



| | | |
|---|--|--|
|  | <p>Gemeinde Uetze</p> <p>Dienstanweisung Informationssicherheit /KI</p> | <p>Version: 2.0 letzte Änderung: 25.08.2025</p> <p>Seite: 1 von 10</p> |
|---|--|--|

| Dokumenteninformation | | | | | |
|-----------------------|-----|--------------------------------|--------|-------------|---------|
| Dokumentenname: | | DA Informationssicherheit / KI | | | |
| | | | | | |
| Erstellt | | Geprüft | | Freigegeben | |
| Team 16 | | z.B. FBL I | | BM | |
| Version | 1.0 | Archivierung: G + 3 J. | | | |
| | | | | | |
| öffentlich | | extern | | intern | x |
| offen | x | vertraulich | | geheim | |
| | | | | | |
| Überprüfung bis: | | 31.10.2026 | durch: | | Team 16 |
| | | | | | |
| Bemerkungen | | | | | |

Inhalt

| | |
|---|---|
| Zweck..... | 2 |
| I. Allgemeines | 2 |
| 1. Geltungsbereich..... | 2 |
| 2. Allgemeine Maßnahmen | 2 |
| 3. Nutzungsberechtigung | 3 |
| 4. Nutzung von KI-Tools..... | 4 |
| 5. Verhalten bei Sicherheitsvorfällen..... | 4 |
| 6. Schutz von IT-Systemen gegen unberechtigten Zugang | 5 |
| II. E-Mail und Internet..... | 6 |
| 7. Nutzung | 6 |
| 8. Abonnieren von E-Mails | 7 |
| 9. Anlagen in Dateiform | 7 |
| 10. Zuständigkeiten..... | 7 |
| 11. Regelung bei Abwesenheit | 7 |
| 12. Löschung von E-Mails | 7 |
| 13. Download aus dem Internet..... | 7 |

| | | |
|---|--|--|
|  | <p>Gemeinde Uetze</p> <p>Dienstanweisung Informationssicherheit /KI</p> | <p>Version: 2.0 letzte Änderung: 25.08.2025</p> <p>Seite: 2 von 10</p> |
|---|--|--|

| | |
|---|----|
| III. Mobile Endgeräte..... | 8 |
| 14. Definition..... | 8 |
| 15. Schutz vor Diebstahl und unberechtigtem Zugang..... | 8 |
| 16. Speicherung dienstlicher Daten..... | 9 |
| 17. Datenschnittstellen und Peripheriegeräte..... | 9 |
| 18. Installation von Anwendungen auf mobilen Endgeräten | 10 |
| 19. Verhalten bei Verlust | 10 |
| 20. Schlussbestimmungen | 10 |

Zweck

Zweck der Dienstanweisung ist es, durch geeignete Vorgaben die Informationssicherheit im Betrieb der eingesetzten Hard- und Software sicherzustellen.

I. Allgemeines

1. Geltungsbereich


Diese Dienstanweisung gilt für alle Beschäftigten der Gemeinde Uetze.

2. Allgemeine Maßnahmen

(1) Alle Anwender*innen von IT-Systemen sind im Rahmen der ihnen übertragenen Aufgaben für den sicheren und rechtmäßigen Umgang mit diesen IT-Systemen verantwortlich.

(2) ¹Die Sicherheitseinstellungen von IT-Systemen dürfen nicht durch die Anwender*innen selbst verändert werden. Eventuell notwendige Anpassungen sind durch das Team IT-Service zu veranlassen bzw. vorzunehmen. ²Eine Umgehung von Sicherheitsmaßnahmen (z. B. Abschaltung des Virens scanners) ist untersagt.

