Benutzung der IT-Systeme

Stand 08/2024

Ziel und Zweck dieser Anweisung

Diese Anweisung legt Regeln **(R)** für die Benutzung von IT-Systemen und die Anwendung von Software-Produkten für alle Nutzer von Gasunie Deutschland (GUD) IT-Systemen verbindlich fest. Sie sind aus der „Informationssicherheitsleitlinie" und der Anweisung „Sicherheit der Informationsverarbeitung" abgeleitet und Bestandteil der Informationssicherheitsdokumentation.

1. Begriffe

Begriff	Definition / Erklärung
Benutzer	Personen mit Zugangsrechten für ein IT–System
IT-Betriebsfunktion	Über die jeweilige Ansprechperson für Office IT, Prozess IT und WAN/PDÜ sowie für betriebliche Offline-Systeme gibt die vertragliche Ansprechperson bei GUD Auskunft.
IT-System	Alle IT-Einrichtungen, sowohl zentrale und dezentrale Hardware wie auch Software
IT-Equipment	Desktop-PC bzw. Tablet-PC, GUD-Smartphone, Wechselspeichermedium, Schlüssel (physisch und elektronisch), usw.
Wechselspeichermedium	z. B. CD-ROMs, DVDs, USB-Sticks, USB-Festplatten
Onsite Support (OSS)	Mitarbeiter des IT-technischen Vor-Ort-Services der Office IT
Service Desk / Meldestelle	Zentrale Anlaufstelle für alle Fragen der Nutzung von IT-Systemen der Office IT: Erreichbarkeit bei der GUD Ansprechperson zu erfragen

2. Zuständigkeiten und Verantwortlichkeiten

Jede Person, die IT-Systeme der GUD nutzt, hat dies unter Anwendung der in dieser Anweisung beschriebenen Regeln durchzuführen. Es ist Aufgabe der zuständigen Auftragnehmerorganisationen, die Einhaltung der Regeln in angemessener Weise zu kontrollieren. Die Regelungen dieser Anweisung sind gemäß Nr. 24 (Nutzung der IT-Systeme) und Nr. 23 (IT-Sicherheit) Bestandteil der vertraglichen Regelungen mit GUD.

Da technische Schutzmaßnahmen und organisatorische Regelungen allein jedoch nicht ausreichen, um IT-Systeme zu schützen, ist informationssicherheitsbewusstes Handeln eines jeden Benutzers erforderlich.

3. Umgang mit Daten

3.1 Umgang mit Informationen

R1 Daten und Informationen sind vor Einsichtnahme Unberechtigter, vor Zerstörung, Verlust und unberechtigter oder versehentlicher Veränderung zu schützen.

3.2 Geheimhaltung

Die in Nr. 16 (Vertraulichkeit) der GUD Einkaufsbedingungen aufgeführte Verpflichtung zur Wahrung von Geschäfts- und Betriebsgeheimnissen erstreckt sich auch auf Informationen, die in elektronischer Form gespeichert werden.

R2 Für Zwecke, die nicht unmittelbar im Beauftragungsverhältnis zur GUD notwendig sind, dürfen keine Datenträger bzw. Wechselspeichermedien, Ausdrucke mit Geschäftsinformationen etc. aus den Räumen der GUD herausgebracht und auch keine Daten über andere Übertragungswege (z.B. E-Mail) an Empfänger außerhalb der GUD versendet werden.

3.3 Schutz personenbezogener Daten

R3 Für die Verarbeitung und Speicherung personenbezogener Daten ist Nr. 22. (Datenschutz) der Einkaufsbedingungen zu beachten.

3.4 Speicherung von Daten

R4 GUD-Daten sind auf den von GUD vorgegebenen zentralen Systemen der GUD zu speichern.

Diese Ablageorte ermöglichen für einen begrenzten Zeitraum eine Wiederherstellung der Daten.

