Benutzung der IT-Systeme

Ziel und Zweck dieser Anweisung

Die Anweisung legt Regeln für die Benutzung von IT-Systemen und die Anwendung von Software-Produkten für alle Nutzer von GUD IT-Systemen verbindlich fest.
Sie sind aus den Anweisungen „IT-Sicherheitsleitlinie" und „Sicherheit der Informationsverarbeitung" abgeleitet und Bestandteil der Informationssicherheitsdokumentation.
Darin sind u. a. Verantwortlichkeiten, organisatorische Maßnahmen, die Handhabung von Risiken sowie grundlegende Verfahren und Prinzipien der Informationssicherheit festgeschrieben.

Inhaltsverzeichnis

1. Begriffe

Begriff	Definition / Erklärung
Benutzer	GUD–Mitarbeiter und Personen mit Zugangsrechten für ein IT–System
Funktion IT-Sicherheit GIP	Abteilung GIP. E-Mail: security@gasunie.de
Informationssicherheit/ IT-Sicherheit	Zustand eines Informationssystems und Maßnahmen, durch die die unberechtigte Nutzung von Ressourcen verhindert und die gewünschte Nutzung ermöglicht wird
ICT-Security Manager	Information and Communication-Security Manager E-Mail: IT-Sicherheit@gasunie.de
IT-System	Alle IT-Einrichtungen, sowohl zentrale und dezentrale Hardware wie auch Software
On-site Support (OSS)	Mitarbeiter des IT-technischen Vor-Ort-Services
Service Desk	Zentrale Anlaufstelle für alle Fragen der Nutzung von IT-Systemen der Office IT (Single Point of Contact), z.B. erreichbar unter der Tel.-Nr. 1180 bzw. unter ccc.gasunie.de
Whitelist	Liste seitens GIP als vertrauenswürdig eingestufter Apps

2. Zuständigkeiten und Verantwortlichkeiten

Jede Person, die IT-Systeme der GUD nutzt, hat dies unter Anwendung der in dieser Arbeitsanweisung beschriebenen Regeln durchzuführen. Es ist Aufgabe der zuständigen GUD-Vorgesetzten, die Einhaltung der Regeln in angemessener Weise zu kontrollieren.
Diese Regeln gelten grundsätzlich auch für die Aspekte der IT-Sicherheit bei der Ausübung der Telearbeit. Weitere diesbezügliche Verhaltensregeln sind in dem Vertrag zur Telearbeit zwischen Mitarbeiter und Personalabteilung festgelegt und auch in der „Betriebsvereinbarung Telearbeit vom 18.07.2012" nachzulesen.

3. Umgang mit Daten

3.1 Umgang mit Informationen

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

3.2 Geheimhaltung

Jeder GUD-Mitarbeiter ist durch die Betriebsordnung verpflichtet, Geschäfts- und Betriebsgeheimnisse zu wahren sowie betriebliche Angelegenheiten vertraulicher Natur geheim zu halten. Dies erstreckt sich auch auf Informationen, die in elektronischer Form gespeichert werden.
Für nicht dienstliche Zwecke dürfen keine Datenträger wie z.B. CD-ROMs, DVDs, USB-Sticks, Ausdrucke mit Geschäftsinformationen etc. aus den Räumen der GUD herausge-

bracht und auch keine Daten über andere Übertragungswege (z.B. E-Mail) an Empfänger außerhalb der GUD versendet werden.

3.3 Schutz personenbezogener Daten

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Für die Verarbeitung und Speicherung solcher Daten ist die Datenschutzrichtlinie der GUD zu beachten.

3.4 Speicherung von Daten

Auf lokalen Laufwerken von Desktops und Notebooks können Daten nicht ausreichend geschützt werden. Daher sind Daten auf den dafür vorgesehenen zentralen Rechnern (Server) im Netzwerk (Netzlaufwerke oder Sharepoint) zu speichern. Diese werden regelmäßig gesichert (Backup) und können nach technischen Defekten oder einem versehentlichen Löschen wiederhergestellt werden (max. 4 Wochen zurück). Weiterhin sind die Server wesentlich besser vor einem Zugriff Unberechtigter geschützt, da sie in überwachten Sicherheitszonen stehen und bestimmte technische Sicherungsmaßnahmen für den Datenzugriff installiert wurden.
Daten, mit denen mehrere Personen arbeiten müssen, sind auf dafür vorgesehenen Laufwerken abzulegen. Die Funktion IT-Sicherheit bei GIP berät bei der Strukturierung derartiger Verzeichnisse.