(3) ¹Den Anwender*innen ist die Installation und der Einsatz von Computerprogrammen, welche nicht durch die Behördenleitung zur dienstlichen Nutzung bestimmt wurden (z. B. Downloads aus dem Internet, auf mobilen Datenträgern mitgebrachte Computerprogramme), auf den zur dienstlichen Nutzung bestimmten IT-Systemen grundsätzlich untersagt. ²Gleiches gilt für das eigenständige Umsetzen oder Tauschen von Soft- oder Hardwarekomponenten. ³Technische Eingriffe, insbesondere das Öffnen von Hardwarekomponenten, sind verboten.

| | | |
|---|--|--|
|  | <p>Gemeinde Uetze</p> <p>Dienstanweisung Informationssicherheit /KI</p> | <p>Version: 2.0 letzte Änderung: 25.08.2025</p> <p>Seite: 3 von 10</p> |
|---|--|--|

3. Nutzungsberechtigung

(1) ¹Die Speicherung von dienstlichen Informationen darf ausschließlich auf dienstlich bereitgestellten Datenträgern erfolgen. ²Dienstlich bereitgestellt werden ausschließlich verschlüsselte Datenträger (z. B. „sicherer USB-Stick“).

(2) ¹Ohne Verschlüsselung dürfen solche Informationen auf externen Datenträgern gespeichert werden, die öffentlich bekannt oder zur Veröffentlichung bestimmt sind. ²Auf eine Verschlüsselung kann in begründeten Ausnahmefällen verzichtet werden, wenn eine dienstlich notwendige Weitergabe an Dritte mit angemessenem Aufwand oder eine dienstlich notwendige Entgegennahme von Dritten auf anderem Wege nicht möglich ist. ³Ein Datentransfer mit unverschlüsselten Datenträgern darf ausschließlich an hierfür eingerichteten Übergabepunkten erfolgen.

(3) ¹Mobile Datenträger dürfen ausschließlich zum Transport dienstlicher Informationen und nicht zu deren dauerhafter Verwahrung verwendet werden. ²Die dauerhafte Aufbewahrung hat auf serverbasierten Speichersystemen zu erfolgen.

(4) Auf dem sicheren USB-Stick dürfen Daten

- a. bis zur Schutzstufe „D“ des Schutzstufenkonzepts des/r Landesbeauftragten für den Datenschutz in Niedersachsen,
- b. bis zur Schutzkategorie „hoch“ gemäß Nr. 3.7.2 der Informationssicherheitsleitlinie Niedersachsen (Nds. ISLL) oder
- c. des Geheimhaltungsgrades „VS – NUR FÜR DEN DIENSTGEBRAUCH“ gemäß Verschlusssachenanweisung des Landes Niedersachsen


transportiert werden.

(5) ¹Bei Verlust eines mobilen Datenträgers ist die Teamleitung zu informieren. ²Diese zeigt den Verlust beim Team IT-Service und bei dem/r ISB (Informationssicherheitsbeauftragten) an.

(6) ¹Daten, die durch Dritte auf einem externen Speichermedium bereitgestellt werden, dürfen ausschließlich an den Übergabepunkten (Absatz 2) auf die IT-Systeme der Gemeinde Uetze übertragen werden. ²Hierbei ist die Vertrauenswürdigkeit der Quelle zu überprüfen. ³Derartige Datenübertragungen sind auf das notwendige Mindestmaß zu beschränken.

(7) ¹Für die Übertragung von Präsentationen (z. B. externer Referent*innen) sind spezielle Notebooks zu verwenden, die einen Zugang in das interne Netzwerk nicht ermöglichen. ²Davon ausgenommen ist der Internet-Zugang.

(8) ¹Die Speicherung dienstlicher Daten außerhalb der IT-Systeme der Gemeinde Uetze ist nicht gestattet. ²Dies gilt insbesondere für Cloud-Services und ähnliche Online-Speicherdienste, soweit diese nicht Teil der IT-Infrastruktur der Gemeinde Uetze sind.

| | | |
|---|--|--|
|  | <p>Gemeinde Uetze</p> <p>Dienstanweisung Informationssicherheit /KI</p> | <p>Version: 2.0 letzte Änderung: 25.08.2025</p> <p>Seite: 4 von 10</p> |
|---|--|--|

4. Nutzung von KI-Tools

(1) Die Nutzung von KI-Tools ist ausschließlich zu dienstlichen Zwecken gestattet, insbesondere für:

- a. die Unterstützung bei der Erstellung von Texten, Zusammenfassungen oder Präsentationen,
- b. die Formulierungsvorschläge bei allgemeinen behördlichen Texten,
- c. die Strukturierung von Informationen oder die Verbesserung sprachlicher Verständigkeit,
- d. die automatisierte Unterstützung bei der Auswertung technischer Inhalte ohne personenbezogene Daten
- e. Für die Registrierung und Nutzung von KI-Tools zu dienstlichen Zwecken ist ausschließlich die dienstliche E-Mail-Adresse zu verwenden. Die Anmeldung mit privaten Accounts für dienstliche Anwendungen ist nicht gestattet.
 - Bei der Registrierung ist grundsätzlich die kostenfreie Nutzungslizenz auszuwählen, ausgenommen sind Mitarbeitende, die im Bereich Öffentlichkeitsarbeit und Social Media Marketing tätig sind und KI generierte Medien erstellen müssen.

