28. APRIL 2023

In der Fassung vom 28. August 2025

DIENSTANWEISUNG FÜR DIE NUTZUNG DER IT-INFRASTRUKTUR BEI DEM AMTSGERICHT WEDDING

1 Inhaltsverzeichnis

2 Vorbemerkung

Die Serviceeinheit ITOG (Dezernat X - Informationstechnik in der ordentlichen Gerichtsbarkeit bei dem Präsidenten des Kammergerichts) und das IT-Dienstleistungszentrum Berlin (ITDZ) stellen zusammen mit dem Behördenvorstand eine IT-Infrastruktur und ausgewählte Online-Dienste (z.B. Intranet, Internet, E-Mail) zur Verfügung und sind für einen störungsfreien technischen Betrieb verantwortlich.

Diese Dienstanweisung regelt den Einsatz der Informationstechnik (Hard- und Software) im Hinblick auf die geltenden Bestimmungen des Datenschutzes, die Anforderungen an die IT-Sicherheit sowie die Erfordernisse des Dienstbetriebes. Sie gilt gleichermaßen für alle Angehörigen des Amtsgerichts Wedding sowie andere Personen, die auf die zur Verfügung stehende IT- Technik zugreifen.

3 Begriffsbestimmungen

Im Sinne dieser Dienstanweisung sind

Dez X beim Präsidenten des KG ITOG	Dezernat für Informationstechnologie in der ordentlichen Gerichtsbarkeit bei dem Präsidenten des Kammergerichts
ITDZ	IT-Dienstleistungszentrum Berlin
FAT- Client	Arbeitsplatz-PC der Anwendenden
VPN Client	Mobiler Arbeitsplatz; Notebook; Zugriffsmöglichkeit über eine direkte, verschlüsselte Datenverbindung zum zentralen Server
SBC	Server Based Computing der ordentlichen Gerichtsbarkeit, in der zurzeit die meisten Programme und Daten auf zentralen Servern

	bereitgestellt, ausgeführt und gesichert werden
IT-Betreuung/Support-Team des AG Wedding	Die geschäftsplanmäßig mit der Wahrnehmung der Aufgaben der IT-Angelegenheiten befassten Mitarbeitenden des Amtsgerichts Wedding
Anwendungsbetreuer*Innen	Die örtlich mit der Wahrnehmung der Aufgaben als Anwendungsbetreuer*In betrauten und geschulten Mitarbeitenden des Amtsgerichts, Ansprechpartner ggü. dem Dez. X; First-Level-Help-Desk
Anwenderbetreuer*Innen	Örtliche Mitarbeitende, die bei der Erledigung von Fachaufgaben mit der Informationstechnik unterstützen

4 Sicherheitsbestimmungen

4.1 Allgemeines

Das ITDZ hat eine Reihe von Maßnahmen (z.B. Installation von Virenscanner und Firewall) ergriffen, um die Sicherheit des IT-Systems beim Amtsgericht Wedding zu gewährleisten. Damit diese Vorkehrungen ihre volle Wirksamkeit behalten, sind über diese Maßnahmen hinaus bei der Benutzung der zur Verfügung stehenden Informationstechnik die nachstehenden Sicherheitsbestimmungen zu beachten.

4.2 Nutzung der eingesetzten Hardware (PC, Drucker, Monitor, etc.)

4.2.1 Aufstellung

Die Geräte dürfen nur durch autorisiertes Personal aufgestellt werden. Sie sind nicht direkt der Sonneneinstrahlung auszusetzen und nicht in der Nähe von Wärmequellen aufzustellen. Die Ventilationsöffnungen dürfen nicht zugedeckt oder blockiert werden. Es dürfen keine eigenmächtigen Standortveränderungen vorgenommen werden.

4.2.2 Umgang

Es ist sorgsam mit den Geräten umzugehen. Die Geräte dürfen nicht gewaltsam behandelt werden. Das Gehäuse darf nicht entfernt oder geöffnet werden, ebenso dürfen keine privaten Aufkleber auf den Gerätegehäusen angebracht werden. Essen und Trinken in der Nähe der Geräte ist insoweit untersagt, als dies zu einer Schädigung der Geräte führen kann. Es dürfen keine Gegenstände auf die Geräte gestellt werden.