3.5 Vertraulichkeitseinstufung von Informationen

Da nicht alle Informationen den gleichen Wert haben, ist es nicht notwendig, alle Daten im gleichen Maß zu schützen. Deshalb werden Daten gemäß der Anweisung „Klassifizierung von Informationen" in vier Vertraulichkeitsklassen eingestuft:

Klasse 1: Offene Informationen
Klasse 2: Interne Informationen
Klasse 3: Vertrauliche Informationen
Klasse 4: Geheime Informationen

Zur Detaillierung der Klassen siehe auch das entsprechende Kapitel der Anweisung „Klassifizierung von Informationen".

Verantwortlich für die Einstufung von Dateien ist immer der Dateneigentümer (Informationseigentümer genannt). Dateneigentümer der persönlichen Daten der Benutzer, z.B. auf den persönlichen (Y:\-) Laufwerken, ist der jeweilige Benutzer selber. Dateneigentümer von Daten auf Verzeichnisse, die mehreren Personen zugänglich sind, sind die jeweiligen Führungskräfte bzw. benannten Mitarbeiter, zum Beispiel Projektleiter.
Die Standardeinstufung für Daten der GUD ist die Klasse 2, für die die standardmäßig in den Systemen eingestellten Sicherheitsmaßnahmen ausreichen. Wenn Daten der Klasse 3 (Vertraulich) oder Klasse 4 (Geheim) gespeichert werden sollen, müssen besondere technische und/oder organisatorische Maßnahmen ergriffen werden, in die der jeweilige Eigentümer/Beauftragte der Daten einbezogen wird.
Änderungen an den Zugriffsberechtigungen und oder Gruppenmitgliedschaften sind vom Eigentümer bzw. dessen Beauftragten zu genehmigen.

E-Mails mit vertraulichem oder geheimen Inhalt sind entsprechend (z.B. im Betreff) zu kennzeichnen.

Geheime Daten dürfen nur in den dafür vorgesehen Bereichen (Verzeichnissen) gespeichert werden, für die eine Überwachung der Zugriffe aktiviert ist. Die Speicherung von geheimen Daten auf den persönlichen (Y:\-) Laufwerken ist ohne zusätzliche Sicherungsmaßnahmen

untersagt. Falls ein entsprechender Bedarf besteht, ist die Funktion IT-Sicherheit bei GIP einzuschalten.

Bei unternehmensübergreifenden Projekten ist durch GUD darauf hinzuwirken, dass es eine einheitliche zwischen den Parteien abgestimmte Vorgehensweise zum Schutz der Informationen gibt. In diesem Fall finden die Regelungen der GUD keine Anwendung, sondern es gelten die im Projekt vereinbarten Regeln. Der zuständige Vorgesetzte des GUD Projektleiters ist dafür verantwortlich, dass die im Projekt vereinbarten Regeln denen dieser Anweisung soweit möglich entsprechen. Ist dies nicht der Fall, ist das dadurch entstehende Risiko einzuschätzen und in Abhängigkeit von den zu schützenden Informationen mit dem ICT-Security Manager dahingehend zu bewerten, ob zusätzliche Risikominderungsmaßnahmen auf Seiten der GUD einzuführen sind, durch die die Abweichungen der im Projekt mit der externen Partei vereinbarten Regeln zu denen dieser Anweisung kompensiert werden. Der Projektleiter der GUD ist verantwortlich für die betreffenden in den GUD-Systemen gespeicherten Daten und überwacht deren Behandlung durch angemessenes Controlling. Der Projektleiter ist dafür verantwortlich, die Teilnehmer des Projektes über die Vorgehensweise zum Schutz von Daten im Projekt und ggf. festgelegten Risikominderungsmaßnahmen zu unterrichten.

3.6 Ausdrucken von Daten

Ausdrucke auf nicht zugangsgeschützten Druckern sind unverzüglich vom Druckenden abzuholen. Vertrauliche und geheime Ausdrucke dürfen nur auf zugangsgeschützten oder mit einem Code gesicherten Druckern unter Nutzung dieser Funktion ausgedruckt werden.

3.7 Löschen/ Vernichten von Daten und Datenträgern

Geheime Daten sind mit speziellen Löschprogrammen zu löschen, die auf Anforderung durch die Funktion GIP zur Verfügung gestellt werden.
Datenträger, auf denen geheime Daten gespeichert waren oder sind, sind ausschließlich über die Funktion IT-Sicherheit bei GIP zu entsorgen.