(2) Die Verarbeitung folgender Inhalte in Zusammenhang mit der Nutzung von KI ist ausdrücklich untersagt:


- a. Personenbezogene Daten von Bürgerinnen und Bürgern, einschließlich sensibler Daten (z.B. Gesundheitsdaten, Adressdaten, Namen),
- b. Dienstliche Inhalte mit Schutz- oder Geheimhaltungsbedürfnis,
- c. Inhalte mit personenbezogenen Daten von Beschäftigten der Gemeinde
- d. Schützenswerte sowie vertrauliche oder hochsensible verwaltungsrelevante Informationen, insbesondere im Zusammenhang mit Sicherheitsbehörden, Sozialleistungen oder hoheitlichen Entscheidungen.

(3) Es darf keine automatisierte Entscheidungsfindung durch KI-Tools ohne menschliche Prüfung erfolgen. Die Anwender*innen tragen die Verantwortung für die durch KI generierten Inhalte und prüfen diese kritisch. Die sachgerechte Nutzung der Tools und die Aufklärung über die Risiken wird regelmäßig in geeigneter Weise durch die Dienststelle geschult. Die Teilnahme an einer solchen Schulung ist durch die Dienststelle zu dokumentieren.

5. Verhalten bei Sicherheitsvorfällen

(1) ¹Ein Sicherheitsvorfall ist ein unerwünschtes Ereignis, das eine Einschränkung oder den Verlust der Vertraulichkeit, Verfügbarkeit oder Integrität von Daten und Systemen nach sich ziehen kann. ²Insbesondere die folgenden Merkmale deuten auf das Vorliegen eines Sicherheitsvorfalls hin:

- a. Datenverlust ohne erkennbaren Grund

| | | |
|---|--|--|
|  | <p>Gemeinde Uetze</p> <p>Dienstanweisung Informationssicherheit /KI</p> | <p>Version: 2.0 letzte Änderung: 25.08.2025</p> <p>Seite: 5 von 10</p> |
|---|--|--|

- b. Sperrung von Nutzerkonten ohne erkennbaren Grund
- c. Meldungen des Virens scanners
- d. Systemmeldungen, die auf einen Missbrauch hinweisen
- e. Funktionsverlust von Programmen

(2) ¹Ein Sicherheitsvorfall oder ein dahingehender Verdacht ist von der Anwenderin oder dem Anwender unverzüglich der Teamleitung und dem Team IT-Service. Team IT Service informiert den ISB. ²Die Arbeit mit dem betroffenen Gerät bzw. Datenträger ist sofort einzustellen. ³Sofern Team IT-Service nicht erreicht werden kann ist das Gerät selbstständig von Netzwerk und von der Stromversorgung zu trennen. (Kabel ziehen oder drahtlose Verbindung trennen).

6. Schutz von IT-Systemen gegen unberechtigten Zugang

(1) ¹IT-Geräte sind in der Regel durch ein Passwort gegen unberechtigten Zugang gesichert. ²Die Anwenderinnen und Anwender haben bei Verlassen des Arbeitsplatzes ihre IT-Geräte zu sperren, sodass ein erneuter Zugang zum IT-Gerät nur mittels eines Passwortes möglich ist. ³Zusätzlich erfolgt eine automatische Sperrung des IT-Geräts nach spätestens 15 Minuten. ⁴Sofern sich keine Person in den Diensträumen aufhält, sind diese beim Verlassen abzuschließen


(2) Insbesondere in Bereichen mit Publikumsverkehr sind Monitore, Drucker und Faxgeräte so aufzustellen, dass das Risiko einer Einsichtnahme Dritter möglichst ausgeschlossen ist.