3.5 Klassifizierung von Informationen

Da nicht alle Informationen den gleichen Schutzbedarf haben, werden Informationen bei GUD in vier Klassen hinsichtlich der Schutzziele „Vertraulichkeit", „Integrität" und „Verfügbarkeit" eingestuft. Für die Durchführung der Klassifizierung ist der Eigentümer der Information zuständig. Sofern nicht explizit ein Eigentümer der Information bestimmt wurde, ist die erstellende Person der Informationen Eigentümer (genannt Informationseigentümer oder auch Dateneigentümer). Bei der Klassifizierung von Informationen unterstützt die Ansprechperson bei GUD.

Klasse IV: Offene Informationen

Klasse III: Interne Informationen

Klasse II: Vertrauliche Informationen

Klasse I: Geheime Informationen

R5 Verantwortlich für die Klassifizierung von Daten ist immer der Informationseigentümer.

Die Standardeinstufung für Daten hinsichtlich der Vertraulichkeit bei GUD ist die Klasse III (intern), für die die standardmäßig in den Systemen eingestellten Sicherheitsmaßnahmen ausreichen

R6 Daten der Klasse II (vertraulich) und der Klasse I (geheim) dürfen nur an festgelegten Ablageorten gespeichert werden. Müssen entsprechende Daten für GUD gespeichert werden, ist die GUD-Ansprechperson darüber in Kenntnis zu setzen. Sie wird Auskunft geben, wo und unter welchen Bedingungen die Speicherung erfolgen kann.

3.6 Ausdrucken von Daten

R7 Nicht zugangsgeschützte Ausdrucke auf Netzwerk-Druckern sind unverzüglich abzuholen.

R8 Vertrauliche und geheime Ausdrucke dürfen nur auf zugangsgeschützten Druckern oder mit einem Code gesichert ausgedruckt werden.

3.7 Löschen/ Vernichten von Informationen in Systemen, auf Geräten oder auf Wechselspeichermedien

R9 Bei Löschung geheimer Daten ist die GUD Ansprechperson zu kontaktieren. Sie wird Auskunft geben, wie die Löschung erfolgt.

R10 R9 gilt auch für Datenträger, auf denen geheime Daten gespeichert waren oder sind.

R11 Datenträger mit vertraulichen Daten sind durch speziell zertifizierte Unternehmen zu entsorgen.

Für CDs und DVDs stehen Entsorgungstonnen bei GUD zur Verfügung. Von GUD bereitgestellte USB-Sticks sind über die GUD-Ansprechperson zurückzugegeben.

4. Systemzugang und Zugriffsrechte

4.1 Benutzerkonto, Benutzername, Authentifizierung

R12 Kennwörter für Benutzerkonten sind unbedingt geheim zu halten. Es ist nicht gestattet, das eigene Benutzerkonto einer anderen Person zur Verfügung zu stellen oder mit dem Benutzerkonto einer anderen Person zu arbeiten.

Zur Anmeldung an den GUD-Systemen aus dem Internet sowie für einige Betriebs- und Anwendungssysteme sind zusätzlich zu Benutzernamen und dem Passwort noch weitere Authentifizierungen (Nachweis der Identität) erforderlich, z.B. durch einen sog. Software-Token.

R13 Die Installation von Apps zur Erzeugung von Software Token für den Zugang zu GUD Systemen ist grundsätzlich auf allen Geräten gestattet. Eine Installation der Token auf einem Gerät ist jedoch nicht zulässig, wenn dasselbe Gerät auch für den Zugang zu dem jeweiligen GUD-System, für den der Token als 2. Faktor dient, genutzt wird.

R14 Alle Authentifizierungsmittel sind sicher und unzugänglich für Dritte aufzubewahren.

4.2 Anforderungen an Kennwörter

R15 Ein persönliches Kennwort muss unabhängig vom System (auch in Online-Portalen) bestimmte Bedingungen erfüllen, um eine ausreichende Sicherheit zu gewährleisten. Sofern technisch möglich, muss es

- mindestens 12 Zeichen enthalten – eine Mischung aus 4 verschiedenen Zeichenarten, Klein/ und Großbuchstaben, Sonderzeichen (z.B. $, _, #) und Ziffern (0, .., 9).
- sich von den in der Vergangenheit verwendeten Kennwörtern unterscheiden.