4.2.3 Verbrauchsmaterialen und Reinigung

Das Öffnen der Geräteklappen ist nur insofern erlaubt, als diese Klappen zum Wechseln bzw. Auffüllen von Verbrauchsmaterialien (Toner, Tonerbehälter und Papier) dienen oder zur Beseitigung eines einfachen Papierstaus vorgesehen sind. Hierzu dürfen nur Hilfsmittel verwendet werden, die zum Zubehör der Geräte oder der Verbrauchsmaterialien gehören oder zu diesem Zweck als Zubehör besonders angeschafft worden sind. Die Einwirkung auf die Geräte mit anderen Hilfsmitteln oder Gegenständen (Schere, Büroklammern, etc.) ist untersagt.

4.2.4 Störungen/Betriebseinschränkungen

Störungen oder Betriebseinschränkungen der Geräte sind umgehend dem Supportteam des Amtsgerichts Wedding (support@ag-we.berlin.de) bzw. der IT-Stelle des Mahngerichts zu melden.

Sofern Störungen sämtliche Bedienstete betreffen (z.B. Systemausfälle), gibt die Verwaltung die vorliegenden Informationen über die Gruppenleitungen sowie die Wachtmeisterei an die Nutzerinnen und Nutzer weiter.

4.2.5 Wartung

Wartungsarbeiten dürfen nur durch autorisiertes IT-Personal oder durch den autorisierten Kundendienst erfolgen.

4.2.6 Regelung des Passwortgebrauchs

Die Benutzerkennung und das Passwort regeln die technische Zugangskontrolle zum IT-Netz. Damit verbunden ist die Festlegung der einzelnen Zugriffsrechte auf Verzeichnisse, Dateien oder Online-Dienste.

Das Startpasswort ist unmittelbar nach der Erstanmeldung durch ein selbst gewähltes Passwort zu ersetzen. Die Länge des Passwortes muss entsprechend den Voreinstellungen im System mindestens 10 Zeichen betragen. Das Passwort muss aus Groß- und Kleinbuchstaben bestehen und mindestens eine Ziffer bzw. ein Sonderzeichen enthalten.

Die Zeichenzusammensetzung des Passwortes muss so komplex sein, dass ein Erraten ausgeschlossen ist. Das Passwort darf zudem keinen persönlichen Bezug haben (Name, Vorname, Tel.-Nr., etc.). Empfehlenswert ist z. B. ein kurzer ungewöhnlicher Satz.

Das Passwort muss geheim gehalten werden, die Weitergabe ist strikt untersagt.

Im Falle einer Weitergabe des Passwortes wird jegliche Aktivität - auch unzulässige Nutzung durch Dritte - der die Kennung innehabenden Dienstkraft zugeschrieben.

Im Falle einer Vertretung in Abwesenheitszeiten (Urlaub, Krankheit,) müssen die vertretenden Dienstkräfte über eine eigene Kennung mit Passwort verfügen. Anmeldungen unter fremden Kennungen sind verboten.

Mehrmalige Falscheingaben von Passwörtern werden vom System protokolliert und unterbunden. Wurde das Passwort vergessen, ist dies der Anwenderbetreuung bzw. der

IT-Stelle des Mahngerichts mitzuteilen, die die Bereitstellung eines neuen Startkennwortes veranlasst.

Das Passwort kann jederzeit geändert werden. Sollte der Verdacht bestehen, dass trotz sorgsamen Umgangs mit dem Passwort, Dritte Kenntnis von ihm erhalten haben, ist das Passwort unverzüglich zu ändern. Dazu sind die Tasten STRG+ALT+ENTF gleichzeitig zu betätigen und die Option „Kennwort ändern“ mit der Maus auszuwählen.

Die Eingabe des Passwortes muss unbedingt unbeobachtet/verdeckt erfolgen. Der Monitor und die Tastatur sind so aufzustellen, dass ein Beobachten der Zeicheneingabe ausgeschlossen ist. Passwörter dürfen nicht auf programmierbaren Funktionstasten gespeichert werden. Ein Zugriff Dritter ist unbedingt auszuschließen.

4.3 Räumliche Zugangskontrolle

Es ist sicherzustellen, dass unberechtigten Personen der Zugang zu den Diensträumen verwehrt bleibt. Eine Einsichtnahme in schutzbedürftige Daten durch Dritte ist zu verhindern (z.B. durch entsprechende Aufstellung des Bildschirms, Verwenden der Bildschirmsperre).

