.2024

Lfd. Nr.	AG: Name des GV (Vollzb) / LG: Bezeichnung des AG / OLG: LG-Bezirk	Zahl der ganzjährig im Vollstreckungsdienst eingesetzten Beamten	Zeitweise im Vollstreckungsdienst eingesetzte Beamte - Zahl der Kalendertage	Eingegangen sind: Schuldbeträge und andere Parteigelder	Gebühren	abzuliefernde Kleinbeträge	Dokumentenpauschale	Wegegelder / Reisekosten Nr. 711 KV-GvKostG Nr. 712 KV-GVKostG	Umsatzsteuer Nr. 717 KV-GvKostG	Pauschale nach Nr. 716 KV-GvKostG	Auslagen nach Nr. 701 bis 710, 713 bis 715 KV-GvKostG	Aus der Landeskasse gewährt sind: 55% der vereinnahmten Gebühren bis 50.000 Euro 45% von dem Mehrbetrag über 50.000 Euro	55% der erhobenen Dokumentenpauschale bis 50.000 Euro 45% von dem Mehrbetrag über 50.000 Euro	Wenn Prozesskostenhilfe bewilligt ist und bei Aufträgen des Gerichts: Wegegelder	sonstige Auslagen	Reisekostenzuschüsse	Summe der Spalten 11 bis 15
				EUR / Ct	EUR / Ct	EUR / Ct	EUR / Ct	EUR / Ct	EUR / Ct	EUR / Ct	EUR / Ct	EUR / Ct	EUR / Ct	EUR / Ct	EUR / Ct	EUR / Ct	EUR / Ct
1	2	3	4	5	6	7	8	9a	9b	10a	10b	11	12	13	14	15	16
																	0,00
																	0,00
																	0,00
																	0,00
																	0,00
																	0,00
																	0,00
																	0,00
																	0,00
																	0,00
																	0,00
																	0,00
																	0,00
																	0,00
																	0,00
																	0,00
																	0,00
																	0,00
																	0,00
																	0,00
																	0,00
																	0,00
																	0,00
	Summe:	0	0	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00

Vermerke (Fußnoten)

Anleitung

1 Die Eintragungen in der Spalte 2 des Abschnitts A (Gerichtsvollzieher) und des Abschnitts B (Vollziehungsbeamte der Justiz) sind in der Spalte 1 je für sich mit fortlaufenden Nummern zu versehen.

2 In der Spalte 2 sind die Vollstreckungsbeamten innerhalb eines jeden Abschnitts in der Buchstabenfolge ihrer Namen, die planmäßigen vor den nichtplanmäßigen, aufzuführen. Dabei ist zwischen den einzelnen Namen für die im Laufe des Rechnungsjahres in den Spalten 5 bis 16 vorzunehmenden Eintragungen genügend Raum freizulassen.

3 In den Spalten 3 und 4 sind die tatsächlich eingesetzten planmäßigen Gerichtsvollzieher und Hilfsbeamten des Gerichtsvollzieherdienstes (mit Vollstreckungsaufgaben betraute Beamte des gehobenen und des mittleren Justizdienstes) anzugeben. Hierzu zählen auch Beamte, die nur als Versteigerer tätig oder nur mit der Einbringung von Pfandgegenständen befasst sind.
Beamte, die zusammenhängend mehr als 21 Kalendertage abwesend sind (z.B. wegen Krankheit, Kur), werden mit dem verbleibenden Anteil nur in Spalte 4 erfasst. Kurzfristige Abwesenheiten bis zu 21 Kalendertagen und Urlaub im üblichen Umfang bleiben unberücksichtigt; mehrere kurzfristige Abwesenheiten werden nicht zusammengezählt.

4 Die Spalten 3 und 4 sind erst beim Abschluss der Übersicht auszufüllen.

5 Es sind zu übernehmen - je auf eine besondere Linie -:
a) in die Spalte 5 die Schlusssummen der Spalte 11 des KB II,
b) in die Spalten 6 bis 10 b die Schlusssummen der Spalten 5 bis 10 A des KB II,
c) in die Spalten 11 bis 16 die Schlusssummen der Spalten 6a bis 6f der Nachweisung über die Entschädigungen der Vollstreckungsbeamten.