Datenträger mit vertraulichen Daten müssen durch speziell zertifizierte Unternehmen entsorgt werden. Für CDs und DVDs stehen hierfür Entsorgungstonnen beim Onsite-Support bereit.

4. Systemzugang und Zugriffsrechte

4.1 Benutzerkonto, Benutzername, Authentifizierung

Jeder Nutzer von GUD IT-Systemen erhält ein Benutzerkonto, welches mindestens über einen Benutzernamen und ein Kennwort zur Authentifizierung verfügt. Dieses ermöglicht, dass alle Aktivitäten, die unter einem bestimmten Benutzernamen durchgeführt werden, eindeutig einer Person zugeordnet werden können.

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

Die Nutzung von sogenannten Funktionsusern ist in zu begründenden Ausnahmefällen mit Zustimmung des Systemeigentümers möglich. Hierbei hat der Eigentümer des Funktionsuserkontos die Pflicht, die in dieser Anweisung genannten Regeln durch geeignete Maßnahmen analog sicherzustellen. Der ICT-Security Manager berät hierbei nach Bedarf.

Einige Betriebs- und Anwendungssysteme erfordern zusätzlich zu Benutzernamen und Passwort noch weitere Authentifizierungen (Nachweis der Identität), z.B. durch einen sog. Software-Token.

Authentifizierungsmittel sind sicher aufzubewahren. Das heißt, dass sie zu keiner Zeit vom Eigentümer unbeaufsichtigt sein dürfen und bei Abwesenheit weggeschlossen werden müssen.

4.2 Anforderungen an Kennwörter

Ein persönliches Kennwort muss unabhängig vom System, in dem es verwendet wird, und unabhängig von den technischen Minimalanforderungen des Systems für Kennwörter bestimmte Bedingungen erfüllen, um eine ausreichende Sicherheit zu gewährleisten. Sofern technisch möglich, muss es

- mindestens 8 Zeichen enthalten - eine Mischung aus Buchstaben, Sonderzeichen (z.B. $, _, #) und Ziffern (0, .., 9),
- in der Windows-Domäne alle 50 Tage gewechselt werden,
- in allen anderen Anwendungen alle 35 Tage gewechselt werden und
- sich von den letzten 13 auf dem System verwendeten Kennwörtern unterscheiden.

Zudem hat der Benutzer 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,
- anfällig für Wörterbuchangriffe sind (d.h. nicht aus Wörtern bestehen, die in Wörterbüchern stehen),
- keine Folge identischer, numerischer oder alphanumerischer Zeichen enthalten und
- nicht notiert oder gespeichert werden.

Auch bei der Nutzung von Online-Portalen, deren Verwaltung nicht in der Verantwortung der GUD liegen (z.B. Buchungs-und Bestellungsportale, Datenportale, Sharepoint-Zugriff auf Datenbanken anderer Firmen), in denen aber GUD-Daten enthalten sind, gelten die zuvor genannten Anforderungen.
Können die bei GUD gültigen Kennwortregeln aus technischer Sicht nicht eingehalten werden, ist ein Kennwort so stark wie technisch möglich zu definieren und entsprechend der definierten Fristen zu ändern

4.3 Beantragung von Benutzerrechten

Für die Verwendung von Programmen und Daten (Ressourcen) werden technische Rechte (Berechtigungen) benötigt. Diese werden nach Arbeitsnotwendigkeit vergeben und müssen für die jeweilige Ressource beantragt werden. Der jeweilige Vorgesetzte bestätigt die Notwendigkeit der Verwendung durch seinen Mitarbeiter mit der Genehmigung des Antrags. Zugriffs- und Nutzungsrechte auf Ressourcen der Klasse 3 und 4 müssen außerdem noch der Eigentümer bzw. Beauftragte der Ressource genehmigen.

Bei Versetzungen über Abteilungsgrenzen hinweg werden einem Benutzer die funktionsspezifischen Berechtigungen entzogen, die über die Standardberechtigungen eines GUD-Mitarbeiters (z. B. Benutzerkonto, E-Mail-Konto, Zugriff auf allgemeine Informationen, Intranet und Internet) hinaus gehen. Sie müssen ggf. vom neuen Vorgesetzten gemäß der neuen Aufgabe beantragt werden.