Können die bei GUD gültigen Kennwortregeln aus technischer Sicht nicht eingehalten werden, ist ein Kennwort so stark wie technisch möglich zu definieren.

R16 Der Benutzer hat sicherzustellen, dass

- die Kennwörter nicht auf Sachverhalten basieren, die eine andere Person unter Zuhilfenahme personenbezogener Daten wie z. B. Namen, Telefonnummern, Geburtstagen einfach erraten oder erschließen kann,
- die Kennwörter nicht anfällig für Wörterbuchangriffe sind (d.h. nicht aus Wörtern bestehen, die in Wörterbüchern stehen),
- die Kennwörter keine Folge identischer, numerischer oder alphanumerischer Zeichen enthalten (z.B. 1234 oder asdf),
- dieselben Kennwörter nicht für unterschiedliche Zwecke bzw. Accounts verwendet werden,
- die Kennwörter nicht unverschlüsselt notiert oder gespeichert werden,
- die Kennwörter nicht an unberechtigte Personen weitergegeben werden,
- die Kennwörter umgehend geändert werden, wenn sie in fremde Hände gelangt sein könnten.
- die von Administratoren gesetzten Initialkennwörter sofort geändert werden und
- die Kennwörter mindestens einmal jährlich geändert werden.

R17 Sofern die Möglichkeit einer Zwei-Faktor-Authentifizierung angeboten wird, so ist diese zwingend zu nutzen.

4.3 Beantragung von Benutzerrechten

Für die Verwendung von Anwendungen und Daten (Ressourcen) werden Berechtigungen benötigt. Diese werden nach Arbeitsnotwendigkeit vergeben und müssen für die jeweilige Ressource beantragt werden. Dazu stehen entsprechende Portale, der Service Desk bzw. sonstige Ansprechpersonen zur Verfügung. Für die Beantragung ist die GUD-Ansprechperson direkt zu kontaktieren.

5. Technische und physische Schutzmaßnahmen

5.1 Sicherung des IT-Arbeitsplatzes

R18 Beim Verlassen des Arbeitsplatzes, auch kurzzeitig, ist die Bildschirmsperre des jeweiligen IT-Equipments manuell zu aktivieren.

R19 Das von GUD genutzte IT-Equipment an den einzelnen Arbeitsplätzen ist grundsätzlich bei längerer Abwesenheit, z.B. nach Feierabend, auszuschalten und die Verbindungen zu den GUD-Systemen durch „ABMELDEN" zu trennen.

5.2 Sicherung des IT-Arbeitsplatzes an den Offlinesystemen betrieblicher Standorte

Zur Sicherung des IT-Arbeitsplatzes in den Messwarten der betrieblichen Standorte ist eine Zutrittsregelung umgesetzt.

R20 Jede zutrittsberechtigte Person muss durch konsequentes Beachten der Zutrittsregelung sicherstellen, dass nur Befugte die Messwarte sowie die Technikräume, in denen sich IT-Systeme befinden, betreten können.

5.3 Sicherung von Datenträgern und mobilen Endgeräten

R21 Von GUD bereitgestellte mobile Endgeräte sind bei längerer Abwesenheit (z.B. nach Feierabend) zu verschließen.

Für Tablet-PCs und Notebooks stehen abschließbare „Docking-Stations" bzw. Sicherheitskabel zur Verfügung.

R22 Von GUD bereitgestellte mobile Endgeräte sind an öffentlichen Orten (z.B. Straßenbahn, Zug, Flughafen etc.) zu beaufsichtigen.