(3) ¹Die Weitergabe von Benutzerkennungen und Passwörtern ist unzulässig. ²Dies gilt auch für die Weitergabe im unmittelbaren Kolleg*innenkreis. ³Dies gilt nicht, soweit es sich um eine berechtigte Weitergabe von Funktionskennungen und korrespondierender Passwörter handelt. ⁴Passwörter dürfen nur an besonders gesicherten und nur für die oder den Berechtigten zugänglichen Stellen notiert oder in anderer Weise abgelegt werden.

(4) Aktivierungs- oder Einrichtungspasswörter sind unverzüglich durch den/die Anwender*in in ein persönliches Passwort zu ändern.

(5) Passwörter haben in Ihrer Zusammensetzung mindestens den folgenden Anforderungen zu entsprechen:

- a. Die Länge beträgt mindestens acht Stellen.
- b. Ein Passwort setzt sich aus Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen zusammen und enthält mindestens jeweils ein Zeichen aus drei der genannten Zeichengruppen.
- c. Leicht zu erratende und damit unsichere Passwörter sind zu vermeiden. Unsicher sind insbesondere: häufige Zeichenwiederholungen, Zeichen, die durch nebeneinanderliegende Tasten eingegeben werden, Zeichenkombinationen, die Suchbegriffen in Wörterbüchern und Lexika entsprechen, Zahlen und Daten aus dem Lebensbereich des/r jeweiligen Anwender*in.

| | | |
|---|--|--|
|  | <p>Gemeinde Uetze</p> <p>Dienstanweisung Informationssicherheit /KI</p> | <p>Version: 2.0 letzte Änderung: 25.08.2025</p> <p>Seite: 6 von 10</p> |
|---|--|--|

(6) Passwörter sollen spätestens nach 180 Tagen geändert werden.

II. E-Mail und Internet

7. Nutzung


(1) ¹Die IT-Systeme werden allen Anwender*innen zur Verfügung gestellt. ²Die mit dem Anschluss von Arbeitsplatz-PCs an das Internet und Vergabe von E-Mail-Adressen geschaffenen technischen Informations- und Kommunikationsmöglichkeiten sowie sämtliche IT-Systeme dürfen nur zu dienstlichen Zwecken genutzt werden. ³Eine private Nutzung ist ausdrücklich untersagt.

(2) ¹Eine Verwendung privater Hard- und Software zu dienstlichen Zwecken durch den/die Anwender*in ist untersagt. ²Dies gilt insbesondere für die Speicherung dienstlicher Daten auf privaten Geräten. ³Die Verbindung privater Geräte mit der Netzinfrastruktur der Gemeinde Uetze ist nicht gestattet.

(3) ¹Anwender*innen haben darauf zu achten, dass aufgerufene Webinhalte vertrauenswürdig sind. Neben einer automatischen Filterung von unerwünschten Inhalten nehmen die Mitarbeiter*innen auch in eigener Verantwortung die Prüfung der Webseiten auf Vertrauenswürdigkeit vor. ²Dies gilt insbesondere, falls die Ausgabe von Daten die dienstliche E-Mail-Adresse bzw. der Daten der Mitarbeiter vorausgesetzt. ³Anhaltspunkte für nicht vertrauenswürdige Webseiten können zudem ein unerwartetes Herkunftsland oder die Endung einer Webadresse (z.B. „.ru“, „.to“) sein.

(4) Anwender*innen achten darauf, dass eingegangenen E-Mails vertrauenswürdig sind. Bei E-Mails von unbekannten Absendern ist das Klicken auf Links innerhalb des Texts zu vermeiden, da diese gefälscht sein könnten. Im Zweifelsfall sind Links in die Adresszeile des Browsers einzugeben. Geheime Daten wie Passwörter dürfen nicht nach dem Aufruf eines Links aus einer E-Mail eingegeben werden. Auch Anhänge von unbekannten Absendern dürfen nicht geöffnet werden, ohne sich zuvor über deren Vertrauenswürdigkeit zu vergewissern. Spam-E-Mails sind aus den Postfächern zu löschen.