6 Es müssen übereinstimmen die Beträge:
a) der Spalte 6 mit denen der Spalte 4 der Nachweisung über die Entschädigung der Vollstreckungsbeamten,
b) der Spalte 8 mit denen der Spalte 3 der Nachweisung über die Entschädigung der Vollstreckungsbeamten,
c) der Spalte 9a, soweit sie dem Beamten voll überlassen worden sind, mit denen der Spalte 5a dieser Nachweisung.

7 Die in das KB I eingetragenen Beträge bleiben, soweit sie noch nicht in das KB II übernommen sind, in dieser Übersicht unberücksichtigt.

8 Zur Berechnung der Vergütungsanteile sind die vereinnahmten Gebühren sowie die erhobenen Dokumentenpauschalen zunächst zu addieren.
Von der Gesamtsumme sind sodann die 55% und im Weiteren die 45% zu errechnen.
Die Gebühren und Dokumentenpauschalen werden bei Erreichen und Überschreiten der Grenze - einmalig - entsprechend ihrem Verhältnis zueinander verteilt.

Bekanntmachungen *)

Staatliche Anerkennung von Einrichtungen nach §§ 35, 36 des Betäubungsmittelgesetzes

Bekanntmachung des Ministeriums der Justiz vom 7. Mai 2024 (4061-0001)

Gemäß der Verwaltungsvorschrift des Ministeriums für Arbeit, Soziales, Gesundheit, Familie und Frauen vom 30. November 2009 (656-75 554-0) - JBl. S. 148 - sind die nachstehenden stationären und ambulanten Einrichtungen der Suchtkrankenhilfe nach §§ 35, 36 Betäubungsmittelgesetz staatlich anerkannt:

Newcare clinic Altenkirchen
Fachklinik für suchtkranke Frauen
Heimstraße 8
57610 Altenkirchen
Tel.: 02681/943-0

MEDIAN Rhein-Haardt-Klinik
Sonnenwendstraße 86
67098 Bad Dürkheim
Tel. 06322/794338

Therapieverbund Ludwigsmühle gemeinnützige Gesellschaft mbH
Fachklinik Villa Maria
Vogesenstraße 18
76831 Billigheim-Ingenheim
Tel. 06349/9969-0

Rehabilitationszentrum Am Donnersberg
Dannenfelser Straße 42
67292 Kirchheimbolanden
Tel. 06352/7536-0

Therapieverbund Ludwigsmühle gemeinnützige Gesellschaft mbH
Psychosomatische Fachklinik
Waldstraße
67363 Lustadt
Tel. 06347/70090

NIDRO REHA
Jugend- und Suchtberatungs- und Behandlungsstellen NIDRO
- in Speyer
  Heydenreichstraße 6
  67346 Speyer
  Tel. 06232/26047
- in Germersheim
  Trommelweg 11b
  76726 Germersheim
  Tel. 07274/919327
- in Neustadt an der Weinstraße
  Schillerstraße 11
  67434 Neustadt an der Weinstraße
  Tel. 06321/9274980

Therapiezentrum Speyer
Wormser Landstraße 1
67346 Speyer
Tel. 06232/6727-0

MEDIAN Klinik Wied GmbH & Co. KG
Mühlental
57629 Wied bei Hachenburg
Tel. 02662/806-0

Die Bek. JM vom 16. Oktober 2023 (4061-0001) - JBl. S. 123 - ist gegenstandslos.

Verlust eines Dienstausweises

Bekanntmachung des Ministeriums der Justiz vom 8. Mai 2024 (2000E24-0027)

Der nachfolgend bezeichnete Dienstausweis wird hierdurch für ungültig erklärt:

Ausweisnummer	Name	Amtsbezeichnung	Ausstellungsbehörde und –datum
58304	Sabine Leinweber	Beschäftigte	Justizvollzugsanstalt Rohrbach 4. Februar 2016

*) Nicht im Landesrecht Rheinland-Pfalz enthalten

Aus Gründen des Datenschutzes
dürfen die Personalnachrichten in
der Internetversion leider nicht
veröffentlicht werden!