4.3.1 Beantragung von Benutzerrechten für die Systeme der Office IT

Berechtigungen für die Systeme der Office IT sind grundsätzlich über den omnitracker zu beantragen. Sofern bei der Neubeantragung eines gesamten Benutzerkontos auf ein vor-

handenes Konto eines anderen Benutzers verwiesen wird, so hat der Vorgesetzte im Rahmen des Beantragungsprozesses zu prüfen, ob alle Berechtigungen des vorhandenen Kontos auch für das neue Konto zur Anwendung kommen sollen..

Das Ausscheiden und somit der Entzug/das Löschen von Berechtigungen sind durch den Vorgesetzten rechtzeitig an die Funktion IT-Sicherheit GIP zu kommunizieren.

Siehe hierzu auch detaillierte Beschreibungen in der Anweisung „Gewährung und Verwaltung von EDV-Zugriffsberechtigungen in der Office-IT".

4.3.2 Beantragung von Benutzerrechten für das zentrale Prozessleitsystem

Die Beantragung der Benutzerrechte für das zentrale Prozessleitsystem erfolgt beim Leiter Dispatching. Dieser entscheidet auch über die Ausgestaltung der Zugriffsberechtigungen. Die Regelungen für den Umgang mit User- und Service-Accounts ist detailliert in der Anweisung „INGa-Account-Management" beschrieben.

4.3.3 Beantragung von Benutzerrechten für Offlinesysteme der betrieblichen Standorte

Die Beantragung der Benutzerrechte für die Offlinesysteme der betrieblichen Standorte erfolgt beim jeweiligen Standortleiter, welcher auch über den Umfang der gewährten Zugriffsberechtigungen entscheidet. Die entsprechenden Prozesse sind detailliert in der Anweisung „Benutzerverwaltung von betrieblichen Offlinesystemen" beschrieben.

5. Technische und physische Schutzmaßnahmen

Um die Risiken des Missbrauchs und des Verlustes von Informationen zu verringern, sind diverse technische Schutzmaßnahmen ergriffen worden. Diese Schutzmaßnahmen reichen aber in der Regel nicht aus, um die Systeme zu schützen. Sie müssen durch aktives und bewusstes Handeln der Benutzer in ihrer Wirksamkeit unterstützt werden.

5.1 Sicherung des IT–Arbeitsplatzes

Ein angemeldeter Benutzer hat die Möglichkeit, den PC, bzw. Notebook oder ThinClient, manuell zu sperren, so dass nur nach Eingabe des persönlichen Kennwortes wieder darauf zugegriffen werden kann. Diese Sperre wird auch automatisch nach einer eingestellten Zeit durch den Bildschirmschoner aktiviert. Beim Verlassen des Arbeitsplatzes, auch kurzzeitig, ist die Bildschirmsperre manuell zu aktivieren. Ausgenommen hiervon sind die Dispatcherarbeitsplätze in der Leitzentrale und die PCs in den Messwarten, da nur autorisierte Personen Zutritt zu den betreffenden Räumen haben.

Das IT-Equipment an den einzelnen Arbeitsplätzen ist grundsätzlich bei längerer Abwesenheit, z.B. nach Feierabend, auszuschalten. Ausnahmen gelten, wenn diese, z.B. im Fall von IT-Wartungsmaßnahmen, kommuniziert wurden und aufgrund der Notwendigkeit der permanenten Verfügbarkeit für die Dispatcherarbeitsplätze.

5.2 Sicherung des IT-Arbeitsplatzes an den Offlinesystemen der betrieblichen Standorte

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

Mobile Endgeräte sind bei längerer Abwesenheit (z.B. nach Feierabend) zu verschließen. Für Tablets und Notebooks stehen abschließbare „Docking–Stations" bzw. Sicherheitskabel zur Verfügung. Datenträger, die geheime Daten enthalten, sind unabhängig von der Verschlüsselung der Daten auch zu den normalen Bürozeiten unter Verschluss zu halten, sofern sie nicht in Gebrauch sind.
Mobile Endgeräte sind an öffentlichen Orten (Zug, Flughafen etc.) zu beaufsichtigen. In einem öffentlich geparkten PKW sind mobile Geräte, wenn überhaupt nötig, so aufzubewahren, dass sie nicht offen sichtbar sind, z.B. im verschlossenen Kofferraum.