(5) ¹Vor dem Versand einer E-Mail ist die Empfängeradresse/Empfängerliste auf Korrektheit zu überprüfen. Beim Versenden von E-Mails an Externe sind die personenbezogenen E-Mail-Adressen grundsätzlich in das Feld „bcc“ einzutragen, sofern keine Einwilligung zur Veröffentlichung vorliegt. ²In die Nachricht ist ein Hinweis auf den Verteilerkreis aufzunehmen, soweit sich dieser nicht bereits aus dem Inhalt ergibt. ³Wenn versehentlich eine E-Mail an einen falschen Adressaten gesendet wurde, ist dieser unverzüglich über die fälschlich übermittelte E-Mail zu informieren und zur Löschung der E-Mail aufzufordern. ⁴Besteht die Gefahr von negativen Folgen durch den versehentlichen Versand, ist unverzüglich die unmittelbare Führungskraft zu informieren und alle notwendigen Maßnahmen zur Begrenzung des Schadens einzuleiten.

| | | |
|---|--|--|
|  | <p>Gemeinde Uetze</p> <p>Dienstanweisung Informationssicherheit /KI</p> | <p>Version: 2.0 letzte Änderung: 25.08.2025</p> <p>Seite: 7 von 10</p> |
|---|--|--|

8. Abonnieren von E-Mails

Das Abonnieren von E-Mails über Mailing-Listen (Newsletter) darf nur zu dienstlichen Zwecken erfolgen und muss in jedem Fall auf das unbedingt notwendige Maß beschränkt werden.

9. Anlagen in Dateiform

(1) ¹Aus Sicherheitsgründen sind nur die folgenden Dateiformate in der E-Mail-Übertragung zulässig: *.docx; *.xlsx; *.pdf; *.txt; *.jpg. ²Andere Formate – insbesondere ausführbare Dateien – werden gefiltert.

(2) Das Versenden von besonders schutzwürdigen personenbezogenen Daten in unverschlüsselter Form ist untersagt.

10. Zuständigkeiten

¹Die notwendige zentrale Steuerung der elektronischen Postdienste wird wie die technische Abwicklung durch den Fachbereich I – Zentrale Dienste – wahrgenommen. ²Das Neuanlegen bzw. die Änderung von bestehenden E-Mailadressen und von fachbereichsbezogenen Freigaben wird vom Team IT-Service ausschließlich durch Auftrag von Team Organisation durchgeführt. ³E-Mail-Verteilerguppen werden direkt durch das Team Organisation angepasst. ⁴Die Funktionspostfächer werden vom Team IT-Service nach Auftrag von Team Organisation angelegt und verwaltet. ⁵Nicht mehr benötigte Postfächer, Veränderungen etc. sind von den Fachbereichen und Teams unaufgefordert an das Team IT-Service zu melden.

11. Regelung bei Abwesenheit


¹Grundsätzlich besteht eine Dokumentationspflicht dienstrelevanter Vorgänge auch im E-Mail-Verkehr. ²Bei geplanten Abwesenheiten ist gemäß der Amtsverfügung Organisation entweder eine Weiterleitung oder aber der Abwesenheitsassistent aktiv einzurichten. ³Darüber hinaus kann jederzeit eine anlassbezogene Einsichtnahme durch die Dienststelle erfolgen; insbesondere bei unerwartet längerer Abwesenheit eines/r Mitarbeiter*in. ⁴Hierüber sind der Personalrat sowie der/die Datenschutzbeauftragte und der/die Datenschutzkoordinator*in zu unterrichten.

12. Löschung von E-Mails

¹Elektronische Post soll innerhalb der E-Mail-Software nur solange gespeichert werden, wie dies für die Aufgabenerledigung erforderlich ist. ²Nicht mehr benötigte E-Mails sind unverzüglich zu löschen. ³Soll die Post längerfristig elektronisch aufbewahrt werden, ist sie als Datei im Dokumentenmanagementsystem (DMS) zu speichern bzw. zu archivieren.