Aus Gründen des Datenschutzes dürfen die Personalnachrichten in der Internetversion leider nicht veröffentlicht werden!

Aus Gründen des Datenschutzes
dürfen die Personalnachrichten in
der Internetversion leider nicht
veröffentlicht werden!

Aus Gründen des Datenschutzes
dürfen die Personalnachrichten in
der Internetversion leider nicht
veröffentlicht werden!

Aus Gründen des Datenschutzes
dürfen die Personalnachrichten in
der Internetversion leider nicht
veröffentlicht werden!

Aus Gründen des Datenschutzes dürfen die Personalnachrichten in der Internetversion leider nicht veröffentlicht werden!

Stellenausschreibungen

- vgl. Nummer 2 der VV JM vom 25. Juni 1990 (2010 - 1 - 14/90) - JBl. S. 120 -

Es wird Bewerbungen entgegengesehen um folgende Stellen:

1,0 Stelle für eine Staatsanwältin oder einen Staatsanwalt (m/w/d) bei der Staatsanwaltschaft Bad Kreuznach

Die Stelle soll mit einer Ernennungsbewerberin oder einem Ernennungsbewerber (Richterin oder Richter auf Probe) besetzt werden.

Ausgeschriebene Stellen können auch als Teilzeitstellen (75 v.H. oder 50 v.H.) besetzt werden, soweit nicht im Einzelfall zwingende dienstliche Belange entgegenstehen (§ 7 Abs. 2 LGG, § 5 Abs. 1 LRiG i.V. mit § 11 Abs. 1 Satz 1, 2. Halbsatz LBG). Soweit sich Richterinnen oder Richter (m/w/d) unter Angabe des entsprechenden vom-Hundert-Satzes auf eine Stelle in Teilzeitform bewerben, kann die Bewerbung nur berücksichtigt werden, wenn die Richterin oder der Richter (m/w/d) zugleich zustimmt, mit Beginn oder bei Änderung der Teilzeitbeschäftigung und beim Übergang zur Vollzeitbeschäftigung auch in einem anderen Gericht desselben Gerichtszweiges verwendet zu werden. Unabhängig davon sind Bewerbungen auf eine Stelle in Teilzeitform die sonstigen Erklärungen zum Vorliegen der Voraussetzungen nach § 8 Abs. 1, § 7 Abs. 2 Nr. 3 und 4 LRiG, § 75 Abs. 1 und 2 LBG und die Dauer der beantragten Teilzeitbeschäftigung beizufügen.

Klarstellend wird darauf hingewiesen, dass bei Besetzung einer Vollzeitstelle mit einer Teilzeitkraft (50 v.H.) die ,,zweite“ Hälfte der Stelle ohne weitere Ausschreibung gleichzeitig besetzt werden kann; Entsprechendes gilt für sich anderweitig ergebende Bruchteile (75 v.H.).

Bewerbungen von schwerbehinderten Menschen sind erwünscht.

Im Ministerium der Justiz Rheinland-Pfalz

ist die Stelle der Leitung der Abteilung 2

– Aus- und Fortbildung, Ehrenamt, Stiftung Rheinland-Pfalz für Opferschutz, Internationale Zusammenarbeit –

zu besetzen.

Zum Aufgabengebiet gehören folgende Bereiche:

- Rechtspflegerausbildung, Ausbildungswesen,
- Ausbildung der Beamtinnen und Beamten im ersten und zweiten Einstiegsamt sowie der Amtsanwältinnen und Amtsanwälte, Weiterbildung, Bioethik-kommission,
- Fortbildung, Karriereportal, Wissensmanagement,
- Stiftung Rheinland-Pfalz für Opferschutz, Ehrenamt, Internationale Zusammenarbeit.