5.4 Virenschutz

5.4.1 Virenschutz von Rechnern

Zum Schutz vor Schadsoftware werden bei GUD verschiedene Schutzprogramme auf den PCs, bzw. Tablets und Notebooks und den zentralen Rechnern eingesetzt. Die auf den Rechnern installierten Virenscanner dürfen auf keinen Fall von den Benutzern deaktiviert werden.

Auf nicht dauerhaft in das GUD–Netzwerk eingebundenen Rechnern (Notebooks, Tablets, etc.) ist durch ein regelmäßiges Starten dieser Rechner im GUD–Netzwerk (mindestens einmal monatlich) für eine Aktualisierung der Schutzmechanismen zu sorgen. Ist dies nicht möglich ist die Aktualisierung über externen Zugriff mit geeigneten technischen Mitteln (z. B. VPN/Checkpoint) durchzuführen.

PCs und Notebooks, die nicht innerhalb der Office-Domäne oder der Netzleitsystem-Domäne eingesetzt werden und bei denen sichergestellt ist, dass sie nicht mit dem Internet verbunden sind oder werden, müssen mindestens einmal jährlich manuell mit einem Virenschutzprogramm geprüft werden.

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.

In allen anderen Fällen ist der ICT-Security Manager zu kontaktieren, um geeignete Schutzmaßnahmen vorab festzulegen.

5.4.2 Verbreitung von Schadprogrammen per E-Mail

Schadprogramme, die per E-Mail verbreitet werden, können sich z.B. in deren Anhängen oder hinter in der E-Mail enthaltenen Links verbergen.

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. Auch Anhänge und Links in E-Mails von bekannten Absendern aber mit ungewöhnlichem Inhalt sind nicht ungeprüft zu öffnen. Auch hier sollte vor dem Öffnen beim Absender eine Information über den Inhalt der E-Mail eingeholt werden.

Bei Zweifeln ist die Funktion IT-Sicherheit GIP oder der ICT-Security Manager zu kontaktieren.

5.4.3 Warnhinweise zu Schadprogrammen

Warnhinweise und Anweisungen zu Schadprogrammen, die von der Funktion IT-Sicherheit GIP oder durch den ICT-Security Manager unter dem Absender "Virenwarnung" oder "Virenalarm" per E-Mail versendet werden, sind unbedingt zu beachten!

Von außen empfangene Virenwarnungen müssen an die Funktion IT-Sicherheit GIP (security@gasunie.de) und den ICT-Security Manager (it-sicherheit@gasunie.de) gesendet werden. Ein weiteres Versenden an interne oder externe Empfänger ist nicht erlaubt.

6. Datenaustausch und Datenübertragung

6.1 Nutzung von E-Mails

Das E-Mail-System der GUD ist für den geschäftlichen Gebrauch bestimmt.

Vor dem Versenden einer E-Mail ist immer die Richtigkeit der E-Mail-Adresse des Empfängers zu überprüfen. Bei der Weiterleitung von empfangenen E-Mails sind Festlegungen bzgl. der Vertraulichkeitsstufe zu beachten.

Vertrauliche oder geheime Daten dürfen nur verschlüsselt an externe Empfänger versendet werden. Vertrauliche Inhalte von E-Mails sind GUD-intern zu kennzeichnen. Geheime Daten sind auch innerhalb der GUD bei der Versendung per E-Mail zu verschlüsseln. Abweichungen hiervon sind nur mit Genehmigung durch einen Manager der 1. Führungsebene für vertrauliche Informationen oder der Geschäftsführung für geheime Informationen möglich und richten sich grundsätzlich nach den unter 3.5 beschriebenen Prozeduren für unternehmensübergreifende Projekte.

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

Eine Weiterleitung dienstlicher E-Mails oder Dokumente (z.B. per Scan-to-mail) an private E-Mail Postfächer ist nicht gestattet.

6.2 Verschlüsselung von Daten

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

Mit dem Programm 7-Zip verschlüsselte Daten können im Regelfall auch von externen Geschäftspartnern problemlos mit gängigen „Zip-Programmen" entschlüsselt werden. Eine Anleitung für die Durchführung der Verschlüsselung befindet sich im GUD-Intranet.

6.3 Nutzung von Wechselspeichermedien (USB-Sticks, CDs, etc.)

6.3.1 Speicherung, Aufbewahrung und Transport von Daten auf Wechselspeichermedien

Auf Wechselspeichermedien wie CD-ROM, DVD, ect. 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. Dieses schließt auch eine ständige Beaufsichtigung bzw. ein sicherer Einschluss bei Mitführung der Datenträger auf Reisen ein. Für den postalischen Versand finden die Regelungen der Anweisung „Klassifizierung von Informationen" Anwendung.