13. Download aus dem Internet

Das Herunterladen bzw. der Download von aktiven Programmen (z.B. Anwendungen, Apps,

| | | |
|---|--|--|
|  | <p>Gemeinde Uetze</p> <p>Dienstanweisung Informationssicherheit /KI</p> | <p>Version: 2.0 letzte Änderung: 25.08.2025</p> <p>Seite: 8 von 10</p> |
|---|--|--|

Skripte) und Dateien (z.B. Dateien mit der Endung *.bat, *.com, *.cmd, *.scr, *.exe) aus dem Internet ist, aufgrund der damit verbundenen sicherheitsrelevanten Aspekte, dem Team IT-Service vorbehalten. Dateien mit den Endungen *.docx, *.xlsx, *.pptx, *.jpg oder *.pdf dürfen heruntergeladen werden. Bei Unsicherheiten bzgl. der Datei oder der Webseite, ist das Team IT-Service über die bekannten Kanäle „Hotline“ oder „Email-Adresse“ zu kontaktieren.

III. Mobile Endgeräte

14. Definition

Mobile Endgeräte i. S. dieser Dienstanweisung sind informationstechnische und kommunikationstechnische Geräte, die aufgrund ihrer Größe und ihres Gewichts ohne größere körperliche Anstrengung tragbar und somit mobil einsetzbar sind. Hierzu zählen insbesondere

- a) Mobiltelefone ohne Datenanbindung
- b) Mobiltelefone mit Datenanbindung (Smartphones)
- c) Tablet-Computer (z.B. iPad und Surface) und
- d) Notebooks.

Die Verwendung eines privaten mobilen Endgerätes zur Führung dienstlicher Telefonate in Ausnahmefällen ist keine dienstliche Nutzung i. S. dieser Dienstanweisung.

15. Schutz vor Diebstahl und unberechtigttem Zugang


(1) ¹Mobile Endgeräte sind von den Anwender*innen sicher aufzubewahren, um einen Zugang von Dritten zu verhindern. ²Das Endgerät darf z. B. nicht sichtbar und unbeaufsichtigt liegen gelassen werden.

(2) Bei einem nicht nur kurzzeitigen Gebrauch eines mobilen Endgerätes in einer offen zugänglichen Umgebung ist das Gerät, soweit technisch möglich, physisch zu sichern.

(3) ¹Mobile Endgeräte dürfen von den Anwender*innen nicht an Dritte weitergegeben werden. ²Dies gilt auch für eine nur kurzzeitige Weitergabe.

(4) ¹Anderen Bediensteten der Gemeinde Uetze darf von den Anwender*innen kurzzeitig der physische Zugang zum mobilen Endgerät gewährt werden, soweit hierfür eine dienstliche Notwendigkeit besteht. ²Der/Die verantwortliche Anwender*in hat dabei das mobile Endgerät ständig zu überwachen. ³Bei einer Weitergabe an das Team IT-Service für etwaige Wartungsarbeiten oder Updates bedarf es keiner ständigen Überwachung. ⁴Ausgenommen hiervon ist die Weitergabe des mobilen Endgerätes im Rahmen der Durchführung eines Rufbereitschaftsdienstes.

(5) ¹Eine Weitergabe an Dritte ist ausnahmsweise gestattet, wenn die Mitführung eines mobilen Endgerätes beim Zugang zu einer Einrichtung nicht gestattet ist und eine Lagerung beim

| | | |
|---|--|--|
|  | <p>Gemeinde Uetze</p> <p>Dienstanweisung Informationssicherheit /KI</p> | <p>Version: 2.0 letzte Änderung: 25.08.2025</p> <p>Seite: 9 von 10</p> |
|---|--|--|

Pförtner oder Sicherheitsdienst dieser Einrichtung vorgesehen ist. ²Eine Weitergabe ist nur bei vertrauenswürdigen Organisationen gestattet. ³Das Gerät ist vor der Weitergabe stets auszuscha-
alten.

(6) ¹Das Endgerät muss durch ein Passwort bzw. PIN geschützt werden. Diese müssen mindestens 4 Stellen, sofern technisch möglich, 6 Stellen umfassen. ²Die Passwortabfrage ist bei jedem Entsperren (Aufheben der Tastensperre) erforderlich und kann durch biometrische Funktionen unterstützt werden.

16. Speicherung dienstlicher Daten

(1) ¹Der Umfang der auf dem mobilen Endgerät gespeicherten Daten ist von den Anwender*innen möglichst gering zu halten. ²Zu diesem Zweck ist die Notwendigkeit des Datenbestandes auf dem Gerät regelmäßig zu überprüfen. ³Nicht länger in der mobilen Anwendung benötigte Daten sind zu löschen. ⁴Dies schließt auch den synchronisierten Datenbestand des E-Mail-Postfachs und des Kalenders ein.