R23 In einem öffentlich geparkten PKW ist IT-Equipment (i. d. R. mobile Geräte), wenn überhaupt nötig und nur im Ausnahmefall, so aufzubewahren, dass sie weder direkt noch erkennbar in einer Tasche offen sichtbar sind, z.B. im verschlossenen Kofferraum.

5.4 Verlust von IT-Equipment

R24 Im Falle des Verlusts von IT-Equipment der GUD, ist umgehend der Service Desk zu informieren.

5.5 Virenschutz

5.5.1 Virenschutz von Rechnern

R25 Zum Schutz vor Schadsoftware dürfen die auf den Rechnern installierten Virenscanner auf keinen Fall deaktiviert werden.

R26 Zusätzlich zu der mindestens jährlichen Überprüfung muss an den betrieblichen Offlinesystemen nach Systemveränderungen wie Softwareupdates, etc. (zum Beispiel in Rahmen von Umbauten oder Wartungsmaßnahmen) eine Virenüberprüfung durchgeführt werden.

5.5.2 Verbreitung von Schadprogrammen per E-Mail

R27 Anhänge und Links in E-Mails von unbekannten Absendern dürfen auf keinen Fall ungeprüft geöffnet werden. Wenn die Nachricht wichtig erscheint, ist beim Absender vor dem Öffnen des Anhangs der Hintergrund der E-Mail zu erfragen.

R28 Anhänge und Links in E-Mails von bekannten Absendern, aber mit ungewöhnlichem Inhalt sind ebenfalls nicht ungeprüft zu öffnen.

Die GUD-Ansprechperson kann u. a. mit Checklisten hierzu unterstützen. Bei Zweifeln ist der Service Desk telefonisch zu kontaktieren bzw. bei Zugriff auf die GUD IT-Systeme die E-Mail als Phishing oder SPAM mittels Phishing/SPAM-Button („Hoxhunt") zu melden.

5.5.3 Warnhinweise zu Schadprogrammen

R29 Warnhinweise und Anweisungen zu Schadprogrammen, die von der GUD unter dem Absender „Virenwarnung" oder „Virenalarm" per E-Mail versendet werden, sind unbedingt zu beachten! Gleiches gilt für entsprechende Warnungen von der GUD-Ansprechperson.

6. Datenaustausch und Datenübertragung

6.1 Nutzung von E-Mails

R30 Das E-Mail-System der GUD ist ausschließlich für den geschäftlichen Gebrauch im Rahmen der von GUD ausgesprochenen Beauftragung bestimmt.

R31 Vor dem Versenden einer E-Mail ist immer die Richtigkeit der E-Mail-Adresse des Empfängers zu überprüfen.

R32 Bei der Weiterleitung von empfangenen E-Mails sind Festlegungen bzgl. der Vertraulichkeitsstufe zu beachten.

R33 Vertrauliche oder geheime Daten dürfen nur verschlüsselt an externe Empfänger versendet werden. Geheime Daten sind auch innerhalb der GUD bei der Versendung per E-Mail zu verschlüsseln. E-Mails mit vertraulichem oder geheimen Inhalt sind zudem entsprechend zu kennzeichnen.

R34 Bei der Freigabe des eigenen E-Mail Postfachs sowie des Outlook-Kalenders für eine Vertretung ist sicherzustellen, dass die Anforderungen an die Vertraulichkeit der enthaltenen Informationen gewahrt bleiben.

R35 Eine Weiterleitung dienstlicher E-Mails oder Dokumente an weitere E-Mail Postfächer ist nicht gestattet.

6.2 Verschlüsselung von Daten

R36 Die Verschlüsselung von vertraulichen oder geheimen Daten ist unter Beachtung der Vorgaben für Kennwörter nach dem AES-256-Verfahren mit dem Programm 7-Zip durchzuführen, das allen GUD-Benutzern zur Verfügung steht.

6.3 Nutzung von Wechselspeichermedien

R37 Wechselspeichermedien dürfen nur in Ausnahmefällen genutzt werden. Sollte in Ausnahmefällen die Nutzung eines Wechselspeichermediums notwendig sein, so sind grundsätzlich nur von GUD ausgegebene Wechselspeichermedien zu verwenden. Diese dürfen nur für dienstliche Zwecke genutzt werden.