Wir erwarten weit überdurchschnittliche Leistungsbereitschaft, hohe Motivation, strategisches Denkvermögen, besonderes Organisationsgeschick, einen kooperativen Führungsstil, Teamfähigkeit und hohe Integrationskraft. Aufgeschlossenheit gegenüber Reformen und wirtschaftlicher Denk- und Handlungsweise sind ebenso wichtig wie ein ausgeprägtes Verständnis für justizpolitische Zusammenhänge.

Im Hinblick auf diese Anforderungen und die herausgehobene Position kommen nur Bewerberinnen oder Bewerber (m/w/d) in Betracht, die bereits mindestens ein Amt der Besoldungsgruppe B 3 oder R 3 innehaben sowie entsprechend eingruppierte Beschäftigte. Die Stelle soll zudem mit einer Beförderungsbewerberin oder einem Beförderungsbewerber (m/w/d) besetzt werden.

In Umsetzung der Selbstverpflichtung „Die Landesregierung - ein familienfreundlicher Arbeitgeber“ bieten wir sehr gute Rahmenbedingungen zur Vereinbarkeit von Beruf und Familie. Das Land fördert aktiv die Gleichstellung aller Mitarbeiterinnen und Mitarbeiter. Wir wünschen uns daher ausdrücklich Bewerbungen aus allen Altersgruppen unabhängig von Geschlecht, einer Behinderung, dem ethnischen Hintergrund, der Religion, Weltanschauung oder sexuellen Identität. Bewerbungen von Frauen werden bei gleicher Eignung, Befähigung und fachlicher Leistung vorrangig berücksichtigt. Schwerbehinderte werden bei sonst gleicher fachlicher und persönlicher Eignung bevorzugt berücksichtigt. Die zu besetzende Stelle erlaubt grundsätzlich die Reduzierung der Arbeitszeit in geringem Umfang. Gehen entsprechende Bewerbungen ein, wird geprüft, ob der Verringerung der Arbeitszeit im Rahmen der dienstlichen Möglichkeiten entsprochen werden kann.

Bewerbungen werden **innerhalb von zwei Wochen unmittelbar** erbeten an das

Ministerium der Justiz
– Personalreferat –
Ernst-Ludwig-Straße 3
55116 Mainz.

Im Ministerium der Justiz Rheinland-Pfalz

ist die Stelle der Leitung (m/w/d) der Abteilung 3

„Öffentliches Recht und Zivilrecht, Verfassungs- und Europarecht, Internationales Recht“

zu besetzen.

Zum Aufgabengebiet gehört die Abteilungsleitung mit den folgenden Bereichen:

- Verfassungs- u. Europarecht, Internationales Recht, Allgemeines Verwaltungs-, Staatsangehörigkeits-, Wahl-, Amts- u. Staatshaftungsrecht, Recht der Informationsfreiheit, GVG,
- Verfahrensordnungen, Aufenthalts- u. Asylrecht, Polizeirecht, Gewerbe- und Berufsrecht, Gesundheitswesen, Verkehrs- und Verkehrswegerecht, Demografie,
- Landwirtschafts- und Weinrecht, Finanzverfassung, Abgaben, Wirtschafts-, Medien-, Jugendschutz-, Geld-, Kredit- u. Sparkassenrecht, Post- und Telekommunikationsrecht, Sozialrecht, Datenschutz,
- Bundesratsangelegenheiten, Bau- u. Raumordnungsrecht, Immissions- und Umweltschutzrecht, Naturschutz-, Energie-, Jagd-, Fischerei- und Forstrecht, Abfallrecht, Gesundheitlicher u. Wirtschaftlicher Verbraucherschutz,
- Rechtsvereinfachung und -bereinigung, Rechtsförmlichkeit, Kommunal-, Denkmalschutz-, Kindertagesstätten-, Schul- und Hochschulrecht, Wissenschaft und Forschung, kulturelle Angelegenheiten,
- BGB (AT), Schuld-, Sachen-, Nachbar-, Urheber-, Stiftungs- und Arbeitsrecht, Verbraucherschutz, Europäisches und Internationales Zivil- und Zivilprozessrecht, Rechtshilfe,
- Handels-, Gesellschafts-, Wettbewerbs- und Wertpapierrecht, Zwangsvollstreckungs-, Insolvenz-, Grundbuch- und Kostenrecht, Rechtspfleger- und Gerichtsvollzieherrecht,
- Familien- und Betreuungsrecht, Zivilrechtlicher Gewaltschutz, Verfahren in Familiensachen und Angelegenheiten der freiwilligen Gerichtsbarkeit, Gerichtliche Verfahren in Landwirtschaftssachen, Prozesskosten- und Beratungshilfe.