(2) Auf mobilen Endgeräten dürfen Daten

- a. bis zur Schutzstufe C gemäß Schutzstufenkonzept der/dem Landesbeauftragten für den Datenschutz,
- b. bis zur Schutzkategorie „hoch“ gemäß Nummer 3.7.2 der ISLL oder
- c. des Geheimhaltungsgrades „VS - NUR FÜR DEN DIENSTGEBRAUCH“ gemäß Verschlusssachenanweisung des Landes Niedersachsen


vorübergehend gespeichert werden, soweit diese Daten durch Verschlüsselung gesichert sind.

17. Datenschnittstellen und Peripheriegeräte

(1) ¹Drahtlose Datenschnittstellen wie Wireless-LAN oder Bluetooth dürfen durch die Anwenderin oder den Anwender ausschließlich bei einem konkreten Bedarf aktiviert werden. ²Sofern es sich um unverschlüsselte Schnittstellen handelt, dürfen Sie nur genutzt werden, um anschließend eine VPN-Verbindung zur Gemeinde Uetze aufzubauen, so dass der Datenverkehr über eine geschützte Verbindung läuft. ³Sollten diese Schnittstellen nicht mehr benötigt werden, sind diese unverzüglich wieder zu deaktivieren. ⁴Hiervon ausgenommen ist die Verbindung mit einem Mobilfunknetz (GSM, UMTS, LTE).

(2) Eine drahtgebundene oder drahtlose Verbindung eines mobilen Endgerätes mit einem Partnergerät (z. B. anderes mobiles Endgerät, Headset, Drucker) darf ausschließlich mit vertrauenswürdigen Partnergeräten erfolgen.

(3) ¹Sollte zur Kopplung mit einem Partnergerät über Bluetooth die „Sichtbarkeit“ des Bluetooth-Adapters notwendig sein, ist dieser als „vorübergehend sichtbar“ zu konfigurieren. ²Die Pflicht zu einer unverzüglichen Deaktivierung des Adapters nach Beendigung der Anwendung bleibt unberührt.

| | | |
|---|--|---|
|  | <p>Gemeinde Uetze</p> <p>Dienstanweisung Informationssicherheit /KI</p> | <p>Version: 2.0 letzte Änderung: 25.08.2025</p> <p>Seite: 10 von 10</p> |
|---|--|---|

(4) Die Pflichten gemäß den Absätzen (1) und (3) bestehen nur, wenn die Anwender*innen beim eingesetzten Gerät auch die tatsächliche Möglichkeit zur Umsetzung haben.

18. Installation von Anwendungen auf mobilen Endgeräten

(1) ¹Auf Smartphones und Tablet-Computern können mobile Anwendungen (Apps) ausschließlich aus dem „Uetze AppPortal“ installiert werden. Für weitere Apps muss eine Genehmigung über die Teamleitung an das IT-Services Team gestellt werden. Nach der Prüfung wird die App im „Uetze AppPortal“ aufgenommen.

²Die Installation und Nutzung von WhatsApp auf dienstlichen Smartphones und Tablet-Computern ist ausdrücklich untersagt.

(2) Die zugelassenen Apps sind im „Uetze App-Portal“ auf den Smartphones und Tablets einsehbar und dürfen installiert werden.

19. Verhalten bei Verlust

¹Bei Verlust eines mobilen Endgerätes, einer Speicherkarte oder einer SIM-Karte sind unverzüglich das Team IT-Service sowie die oder der Vorgesetzte zu informieren. ²Von dort erfolgt eine Information an den/die ISB. ³Dies gilt auch, falls das Gerät wiederaufgefunden wird. **20.**

20. Schlussbestimmungen

Diese Dienstanweisung tritt am 01.10.2025 in Kraft und ersetzt die vorhergehende Fassung.

Sollten einzelne Punkte dieser Dienstanweisung ungültig sein oder ihre Gültigkeit aufgrund neuer Gesetzgebung oder Rechtsprechung verlieren, so bleiben die übrigen Bestimmungen hiervon unberührt und weiterhin in Kraft.

Uetze, 30.09.2025

Florian Gahre
Bürgermeister