Beim Verlassen des Raumes - auch bei kurzer Abwesenheit - ist die passwortgeschützte Bildschirmsperre zu aktivieren (aufzurufen über die Tastenkombination STRG+ALT+ENTF und „Computer sperren“). Die Verpflichtung zum Abschließen der Diensträume bleibt unberührt. Bei längerer Abwesenheit und zum Dienstschluss ist der PC ordnungsgemäß herunterzufahren.

4.4 Datenübertragung in das IT-Netz

Die Übertragung von Daten in das IT-Netz (z. B. per E-Mail) sind auf das dienstlich unbedingt erforderliche Maß zu beschränken. Es dürfen nur Daten von Datenträgern, deren Herkunft bekannt ist, in das IT-Netz übertragen werden. Die Übernahme von ausführbaren Programmdateien (z. B. *.com, *. exe) ist unzulässig. Die von mobilen Datenträgern zu übertragenden Daten sind ausschließlich über den Transfer-PC einzuspeisen. Nicht mehr benötigte Daten sind umgehend zu löschen.

Verwenden Sie eine Datenverschlüsselung bei der Speicherung von personenbezogenen Daten. Die Anleitung für die Verschlüsselungssoftware 7Zip finden Sie hier: https://justiz.b-intern.de/ag-wedding/arbeitshilfen/bedienungsanleitungen/

4.5 Verhalten bei Virenbefall und sonstigen Sicherheitsvorkommnissen

Sollte es trotz der vom ITDZ getroffenen technischen und in dieser Dienstanweisung enthaltenen Vorbeugemaßnahmen zu einem Virenbefall kommen, ist - auch bereits bei bloßem Verdacht auf Virenbefall - Folgendes zu beachten:

a) Beachten Sie auf keinen Fall die auf dem Bildschirm ausgegebenen Meldungen! Stellen Sie die Anwendung sofort ein und benachrichtigen Sie umgehend die/den IT-Sicherheitsbeauftragte(n), die Anwendungsbetreuung (-777) oder die Annahmestelle für IT-Störungsmeldungen beim Kammergericht (Anita - Servicenummer: 915-2515).

b) Der Rechner ist sofort durch Lösen des Datenkabels aus der Anschlussdose der Hausverkabelung vom Netz zu nehmen. Das Lösen des Datenkabels ist in diesem Fall ausnahmsweise durch den bzw. die Nutzer/in vorzunehmen.

c) Weitere Maßnahmen sind nur nach Maßgabe der/des IT-Sicherheitsbeauftragten bzw. der Anwendungsbetreuung zu treffen. Die Weitergabe von Informationen über das Sicherheitsvorkommnis an Dritte ist unzulässig.

5 Laufwerke (Dateiablage)

5.1 Allgemeines

Die nachstehenden Regelungen gelten nur, soweit Dateien außerhalb der Fachverfahren (AULAK, forumSTAR, AUMAV, EUMAV) gespeichert werden. Sie gewährleisten, dass die Dateien im IT-Netz gefunden werden können. Die Regelungen sind daher unbedingt einzuhalten.

5.2 Home-Laufwerk „H:“

Jeder bzw. jedem Benutzer/in wurde in der SBC-Umgebung ein Home-Verzeichnis zugeordnet, auf das außer der Systemadministration kein Dritter Zugriff hat. Dateien und Entwürfe, die nicht von Dritten gelesen werden sollen, sind in diesem Verzeichnis abzulegen.

5.3 Gemeinsame Laufwerke

Sobald eine Weiterbearbeitung von Dateien durch Dritte erfolgen soll, sind diese in den entsprechend eingerichteten gemeinsamen Verzeichnissen abzulegen. Die Verzeichnisse werden von der Nutzerverwaltung in den Zugriffsrechten auf den jeweils vorgesehenen Nutzerkreis beschränkt.

5.4 Laufwerk „I:“

In diesem Laufwerk werden allgemeine Informationen für die Bediensteten bereitgestellt, wie z.B. Telefonverzeichnisse, Antragsformulare, etc. Die Daten können gelesen, aber nur von der Nutzerverwaltung verändert werden.