Vertrauliche oder geheime Informationen dürfen nur in begründeten Ausnahmefällen (z.B. wenn keine andere sichere und angemessene Möglichkeit für die Speicherung bzw. den

Transport von Daten besteht) auf Wechselspeichermedien gespeichert werden. In diesem Falle sind die Daten zusätzlich zu den zuvor beschriebenen Maßnahmen zu verschlüsseln und mit einem Passwort zu schützen. Das Wechselspeichermedium ist in diesem Falle sicher zu verschließen, sofern es gerade nicht im Gebrauch ist.

6.3.2 Nutzung von Wechselspeichermedien zum Datenaustausch

Datenaustausch mit externen bekannten Geschäftspartnern sollte nach Möglichkeit via E-Mail erfolgen. Sollte in Ausnahmefällen doch einmal die Nutzung eines Wechselspeichermediums notwendig sein, so ist zu beachten, dass grundsätzlich nur von GUD ausgegebene Speichermedien verwendet werden dürfen. Im Fall von USB-Sticks dürfen ausschließlich Sticks, die mit einer Verschlüsselungsfunktion ausgestattet sind, verwendet werden. Diese dürfen nur für dienstliche Zwecke genutzt werden. Sollte die Notwendigkeit bestehen, Speichermedien (USB-Sticks, DVDs, CDs) externer bekannter Geschäftspartner z.B. im Rahmen einer Besprechung zu verwenden, so ist eine Nutzung unter folgenden Voraussetzungen möglich:

- auf dem Datenträger befinden sich nur geschäftsbezogene Daten
- auf dem Datenträger befindliche Dateiarten sind bekannt (z.B. doc, .xls., pdf, .ppt etc.)
- auf dem Datenträger befindet sich keine Software sowie keine ausführbaren Dateien (z.B. .exe, .bat, etc.). Im Zweifelsfalle ist der ICT-Sercurity Manager zu kontaktieren.

Die Einhaltung der genannten Voraussetzungen ist durch den jeweiligen GUD-Mitarbeiter durch entsprechende Nachfragen beim Geschäftspartner sicherzustellen.

Zusätzlich ist ein Antivirus-Scan vorzunehmen, wobei die Überprüfung der Wechselspeichermedien (auch der Wechselspeichermedien von Kontraktoren) grundsätzlich nur durch GUD-Mitarbeiter erfolgen darf.

Medien, bei denen Malware detektiert wurde, dürfen erst nach weiterer Prüfung und Freigabe durch die Funktion für IT-Sicherheit GIP oder den On-site Support genutzt werden.

Die Nutzung von Wechselspeichermedien aus unbekannter Quelle oder mit unbekanntem Inhalt (z.B. zugesandte CDs/USB-Sticks mit Produktinformationen, auf Messe erhaltene CDs etc.) ist erst nach Freigabe durch die Funktion für IT-Sicherheit GIP oder den On-site Support möglich.

Die Nutzung von Wechselspeichermedien an potenziell unsicheren Rechnern (z.B. in Internetcafes, Hotel-PCs etc.) ist nicht gestattet.

Für Fragen ist die Funktion für IT-Sicherheit GIP rechtzeitig anzusprechen oder/und bei vorhersehbaren Fällen (z.B. Mitbringen von Wechselspeichermedien zur Nutzung vor Ort durch Kontraktoren) darauf hinzuweisen, wenn möglich andere Übertragungswege (z.B. Vorabversand per E-Mail oder eine Datenaustauschplattform (siehe 6.4)) zu nutzen).

6.3.2.1 Antivirus-Scan von Wechselspeichermedien an den Standorten Hannover und Schneiderkrug

An den Standorten Hannover und Schneiderkrug ist der Antivirus-Scan von Wechselspeichermedien an den vorhandenen Antivirus-Scanstationen vorzunehmen, wobei eine Überprüfung von passwortgeschützten, selbstverschlüsselnden Datenträgern jedoch nicht möglich ist. In diesen Fällen ist die Funktion für IT-Sicherheit GIP bzw. in Schneiderkrug der On-site Support zu kontaktieren.

6.3.2.2 Antivirus-Scan von Wechselspeichermedien an den betrieblichen Standorten

An den betrieblichen Standorten steht ein Scan-Laptop zur Verfügung. Dieser Scan-Laptop ist ausschließlich zum Prüfen von Wechselspeichermedien vorgesehen und darf nicht für

andere Zwecke genutzt werden. Vor jeder Überprüfung ist der Virenscanner zu aktualisieren. Während der Überprüfung ist der Scan-Laptop vom GUD-Netz zu trennen.