Für die Abteilungsleitung suchen wir eine besonders qualifizierte Persönlichkeit mit abgeschlossener wissenschaftlicher Hochschulausbildung und der Befähigung zum Richteramt. Erforderlich ist eine mehrjährige Berufserfahrung in einer verantwortlichen Position mit Führungsaufgaben.

Wir erwarten weit überdurchschnittliche Leistungsbereitschaft, hohe Motivation, strategisches Denkvermögen, ausgeprägtes Organisationsvermögen, Kommunikationsfähigkeit, Verhandlungsgeschick und Durchsetzungsvermögen. Kooperativer Führungsstil, Teamfähigkeit und hohe Integrationskraft werden vorausgesetzt. Aufgeschlossenheit gegenüber Reformen und wirtschaftlicher Denk- und Handlungsweise sind ebenso wichtig wie ein ausgeprägtes Verständnis für justizpolitische Zusammenhänge.

Im Hinblick auf diese Anforderungen und die herausgehobene Position kommen nur Bewerberinnen oder Bewerber (m/w/d) in Betracht, die bereits mindestens ein Amt der Besoldungsgruppe B 3 oder R 3 innehaben sowie entsprechend eingruppierte Beschäftigte.

Die Stelle soll zudem mit einer Beförderungsbewerberin oder einem Beförderungsbewerber (m/w/d) besetzt werden.

In Umsetzung der Selbstverpflichtung „Die Landesregierung - ein familienfreundlicher Arbeitgeber“ bieten wir sehr gute Rahmenbedingungen zur Vereinbarkeit von Beruf und Familie. Das Land fördert aktiv die Gleichstellung aller Mitarbeiterinnen und Mitarbeiter. Wir wünschen uns daher ausdrücklich Bewerbungen aus allen Altersgruppen unabhängig von Geschlecht, einer Behinderung, dem ethnischen Hintergrund, der Religion, Weltanschauung oder sexuellen Identität. Bewerbungen von Frauen werden bei gleicher Eignung, Befähigung und fachlicher Leistung vorrangig berücksichtigt. Schwerbehinderte werden bei sonst gleicher fachlicher und persönlicher Eignung bevorzugt berücksichtigt. Die zu besetzende Stelle erlaubt grundsätzlich die Reduzierung der Arbeitszeit in geringem Umfang. Gehen entsprechende Bewerbungen ein, wird geprüft, ob der Verringerung der Arbeitszeit im Rahmen der dienstlichen Möglichkeiten entsprochen werden kann.

Bewerbungen werden **innerhalb von zwei Wochen unmittelbar** erbeten an das

Ministerium der Justiz
– Personalreferat –
Ernst-Ludwig-Straße 3
55116 Mainz.

Bei den Justizvollzugseinrichtungen des Landes

wird Bewerbungen entgegengesehen um

1 Stelle für eine Dezernentin oder einen Dezernenten (viertes Einstiegsamt) bei der Justizvollzugsanstalt Wittlich (m/w/d), die im Wege der Fortbildungsqualifizierung gem. § 29 LbVO besetzt werden soll.

Die Justizvollzugsanstalt Wittlich ist eine Einrichtung für den Strafvollzug an männlichen erwachsenen Inhaftierten. Die Anstalt verfügt über 535 Haftplätze im geschlossenen und 41 Haftplätze im offenen Vollzug sowie ein Justizvollzugskrankenhaus mit 68 Haftplätzen.