R38 Auf Wechselspeichermedien sollten grundsätzlich nur „offen" oder „intern" klassifizierte Informationen gespeichert werden. Sie sind jederzeit sorgfältig zu verwahren, so dass ein unbefugter Zugriff auf die gespeicherten Informationen nicht möglich ist. Bei postalischem Versand ist vorher die GUD-Ansprechperson zur Klassifizierung von Informationen zu kontaktieren.

R39 Im Falle des Verlustes eines Wechselspeichermediums ist umgehend die GUD-Ansprechperson zu informieren.

6.3.1 Nutzung von Wechselspeichermedien zum Datenaustausch

R40 Datenaustausch mit externen bekannten Geschäftspartnern sollte grundsätzlich via E-Mail oder über eine sichere Datenaustauschplattform (siehe 6.3.2) erfolgen.

R41 Sollte die Notwendigkeit bestehen, Wechselspeichermedien mit bekanntem Inhalt externer bekannter Geschäftspartner zu verwenden, so ist vor der Verwendung ein Antivirus-Scan vorzunehmen, wobei die Überprüfung (auch der Wechselspeichermedien von Kontraktoren) grundsätzlich nur durch GUD-Mitarbeitende erfolgen darf.

R42 Falls bei einem Wechselspeichermedium Malware detektiert wird, darf dieses nicht verwendet werden.

R43 Die Nutzung von Wechselspeichermedien aus unbekannter Quelle oder mit unbekanntem Inhalt ist nicht gestattet.

R44 Die Verwendung von GUD-Wechselspeichermedien an potenziell unsicheren Rechnern (z.B. in Internetcafes, Hotel-PCs etc.) ist nicht erlaubt.

6.3.2 Austausch von Datenmengen über eine Datenplattform

Für den Austausch von Datenmengen kann im Bedarfsfall die Einrichtung einer sicheren Datenaustauschplattform beantragt werden. Die GUD-Ansprechperson ist in diesem Fall zu kontaktieren.

6.4 Internetnutzung

R45 Der Internetzugang bei GUD ist für dienstliche Zwecke bestimmt.

R46 Es dürfen keine Informationen mit rechtswidrigen oder sittenwidrigen Inhalten genutzt und verbreitet werden.

R47 Die Nutzung sozialer Netzwerke (z. B. Facebook, Xing, Linkedin) ist zu unterlassen.

R48 Websites werden unter bestimmten Randbedingungen durch die IT-Systeme der GUD blockiert. Sollte bei anzunehmender Seriosität des Websiteanbieters bei gleichzeitigem dienstlichem Zweck die Nutzung einer blockierten Website notwendig sein, ist dies über den Service Desk anzufordern.

R49 Es dürfen keine Programme und Apps aus dem Internet heraus ausgeführt oder aus dem Internet heruntergeladene Programme und Apps ohne Einschalten der Office IT installiert werden. Hiervon ausgenommen ist das Ausführen von Webkonferenzdiensten (z.B. WebEx, Zoom, Go to meeting etc.).

R50 Bei der Weiterverwendung von Informationen aus dem Internet .(inklusive KI-generierte Texte) z.B. eigenen Texten sind das Urheberrecht und entsprechende Hinweise auf der Quellseite im Internet zu beachten.

R51 Nachrichten und Informationen, die in das Internet eingebracht werden, z.B. über Diskussionsforen oder Feedback-Formulare, dürfen nur als „offen" klassifizierte Informationen enthalten.

R52 Bei der Nutzung von frei zugänglichen Online-Übersetzungsdiensten für ganze Textpassagen (z.B. Google Translator, DeepL, etc.) oder KI-basierte Textgeneratoren wie ChatGPT dürfen nur Texte, die als „offen" klassifiziert sind, an diese Dienste übermittelt werden.