6.4 Austausch großer Datenmengen über eine Datenplattform

Für den Austausch großer Datenmengen mit externen bekannten Geschäftspartnern, die nicht per E-Mail-Anhang verschickt oder empfangen werden können, kann im Bedarfsfall die Einrichtung einer sicheren Datenaustauschplattform bei der Funktion IT-Sicherheit GIP (security@gasunie.de) per E-Mail beantragt werden.

6.5 Internetnutzung

Der Internetzugang bei GUD ist für dienstliche Zwecke bestimmt.

Es dürfen keine Informationen mit rechtswidrigen oder sittenwidrigen Inhalten genutzt und verbreitet werden. Hierzu zählen insbesondere alle Informationen, die i.S.d. §§ 130, 130a und 131 StGB der Volksverhetzung dienen, zu Straftaten anleiten oder Gewalt verherrlichen oder verharmlosen, sexuell anstößig sind, im Sinne des § 184 StGB pornografisch sind, geeignet sind, Kinder oder Jugendliche sittlich zu gefährden oder in ihrem Wohl zu beeinträchtigen oder das Ansehen der Gasunie schädigen können. Die Bestimmungen des Jugendmedienstaatsvertrages und des Jugendschutzgesetzes sind zu beachten.

Die Nutzung sozialer Netzwerke (z. B. Facebook, Xing, Linkedin) ist zu unterlassen, solange dies nicht der entsprechenden Person aus betrieblicher Notwendigkeit gestattet wurde. Empfehlungen für die private Nutzung sind dem im GMS System 11.2 verlinkten „Hinweisblatt zur Nutzung sozialer Netzwerke zu entnehmen".

Es dürfen keine Programme aus dem Internet heraus ausgeführt oder aus dem Internet heruntergeladene Programme ohne Einschalten von GIP installiert werden. Hiervon ausgenommen ist das Ausführen von Webkonferenzdiensten (z.B. WebEx).

Bei der Weiterverwendung von Informationen aus dem Internet z.B. in eigenen Texten sind das Urheberrecht und entsprechende Hinweise auf der Quellseite im Internet zu beachten. In Zweifelsfällen ist bei der kommerziellen Verwendung von Texten und Bildern aus dem Internet die Funktion Legal zu befragen.

Werden Nachrichten und Informationen in das Internet eingebracht, z.B. über Diskussionsforen oder Feedback-Formulare, so dürfen diese nur als „offen" klassifizierte Informationen enthalten. Bei der Nutzung von frei zugänglichen Online-Übersetzungsdiensten für ganze Textpassagen (z.B. Google Translator, DeepL ect.) dürfen ebenfalls nur Texte, die als offen klassifiziert sind, an diese Dienste übermittelt werden. Sollen interne oder vertrauliche Texte (z.B. Verträge) übersetzt werden, sind entsprechend geschützte Dienste zu nutzen (i.d.R. kostenpflichtig). Hierzu ist die IT-Abteilung anzusprechen. Geheime Daten dürfen grundsätzlich nicht in Online-Diensten verarbeitet werden, da die hierfür notwendigen Schutzanforderungen nicht umgesetzt werden können.

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

Die Nutzung einer Web-Cam o.ä. ist freiwillig. Unternehmensseitig werden beim Einsatz von Web-Cams keine Kommunikationsdaten gespeichert oder mitgeschnitten, die das Verhalten oder die Leistung der Mitarbeiter überwachen. Es ist nicht auszuschließen, dass die von einer Web-Cam übertragenen Bilder einem erweiterten Personenkreis sichtbar sind. Deshalb ist der aktive Betrieb der Web-Cam für Dritte vor dem Einschalten durch eine deutliche Kennzeichnung anzuzeigen. Die Nutzung von Web-Cams bei Gasunie Deutschland ist aus-

schließlich über die von GIP freigegebenen Conferencing-Tools zulässig. Beim Einsatz der Web-Cam ist der Mitarbeiter verpflichtet, einen Hinweis, der auf die aktive Verwendung der Web-Cam hinweist, gut sichtbar zu platzieren. Vordrucke dafür gibt es im Intranet. Auf eine Telefonkonferenz sind alle Teilnehmer vorab geeignet hinzuweisen (z.B. in der Einladung, mündlich bei Start der Telefonkonferenz).