Das Aufgabengebiet hat folgende Schwerpunkte:

- Aufsicht über Vollzugs- und Verwaltungsabteilungen,
- vollzugsorientierte Aufsicht über die Fachabteilung Medizin,
- Bearbeitung von Rechtsangelegenheiten,
- Mitwirkung bei der Einstellung des Personals und in Personalentscheidungen,
- Mitwirkung bei dienstlichen Beurteilungen,
- Mitwirkung bei Entscheidungen nach Nr. 2.2.1.28 GrundsO, soweit es sich um Eingaben, Beschwerden und Dienstaufsichtsbeschwerden betreffend die Vollzugs-, die Verwaltungs- und die Fachabteilungsleitungen handelt, die dem jeweils zuständigen Dezernat unterstehen,

- Durchführung der Ermittlungen in beamtenrechtlichen Disziplinarverfahren und Vorbereitung von Disziplinarverfügungen, soweit es sich um Bedienstete der Abteilungen handelt, die dem jeweils zuständigen Dezernat unterstehen,
- Führen von Mitarbeitendengesprächen,
- Erarbeitung, Implementierung und Begleitung von Resozialisierungskonzepten,
- Bewältigung von besonderen Vorkommnissen,
- Vorlage zur Weiterleitung geeigneter unterschriftsreifer Entwürfe aus den Vollzugs- sowie den Verwaltungsabteilungen an den Anstaltsleiter,
- Vertretung des Anstaltsleiters in Pressesachen,
- Repräsentation des Justizvollzuges und der JVA Wittlich bei öffentlichkeitswirksamen Veranstaltungen,
- vertrauensvolle Zusammenarbeit mit der Aufsichtsbehörde.

Hierbei handelt es sich um umfangreiche und schwierige Aufgaben. Für die Fortbildungsqualifizierung kommen daher nur Beamtinnen und Beamte in Betracht, die mit Blick auf das Aufgabenprofil bereits über langjährige, tiefgehende und breite Erfahrungen in den Verwaltungsabteilungen einer Justizvollzugs- oder Jugendstrafanstalt sowie insbesondere über langjährige und umfangreiche Personalführungsverantwortung in einer größeren Einrichtung verfügen. Zu der Fortbildungsqualifizierung können nur Beamtinnen und Beamte zugelassen werden, die sich in ihren bisherigen Verwendungen entsprechend bewährt haben. Zudem sollen die Gesamtpersönlichkeit und die bisherigen Leistungen der Beamtinnen und Beamten erwarten lassen, dass sie sich im Rahmen der Fortbildungsqualifizierung die notwendigen Kenntnisse und Fertigkeiten für ein Beförderungsamt der Besoldungsgruppe A 14 LBesO aneignen können.

Bewerbungen werden bis 21. Juni 2024 auf dem Dienstweg erbeten an das

Ministerium der Justiz
- Personalreferat Abteilung 5 –
- Justizvollzug -
Ernst-Ludwig-Straße 3
55116 Mainz.

In der Leitstelle für Informationstechnologie, Informationssicherheit und Finanzbuchhaltung (LITISF) im Justizvollzug Rheinland-Pfalz

ist zum nächstmöglichen Zeitpunkt

eine Vollzeitstelle als

Informatikerin / Informatiker (m/w/d)
(Tätigkeitsschwerpunkt Informationssicherheit)

(Bachelor of Science, Diplom oder vergleichbare abgeschlossene Hochschulausbildung) zu besetzen.

Die LITISF nimmt für den Bereich des Justizvollzugs für alle Justizvollzugseinrichtungen die Aufgaben eines Servicecenters in den Bereichen Informationstechnologie, Informationssicherheit und Finanzbuchhaltung wahr und ist insbesondere für die Betreuung und Pflege der im Justizvollzug des Landes Rheinland-Pfalz eingesetzten IT-Programme zuständig.
Sie ist eine eigenständige Organisationseinheit mit landesweiter Zuständigkeit, die organisatorisch der Justizvollzugsanstalt Koblenz angegliedert und extern im Stadtgebiet von Koblenz angesiedelt ist.