R53 Geheime Daten dürfen nicht in Online-Diensten verarbeitet werden.

7. Nutzung von Web-Cams, Videotelefonie oder Videokonferenzsystemen und Telefonkonferenzen

R54 Eine Web-Cam ist so zu platzieren, dass andere Personen nicht zufällig in das Übertragungsfeld der Web-Cam treten.

R55 Es ist grundsätzlich untersagt, Telefonkonferenzen aufzunehmen oder Videokonferenzen aufzuzeichnen.

Ausnahmen hiervon kommen in Betracht, wenn z.B. Vorträge oder Schulungen aufgezeichnet werden, um diese später nicht anwesenden GUD-Mitarbeitenden zur Verfügung zu stellen. Allerdings ist hierfür die vorherige ausdrückliche Einwilligung aller Teilnehmenden erforderlich. Lediglich ein Hinweis auf die Aufzeichnung ist nicht ausreichend.

Einige Conferencing Tools (darunter z.B. auch das GUD-Teams) verfügen nicht über eine vorgeschaltete Einmal-Zulassung per Sicherheitscode, sondern nur über einen sogenannten Warteraum,

aus dem dort Wartende durch den Organisator oder andere in der Konferenz befindliche Teilnehmende zur Sitzung zugelassen werden können.

R56 Um die Teilnahme einer unbefugten Person zu verhindern, erfordert das Einlassen von Teilnehmern in eine Video-/Telefonkonferenz hohe Achtsamkeit.

8. Nutzung von GUD-Smartphones

Sofern Sie im Rahmen Ihrer Beauftragung mit einem GUD-Smartphone ausgestattet werden, gelten folgende Regelungen:

R57 Updates für das Betriebssystem des Smartphones sind nach Bereitstellung von jedem Benutzer unverzüglich zu installieren. Hierfür ist die automatische Updatefunktion im Betriebssystem zu aktivieren.

9. Änderungen an IT-Systemen

9.1 Änderungen an Hardwaresystemen

R58 Es dürfen keine neuen Hardwarekomponenten an den bestehenden IT-Systemen installiert oder technische Veränderungen an Komponenten durchgeführt werden. Auch dürfen eigenständig keine räumlichen Veränderungen, z.B. Umzüge der Systeme, vorgenommen werden.

9.2 Beschaffung, Installation und Änderung von Software

R59 Bei der Beschaffung und Installation neuer oder zusätzlicher Software, einschließlich Updates, ist grundsätzlich die Ansprechperson einzuschalten. Es ist nicht gestattet, Software ohne Zustimmung zu installieren.

10. Störungen und Sicherheitsschwachstellen

Für die Erkennung von Störungen bzw. Sicherheitsschwachstellen ist die Aufmerksamkeit und Mithilfe aller Benutzer erforderlich.

R60 Erkannte Sicherheitsschwachstellen dürfen auf keinen Fall durch den Benutzer ausgenutzt werden. Sie sind, wie auch erkannte Störungen, unverzüglich zu melden.

Es sind nachfolgende Meldestellen eingerichtet:

- Office IT: Service Desk
- IT-Systeme in Betriebsverantwortung (Betriebliche Offlinesysteme):
  Jeweiliger Standortleiter

R61 Die Behebung von Störungen durch den Benutzer selbst ist grundsätzlich nicht erlaubt. Ausnahmen sind Störungen, deren Beseitigung keine Fachkenntnisse erfordert (z.B. Beseitigung eines Papierstaus am Drucker, Neustart des eigenen Rechners).

11. Datenschutzinformation

Im Rahmen der Bereitstellung und des Betriebs der IT-Systeme durch GUD werden personenbezogene Daten der Nutzer von GUD erhoben, gespeichert und verarbeitet. Detaillierte Informationen zur „Datenschutzinformation für Nutzer von IT- und Telekommunikationssystemen der Gasunie Deutschland Gesellschaften“ sind hier zu entnehmen.

12. Anlagen

Keine