Die Richtlinie wurde in deutscher Sprache erstellt und ins Englische übersetzt.
Um die Lesbarkeit und Verständlichkeit des vorliegenden Regelwerks zu verbessern, wird auf die Nutzung von Gendersternchen u.ä. verzichtet. Das Regelwerk richtet sich gleichermaßen wertschätzend an alle Personen (W/D/M).

Anweisung / Kommunikation				
Aktivität	**OE**	**Name**	**Datum**	**Freigabe**
Erstellung	Group Cyber Security (CHV-CG)	Stefan Wigchers	22.07.2025	Per E-Mail
Fachliche Freigabe	Cyber Security (CHV-C)	Nikk Gilbert	23.07.2025	Per E-Mail

Inhaltsverzeichnis

1 Änderungsverfolgung 3

2 Zweck 4

3 Anwendungsbereich 4

4 Begriffsbestimmungen 6

4.1 Verwendete Symbolik 7

5 Regelungstatbestände / Prozesse / Verantwortlichkeiten 7

5.1 Umgang mit Informationen 7

5.1.1 Einstufen und Kennzeichnen 9
5.1.2 Aufbewahren und Speicherung von Informationen 10
5.1.3 Arbeiten mit Informationen 11
5.1.4 Versenden und Weitergeben von Informationen 13
5.1.5 Vernichten von Informationen 14

5.2 Sichere Kommunikation 15

5.2.1 E-Mails und Messenger 15
5.2.2 Telefon- und Videokonferenzen 16
5.2.3 Besprechungen 17
5.2.4 Internet 18
5.2.5 Social Media 19

5.3 Sicherer Umgang mit IT-Komponenten und Zugängen 20

5.3.1 Kennwörter und Zugriffsschutz 20
5.3.2 Nutzung von IT-Komponenten 21
5.3.3 Schutz vor Schadprogrammen 23
5.3.4 Verwendung von Apps auf Smartphones und Tablets 24
5.3.5 Mobile Datenträger 25
5.3.6 Datensicherung 26

5.4 Sicherheit auf Dienstreisen 27

5.4.1 Während der Reise 27
5.4.2 Nach der Reise 28

5.5 Meldungen von Sicherheitsvorfällen 29

6 Außer Kraft gesetzte / Mitgeltende Konzernregelungen 29

6.1 Außer Kraft gesetzte Konzernregelungen 29

6.2 Mitgeltende Konzernregelungen 29

7 Anhänge 29

Anhang 1: Klassifikation des Schutzbedarfs einer Information 30

1 Änderungsverfolgung

Datum	**Änderung** (max. 10 Einträge/Zeilen rollierend)	**Verfasser** (Vorname, Name, OE)
01.04.2020	Ersterstellung	Stefan Wigchers (CHV-CG)
01.10.2020	Redaktionelle Überarbeitung und Anpassung der Kennwort Vorgaben.	Stefan Wigchers (CHV-CG)
03.03.2021	Redaktionelle Überarbeitung und Abänderung des Begriffs Passwort in Kennwort Ergänzung der Begriffsdefinitionen um IT und OT Aktualisierung des Disclaimers	Stefan Wigchers (CHV-CG)
25.07.2025	Redaktionelle Änderung (Datum, OE, Entflechtungsklausel etc.)	Stefan Wigchers (CHV-CG)

2 Zweck

Cybersicherheit dient nicht nur dem Schutz von materiellen und immateriellen Werten, sondern auch dem Schutz aller Mitarbeitenden, die mit RWE in Verbindung stehen. Besonders schützenswerte Vermögenswerte stellen für RWE die Informationen und Daten des Unternehmens sowie die Systeme, die diese Daten verarbeiten, dar. Aus diesem Grund ist die Cybersecurity Teil der umfassenden Sicherheitsstrategie von RWE und soll die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und IT-Systemen sicherstellen.

Diese Konzernfachregelung enthält verbindliche Regelungen für die Cyber Security und gibt dem Mitarbeiter einen verlässlichen Handlungsrahmen zur sicheren Arbeit mit Informationen sowie für den sicheren Umgang mit Informations- und Telekommunikationssystemen vor. Abweichende Regelungen für IT-Administratoren werden in den aktuell gültigen Vorgaben zur IT Security definiert. Bei Fragen, Anmerkungen etc. zur Umsetzung der Konzernfachregelung wenden Sie sich an die Fachabteilung Group Cyber Security (CHV-CG) in der Konzernsicherheit. Sie haben zusätzlich die Möglichkeit, einfach und unkompliziert per E-Mail Feedback an die dafür vorgesehene E-Mail-Adresse Konzernrichtlinien@rwe.com zu senden.