Ihre Aufgaben sind insbesondere:

- Erstellung, Koordination und Begleitung von Regelwerken zur Informationssicherheit und von IT-Sicherheitskonzepten
- Beratung und Unterstützung der Behördenleitungen in allen Belangen der Informationssicherheit sowie Ansprechperson für alle Beschäftigten für Belange der Informationssicherheit
- Konzeption, Durchführung und Dokumentation von IT Sicherheitsmaßnahmen
- Planung und Steuerung des Informationssicherheitsprozesses (inkl. der Dokumentation) sowie ständige Auswertung der aktuellen Entwicklungen im Bereich der Informationssicherheit (auch Zusammenarbeit mit dem CERT-rlp)
- Gremienarbeit im Bereich der Informationssicherheit (insbesondere Mitarbeit in der Informationssicherheitsorganisation der rheinland-pfälzischen Justiz)
- Erstellung, Abstimmung und Prüfung von Grob- und Feinkonzepten der im rheinland-pfälzischen Justizvollzug zum Einsatz kommenden IT-Basiskomponenten (z. B. elektronisches Gerichts- und Verwaltungspostfach EGVP, besondere Postfächer im Rahmen des elektronischen Rechtsverkehrs, E-Rechnungen) und den vollzugsspezifischen IT-Fachverfahren (wie z.B. BASIS-Web, MACH, NEXUS-VeLis)
- Mitarbeit bei landesinternen oder länderübergreifenden Projekten und Arbeitsgruppen, zu denen das Ministerium Mitglieder entsendet – Konzepterstellung, Mitwirkung und Vorbereitung von Rolloutplanungen
- Installation, Administration und Wartung von Teilen der IT-Basisinfrastruktur des rheinland-pfälzischen Justizvollzuges

Sie verfügen über:

- eine abgeschlossene Hochschulausbildung (Bachelor of Science B.Sc. oder Diplom) als Informatikerin oder Informatiker, Wirtschaftsinformatikerin oder Wirtschaftsinformatiker
- gute Kenntnisse der BSI Standards 200-1 / 200-2 / 200-3, der BSI Grundschutzkataloge und der technischen Richtlinien des BSI (BSI TR)
- Kenntnisse im Projektmanagement
- Programmierkenntnisse und Erfahrungen in modernen und gebräuchlichen Programmiersprachen und Datenbankabfragen
- ausgeprägtes analytisches Denkvermögen in vernetzten Zusammenhängen einer IT-Landschaft
- Kenntnisse in Betriebswirtschaftslehre
- Grundkenntnisse im Bereich der System- und Datenbankadministration
- Bereitschaft zu regelmäßigen auch mehrtägigen Dienstreisen
- Führerschein Klasse B (Pkw)

Wir erwarten:

- Fähigkeit zu sorgfältigem und serviceorientiertem Denken und Handeln
- Fähigkeit Arbeitsabläufe kritisch zu analysieren und zu gestalten
- besondere Zuverlässigkeit im Hinblick auf die besonderen Sicherheitsanforderungen des Justizvollzuges
- selbstbewusstes und sicheres Auftreten, Verhandlungsgeschick und gute Kommunikationsfähigkeiten
- ein hohes Maß an Selbstständigkeit und Eigeninitiative
- Freude an der Zusammenarbeit im Team
- Flexibilität und Kommunikationsfähigkeit
- Leistungs-und Lernbereitschaft zur Einarbeitung in justizielle Fachgebiete für Projekte und Arbeitsgruppen
- Lern- und Fortbildungsbereitschaft
- Mobilität

Wir bieten Ihnen:

- einen krisensicheren Arbeitsplatz
- interessante und anspruchsvolle Aufgabenstellungen
- ein sehr gutes Betriebsklima in einem hoch motivierten Umfeld
- eigenverantwortliche Tätigkeit
- einen modernen Arbeitsplatz mit flexiblen Arbeitszeitmodellen und der Möglichkeit des Arbeitens auch außerhalb der Dienststelle
- ein familienfreundliches Arbeitsumfeld
- qualifizierte Weiterbildungsmöglichkeiten

Die Eingruppierung orientiert sich an der Qualifikation und dem Tarifvertrag für den öffentlichen Dienst der Länder TV-L.
Eine Übernahme in das Beamtenverhältnis (bis Besoldungsgruppe A 12 LBesG) ist bei Vorliegen der laufbahnrechtlichen Voraussetzungen möglich.

Ihre Bewerbung richten Sie bitte bis zum 15. August 2024 an das

Ministerium der Justiz
- Personalreferat Abteilung 5 –
- Justizvollzug -
Ernst-Ludwig-Straße 3
55116 Mainz.

Elektronische Bewerbungen richten Sie bitte an das Bewerbungspostfach
bewerbung-justizvollzug@jm.rlp.de

Ausgeschriebene Stellen können auch als Teilzeitstellen (75 v.H. oder 50 v.H.) besetzt werden, soweit nicht im Einzelfall zwingende dienstliche Belange entgegenstehen.
Bei Bewerbungen von Beamtinnen und Beamten auf eine Stelle in Teilzeitform sind die sonstigen Erklärungen zum Vorliegen der Voraussetzungen nach § 75 LBG und die Dauer der beantragten Teilzeitbeschäftigung beizufügen. Zur Klarstellung wird darauf hingewiesen, dass bei Besetzung einer Vollzeitstelle mit einer Teilzeitkraft (50 v.H.) die zweite Hälfte der Stelle

ohne weitere Ausschreibung gleichzeitig besetzt werden kann. Entsprechendes gilt für sich anderweitig ergebende Bruchteile (z.B. 75 v.H.).

In Umsetzung der Selbstverpflichtung „Die Landesregierung – ein familienfreundlicher Arbeitgeber“ bieten wir sehr gute Rahmenbedingungen zur Vereinbarkeit von Beruf und Familie. Das Land fördert aktiv die Gleichstellung aller Mitarbeiterinnen und Mitarbeiter. Wir wünschen uns daher ausdrücklich Bewerbungen aus allen Altersgruppen unabhängig von Geschlecht, einer Behinderung, dem ethnischen Hintergrund, der Religion, Weltanschauung oder sexuellen Identität. Bewerbungen von Frauen werden bei gleicher Eignung, Befähigung und fachlicher Leistung vorrangig berücksichtigt. Schwerbehinderte werden bei sonst gleicher fachlicher und persönlicher Eignung bevorzugt berücksichtigt.

HERAUSGEBER: Ministerium der Justiz Rheinland-Pfalz, Postfach 32 60, 55022 Mainz, Ernst-Ludwig-Straße 3, 55116 Mainz, Telefon (0 61 31) 16-4876

DRUCK und VERLAG: JVA Diez Druckerei, Limburger Str. 122, 65582 Diez, Telefon (0 64 32) 6 09-3 01, Telefax (0 64 32) 60 9-3 04
E-Mail druckerei.jvadz@vollzug.jm.rlp.de

ERSCHEINUNGSWEISE UND BEZUGSBEDINGUNGEN:

Das Justizblatt Rheinland-Pfalz erscheint nach Bedarf. Bezugspreis halbjährlich 11,76 EUR. Bestellungen sind unmittelbar an den Verlag zu richten. Abbestellungen zum 30.6. oder 31.12. müssen bis spätestens 15.5. bzw. 15.11. beim Verlag vorliegen. Einzelpreis (auch für Nachbestellungen des laufenden oder eines früheren Jahrgangs) 1,38 EUR zuzüglich Versandkosten.

Justizvollzugs- und Sicherungsverwahrungsanstalt Diez · Limburger Straße 122 · 65582 Diez · Postvertriebsstück · ZKZ 63004 · Entgelt bezahlt