5.5 Laufwerke „U:“ und „S:“

Das Laufwerk „U:“ dient dem Datenaustausch innerhalb der Fachabteilungen. Das Laufwerk „S:“ steht für den Datenaustausch innerhalb der Verwaltungsabteilung zur Verfügung. Das Anlegen von Verzeichnissen sowie die Erweiterung bzw. Beschränkung von Zugriffsrechten obliegt der Nutzerverwaltung.

5.6 Laufwerk „T:“

Dieses Laufwerk dient dem Daten-Transfer z.B. zur Datenübertragung vom Transfer-PC in das IT-System sowie zur Datenübertragung zwischen einzelnen Nutzerinnen/Nutzern. Die Speicherung von Daten im Laufwerk T: soll grundsätzlich nur von vorübergehender Dauer sein.

Daten, die sich längere Zeit in diesem Laufwerk befinden, werden in regelmäßigen Abständen vom ITDZ gelöscht.

6 Online-Dienste (Intranet/Internet) und elektronische Post

Mit der bereitgestellten IT-Infrastruktur ist generell die Nutzung des Intranets der Berliner Verwaltung, des Internets sowie die Versendung und der Empfang elektronischer Post (E-Mail) möglich.

Die Einzelheiten der Nutzung der Online-Dienste (Internet, Intranet und E-Mail) sind in der zwischen der Senatsverwaltung für Inneres und dem Hauptpersonalrat für die Behörden, Gerichte und nichtrechtsfähigen Anstalten des Landes Berlin geschlossenen Dienstvereinbarung über die Nutzung des Internet und anderer elektronischer Informations- und Kommunikationsdienste in der Berliner Verwaltung vom 20.02.2002 sowie in der zwischen der Senatsverwaltung für Justiz im Einvernehmen mit der Senatsverwaltung für Integration, Arbeit und Soziales und dem Hauptrichterrat des Landes Berlin geschlossenen Dienstvereinbarung über die Nutzung des Internet und anderer elektronischer Informations- und Kommunikationsdienste in den Berliner Justizbehörden und Gerichten vom Stand 20.10.2010 geregelt.

7 Elektronischer Rechtsverkehr

7.1 Empfang

Der elektronische Empfang verfahrensbezogener Dokumente und Anträge erfolgt ausschließlich über Postfächer des Elektronischen Gerichts- und Verwaltungspostfachs - EGVP - mit Hilfe der Eingangslistenapplikation (ELA) oder der in den Mahnverfahren vorgehaltenen Applikationen. Näheres regelt die Dienstanweisung
für die Behandlung elektronischer Eingänge und jene für die IT-Stelle im Zentralen Mahngericht Berlin-Brandenburg und im Europäischen Mahngericht Deutschland; veröffentlicht in der Vorschriftendatenbank unter Organisation – Dienstliche Regelungen:

https://justiz.b-intern.de/ag-wedding/organisation/dienstliche-regelungen/vorschrift.451493.php sowie https://justiz.b-intern.de/ag-wedding/organisation/dienstliche-regelungen/vorschrift.1074371.php .

7.2 Versand aus forumSTAR

Das elektronische Versenden und Weiterleiten von Dokumenten erfolgt über die Fachanwendung forumSTAR. Hierbei sind die Dokumente regelmäßig mit einer qualifizierten elektronischen Signatur mittels Signaturkarte zu versehen. Durch Einstecken der Karte in den SC-Kartenslot der Tastatur und Eingabe der persönlichen PIN wird der qualifizierte Versand ausgelöst.

7.3 Versand über das elektronische Gerichts- und Verwaltungspostfach (EGVP)

In Verwaltungsangelegenheiten erfolgt die Kommunikation mit anderen Gerichten und Behörden in den gesetzlich vorgeschriebenen Fällen in elektronischer Form. Der Versand erfolgt über die Fachanwendung durch autorisierte Personen. Sofern die Fachanwendung geeignet ist den vertrauenswürdigen Herkunftsnachweis zu erzeugen, bedarf es einer qualifizierten elektronischen Signatur der Dokumente nicht mehr.