3 Anwendungsbereich

Diese Konzernrichtlinie gilt für externe Mitarbeiter der RWE AG und allen Konzerngesellschaften sofern auch Gestaltungsmacht oder rechtliche bzw. faktische Beeinflussungsmöglichkeiten bestehen und ausgeübt werden. Bei Minderheitsgesellschaften ist je nach Einflussmöglichkeit die bestmögliche Umsetzung dieser Konzernrichtlinie anzustreben; zumindest sind Informationsflüsse sicherzustellen.

Sämtliche Sicherheitsmaßnahmen erfolgen auf Basis der gültigen Gesetze und der jeweils aktuellen Rechtsprechung inklusive der Mitbestimmungsrechte, wobei ggf. unterschiedliche Rechtsräume zu berücksichtigen sind

Wo erforderlich sieht diese Richtlinie abweichende Regelungen für Konzerngesellschaften vor, die den Entflechtungsvorgaben unterliegen. Hierdurch werden insbesondere die gesetzlichen Vorgaben bezüglich der Unabhängigkeit der Konzerngesellschaften, die den Entflechtungsvorgaben unterliegen, hinsichtlich der Organisation, der Entscheidungsgewalt und der Ausübung des jeweils zu entflechtenden Geschäfts sichergestellt und die Vertraulichkeit wirtschaftlich sensibler Informationen sowie die Einhaltung des Grundsatzes der Nichtdiskriminierung gewährleistet.

Konzerngesellschaften, die den Entflechtungsvorgaben unterliegen, haben sicherzustellen, dass wirtschaftlich sensible Informationen, von denen sie in Ausübung ihrer Tätigkeit Kenntnis erlangen, vertraulich zu behandeln sind und insbesondere ordnungsgemäß gegen Weitergabe an wettbewerbliche und nicht wettbewerbliche Einheiten des Konzerns geschützt werden. Im Falle der Offenlegung von Informationen, die wirtschaftliche Vorteile bringen können, wird die Einhaltung des Grundsatzes der Nichtdiskriminierung sichergestellt.

Für den Bereich Operational Technology (OT) kann es zu abweichenden Regelungen kommen. Bitte kontaktieren Sie bei Fragen dazu Ihren OT Verantwortlichen oder Vorgesetzten.

4 Begriffsbestimmungen

Begriff	Erläuterung
Konzernsicherheit (CHV-CG)	Die Konzernsicherheit steuert und überwacht die Sicherheit im RWE-Konzern.
Informationseigentümer	Diejenige Person, die den Auftrag zur Erstellung einer Unterlage bzw. Information erteilt.
Messenger	(Instant) Messaging ist eine Kommunikationsmethode, bei der sich zwei oder mehr Teilnehmer per Textnachrichten unterhalten. Beispiele sind Threema oder Skype.
IT	Der Begriff Information Technology bezeichnet die Konstellation transaktionaler Systeme, die zur Unterstützung und Automatisierung administrativer und unterstützender Prozesse in Organisationen eingesetzt werden.
OT	Operational Technology (OT) konzentriert sich auf die Unterstützung technischer Prozesse und die Prozess-automatisierung. Dabei geht es um die Steuerung und Überwachung von Anlagen in einem Produktionsprozess z. B. Stromerzeugung oder Braunkohlenförderung.
Security-Organisation/ Security Management	Gesamtheit aller Personen, Strukturen und Prozesse, die innerhalb von RWE mit der Durchsetzung, Gewährleistung und Weiterentwicklung von Security betraut sind.
Single Sign-on	Single Sign-on (SSO) ermöglicht es, über einen einzigen Authentifizierungsprozess Zugriff auf Services, Applikationen oder Ressourcen zu erhalten. SSO ersetzt einzelne Anmeldeverfahren mit verschiedenen Userdaten und nutzt eine übergreifende Identität des Anwenders.
Social Engineering	Social Engineering nennt man zwischenmenschliche Beeinflussungen mit dem Ziel, bei Personen bestimmte Verhaltensweisen hervorzurufen, sie z. B. zur Preisgabe von vertraulichen Informationen, zum Kauf eines Produkts oder zur Freigabe von Finanzmitteln zu bewegen.