8. Nutzung von GUD-Smartphones

Auf einem GUD-Smartphone sind durch die Synchronisation mit dem Gasunie E-Mailkonto Unternehmensdaten gespeichert. Dies betrifft sowohl die synchronisierten Inhalte (E-Mails inkl. Anhänge, Kalendereinträge, Kontakte, etc.) als auch die Zugangsdaten (Anmeldedaten für das GUD-Netz). Diese Daten gilt es zu schützen.

8.1 Verlust/Diebstahl des Smartphones

Im Rahmen der Einbindung des E-Mail-Kontos werden Sicherheitsrichtlinien auf das Gerät übertragen. Dazu gehört die vollständige Verschlüsselung des Gerätespeichers sowie die Möglichkeit, die Daten auf dem Gerät aus der Ferne komplett zu löschen. Die Bildschirmsperre mit Passwort ist verbindlich zu nutzen.

Im Falle des Verlust des Smartphones ist umgehend die Abteilung GIP zu informieren.

8.2 Aktualisierung des Betriebssystems

Von dem Hersteller des Smartphones werden regelmäßig Updates für das Betriebssystem des Smartphones bereitgestellt, mit denen u.a. Sicherheitsschwachstellen behoben werden. Diese Updates sind nach Aufforderung per Massenmail durch GIP zeitnah zu installieren.

8.3 App-Whitelist

Ergänzend zu den im Auslieferungszustand auf dem Smartphone vorhandenen Apps dürfen nur seitens GIP als vertrauenswürdig eingestufte Apps auf dem Smartphone installiert werden. Diese sind auf einer sogenannten „Whitelist" verzeichnet. Die jeweils aktuelle Whitelist ist im Intranet veröffentlicht. Dort ist auch der Prozess zur Aufnahme weiterer Apps in die Whitelist beschrieben.

9. Änderungen an IT-Systemen

9.1 Änderungen an Hardwaresystemen

Ohne Zustimmung der jeweiligen IT-Betriebsfunktion dürfen keine neuen Hardwarekomponenten an den bestehenden IT-Systemen installiert oder technische Veränderungen an Komponenten durchgeführt werden. Auch dürfen keine räumlichen Veränderungen, z.B. Umzüge der Systeme vorgenommen werden, da ansonsten die zentrale Erfassung und Funktionsfähigkeit der Systeme und versicherungsrelevante Rahmenbedingungen ggf. nicht mehr gewährleistet werden können.

9.2 Installation und Änderung von Software

Bei der Beschaffung und Installation neuer oder zusätzlicher Software einschließlich Updates ist grundsätzlich die verantwortliche Betriebsfunktion einzuschalten. Es ist nicht gestattet, Software ohne Tests und Zustimmung der verantwortlichen Betriebsfunktion zu installieren. Diese Regel gilt auch für Free- und Shareware.

Software ist grundsätzlich über den Bereich GI zu beschaffen bzw. GI ist in die Beschaffung mit einzubeziehen. Es darf keine lizenzpflichtige Software installiert werden, für die GUD keine Lizenz besitzt. Details für den Beschaffungsprozess regelt die Anweisung „Lizenzmanagement".

Von GUD beschaffte Software darf nur mit ausdrücklicher Erlaubnis durch GUD und dann auch nur unter Einhaltung der festgelegten Nutzungsbedingungen auf dem privaten Rechner zu Hause installiert werden.

10. Störungen und Sicherheitsschwachstellen

Für die Erkennung von Störungen bzw. Sicherheitsschwachstellen ist die Aufmerksamkeit und Mithilfe aller Benutzer erforderlich. Erkannte Sicherheitsschwachstellen dürfen auf keinen Fall durch den Benutzer ausgenutzt werden. Sie sind wie auch erkannte Störungen unverzüglich den jeweiligen IT-Betriebsfunktionen zu melden.

Es sind nachfolgende Meldestellen eingerichtet:

- Office IT (int): Servicedesk von BTC
- Zentrales Prozessleitsystem (D2GTD) und PDÜ-Netz: inga-betrieb@gasunie.de
- IT-Systeme in Betriebsverantwortung von GO (Betriebliche Offlinesysteme):Leiter des jeweiligen Standorts

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).

11. Ergänzende Dokumente / Verweise

Hinweisblatt zur Nutzung sozialer Netzwerke

12. Anlagen

keine