7.4 Signaturkarten

Bei der Signaturkarte handelt es sich um eine Chipkarte, die den privaten Schlüssel eines digitalen Zertifikats enthält. Eine qualifizierte elektronische Signatur (qeS) hat die gleiche Rechtswirkung wie eine handschriftliche Unterschrift. Die Identität der Person, die das Dokument signiert hat, ist damit zweifelsfrei nachweisbar. Die Signaturkarte wird für die Mitarbeitenden über den IT-Support beantragt. Nach Erhalt der Signaturkarte ist ein*e Mitarbeiter*in der IT-Stelle zu informieren, damit dieser*diese die Aktivierung der Karte vornehmen kann. Die zur Signaturkarte gehörige PIN und PUK sind geheim zu halten. Die Karte ist diebstahlsicher und vor Fremdzugriff geschützt aufzubewahren. Die Nutzung der Karte ist

personengebunden und ausschließlich zu dienstlichen Zwecken zulässig. Beim Ausscheiden aus dem Dienst ist die Karte der Dienststelle zu übergeben. Beim Wechsel der Dienststelle darf diese weiter genutzt werden. Bei Verlust, Beschädigung oder unbefugter Benutzung ist die Dienststelle unverzüglich in Kenntnis zu setzen.

8 Fachverfahren

Zur dienstlichen Nutzung stehen Fachanwendungen und Online-Abfragen zur Verfügung.
Die Einrichtung und Verwaltung der Zugangsberechtigungen obliegt dem IT-Support-Team bzw. der IT-Stelle des Mahngerichts.
Hierzu zählen insbesondere:

- **beck-online** und **juris** (juristische Recherche)
- **AUMAV** (Automatisiertes Mahnverfahren)
- **EUMAV** (Europäisches Mahnverfahren)
- **Olmera** (Zugriff auf Einwohnermeldedaten.) Bei Abfragen ist in jedem Fall das Aktenzeichen des Bezugsverfahrens anzugeben.
- **ZTR** (Zentrales Testamentsregister)
- **Vollstreckungsportal** (Einsicht in Schuldner- und Vermögensverzeichnisse)
- **ProFiskal** (Rechnungswesen)
- **AULAK** (Aktenverwaltung und Schriftguterstellung, nur noch für die Nachlassabteilung)
- **forumSTAR** (Aktenverwaltung und Schriftguterstellung)

9 Mobiles Arbeiten

9.1 Ausstattung

Der Empfang der Geräte ist zu quittieren. Sie sind sorgfältig zu behandeln. Die Einrichtung, Wartung und ggf. Reparatur der Geräte bzw. die entsprechende Beauftragung obliegen dem Support-Team des Amtsgerichts.

9.2 Umfang der Nutzung

Die Geräte dürfen nur für dienstliche Zwecke genutzt werden. Dienstliche Angelegenheiten umfassen auch Angelegenheiten der Gerichtsverwaltung, die Tätigkeit als Güterichterin/ Güterichter, Schulungstätigkeiten sowie ehrenamtliche Tätigkeiten im Zusammenhang mit richterlicher Tätigkeit (z.B. im Präsidium, in Mitwirkungsgremien, als Datenschutz- oder Schwerbehindertenbeauftragte*r oder im Richterwahlausschuss). Das Speichern von nicht für die dienstliche Nutzung bestimmten Daten auf dem Laptop ist unzulässig. Für das mobile Arbeiten sowie das Arbeiten am häuslichen Arbeitsplatz sind, vorbehaltlich speziellerer, Regelungen, grundsätzlich nur die dienstlich zur Verfügung gestellten und an die sichere IT-Umgebung der Berliner Justiz angeschlossenen Endgeräte einzusetzen.

9.3 Notebook/Tablet-Benutzung

Bei der Nutzung eines dienstlich zur Verfügung gestellten Notebooks/Tablets sind folgende Regeln einzuhalten:

Das Gerät ist pfleglich zu behandeln und nicht direkter Sonneneinstrahlung oder Feuchtigkeit auszusetzen. Es ist untersagt, das Gerät zu manipulieren oder zu warten. Wartungsarbeiten darf allein die IT-Stelle vornehmen bzw. beauftragen. Das Gerät ist stets verschlossen aufzubewahren. Beim Transport ist mit besonderer Sorgfalt darauf zu achten, dass Beschädigungen vermieden werden. Beim Transport mit einem Kraftfahrzeug ist es außerdem gesichert und für Dritte nicht einsehbar aufzubewahren. Nach dem derzeit bekannten technischen Sachstand ist der Zugang zum VPN der Justiz über jede Form der Netzwerkverbindung unter Aspekten der Datensicherheit gefahrlos, da von dem Gerät eine direkte, verschlüsselte Datenverbindung zu den beim ITDZ betriebenen Systemen aufgebaut wird. Dennoch besteht die Möglichkeit, dass z. B. der Nutzung von öffentlichen WLAN-Hotspots aus der Anmeldung des Gerätes am Netzwerk Nutzer*Innenprofile erstellt werden können.
Es obliegt daher wie bei anderen privaten netzwerkfähigen Geräten dem oder der Nutzer*in des Notebooks, welche WLAN-Netzwerke als vertrauenswürdig eingestuft werden.

Kommunikationsschnittstellen wie Netzwerkanschlüsse, drahtlose Kommunikationsschnittstellen und andere Schnittstellen zum VPN der Berliner Justiz dürfen mit einem mobilen Gerät nur dann genutzt werden, wenn das Gerät dafür berechtigt ist, m.a.W. das Gerät darf nicht eigenmächtig, sondern nur nach entsprechender Instruktion durch einen Mitarbeitenden der IT-Stelle mit den im Dienstgebäude befindlichen Netzwerkanschlüssen verbunden werden. Bei Übergabe und Rückgabe ist die Vollständigkeit des Gerätes sowie des Zubehörs sicherzustellen.

9.4 Kosten des mobilen Arbeitens

Die durch das mobile Arbeiten anfallenden Kosten, einschließlich Verbrauchskosten, z.B. für Strom oder Telekommunikation, sind von den Mitarbeitenden selbst zu tragen. Etwaige im Rahmen der Einführung der E-Akte ausbedungene Kostenregelungen bleiben hiervon unberührt. Weiterhin unberührt bleibt der durch Ortstermine und Anhörungstermine bestehende Anspruch auf Auslagenersatz.

10 Sicherheitsmaßnahmen

10.1 Sicherheitsrelevante Ereignisse

Alle bei der Nutzung der Dienste auftretenden sicherheitsrelevanten Ereignisse, wie z.B. unerklärliches Systemverhalten, Verlust oder Veränderung von Daten und Programmen, Verdacht auf Missbrauch der Benutzer*innenkennung, des Passwortes usw., sind durch den*die Anwender*in unverzüglich dem IT-Support-Team anzuzeigen. Aufklärungsversuche durch den*die Anwender*in sind erst nach Absprache mit den dort Zuständigen zulässig.

10.2 Vorbehalte

Bei der Beschaffung, Weiterverarbeitung und Weitergabe der über die Dienste zugänglichen Informationen sind Urheber- und Lizenzrechte zu beachten. Zweifelsfälle sind unverzüglich mit der Gerichtsleitung zu klären.

10.3 Kostenpflichtige Angebote

Der Zugriff auf kostenpflichtige Angebote ist nur nach Zustimmung der Gerichtsleitung zulässig. Mit Zustimmung des Dezernats X bei der Präsidentin des Kammergerichts angebotene Informationen (z.B. Juris und beck-online) bleiben hiervon unberührt.

11 Sanktionen

Vorsätzliche und grob fahrlässige Verstöße gegen die Regelungen zur Nutzung der ITInfrastruktur können den sofortigen Ausschluss der Dienstkraft von der Nutzung der ITSysteme zur Folge haben sowie ggf. weitere dienst- und strafrechtliche Konsequenzen nach sich ziehen. Die Haftung der Beschäftigten gegenüber dem Dienstherrn für Beschädigungen bzw. Abhandenkommen von Geräten für das mobile Arbeiten ist auf Vorsatz und grobe Fahrlässigkeit beschränkt. Eine Haftung für unabwendbare oder auf höherer Gewalt beruhende Ereignisse besteht nicht.

12 Inkrafttreten/Außerkrafttreten

Diese Dienstanweisung ersetzt die „Dienstanweisung für die Nutzung der IT-Infrastruktur bei dem Amtsgericht Wedding“ vom 01.04.2018. Sie tritt mit Wirkung vom 28.04.2023 in Kraft und mit Ablauf des 28.04.2028 außer Kraft.

Berlin, den 28.04.2023
Die Präsidentin des Amtsgerichts Wedding