Virtual Desktop Infrastructure (VDI)	Infrastruktur virtueller Desktops. Erlaubt das Arbeiten an einem virtuellen RWE-Computer über das Internet.
Virtual Private Network (VPN)	Ein VPN (Virtual Private Network, "Virtuelles Privates Netzwerk") verbindet zwei Netzwerke, einen Computer mit einem Netzwerk oder zwei Computer über öffentliche Verbindungen wie z. B. das Internet.

4.1 Verwendete Symbolik

Symbol	Beschreibung
	Einzuhaltende Anforderungen der Cyber Security („Do's“)
	Einzuhaltende Verbote der Cyber Security („Don'ts“)
	Ergänzende Hinweise zur Umsetzung der vorher aufgeführten Anforderung und Verbote.

5 Regelungstatbestände / Prozesse / Verantwortlichkeiten

5.1 Umgang mit Informationen

Informationen stellen ein wichtiges Gut für den RWE-Konzern dar und sind zu jedem Zeitpunkt ihres Vorhandenseins angemessen zu schützen (Information Life Cycle). Dies gilt von der Erstellung/Erfassung bis zur Löschung/Entsorgung. Die Ausgestaltung der Schutzmaßnahmen richtet sich nach dem Schutzbedarf einer Information. Dieser Schutz erfolgt unabhängig vom Medium (analog oder digital) in dem die Informationen vorliegen.

Hierzu unterteilt RWE den Schutzbedarf jeder Information in drei Schutzklassen anhand der Auswirkungen eines möglichen Schadens:

niedrig - mittel	Die Schadensauswirkungen sind begrenzt und überschaubar (z. B. interne Richtlinien, Prozessbeschreibungen; Personenbezogene

	Daten, die allgemein erforderlich sind, um die geschäftlichen Aufgaben zu erfüllen, z. B. Adressbücher).
hoch	Die Schadensauswirkungen können beträchtlich sein (z. B. vorzeitige Veröffentlichung von Projektplänen, Veröffentlichung von Vertragsunterlagen; Personenbezogene Daten, die bei Verlust, Beschädigung, Offenlegung oder unrechtmäßiger Verarbeitung ggf. einen erheblichen Schaden für den Betroffenen hervorrufen können, z. B. Bankdaten).
sehr hoch	Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß erreichen (z. B. Entscheidungen zu beabsichtigten Unternehmensan- und -verkäufen, Geschäftsgeheimnisse; Personenbezogene Daten, die Informationen über den Gesundheitszustand, das Sexualleben, die ethnische Herkunft, politische Meinung, religiöse/weltanschauliche Überzeugung, Gewerkschaftszugehörigkeit ermöglichen sowie genetische/biometrische Daten).

Kriterien für die Einstufung des Schutzbedarfs befinden sich im **Anhang 1** dieser Konzernfachregelung. Außerdem unterstützt Sie die im RWE Appstore auf Ihrem Smartphone verfügbare App „InfoClass“ bei der Klassifizierung von Daten.

Nachfolgend werden Informationen der Schutzklassen **„hoch“ und „sehr hoch“ zusammenfassend** als **„sensible Informationen“** bezeichnet, wenn beide gemeint sind.

RWE verfolgt bei der Cyber Security die drei Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit:

Vertraulichkeit	Informationen dürfen nur berechtigten Personen zugänglich gemacht werden.
Integrität	Informationen dürfen nicht unberechtigt verändert werden und müssen richtig und vollständig sein.
Verfügbarkeit	Informationen müssen uneingeschränkt im notwendigen, vereinbarten Umfang bzw. Zeitrahmen vorhanden sein.

5.1.1 Einstufen und Kennzeichnen

Die Grundlage für die Cyber Security ist ein angemessener Schutz der Informationen über den gesamten Lebenszyklus.

Einstufung:

- Der Informationseigentümer legt für seine Informationen zu Beginn des Lebenszyklus den Schutzbedarf fest (z. B. anhand der Kriterien in Anhang 1).
- Zur Einstufung des Schutzbedarfs sind die Schutzklassen „niedrig bis mittel“, „hoch“ und „sehr hoch“ zu verwenden.
- Liegt der Informationseigentümer außerhalb des RWE Konzerns und hat dieser keine Klassifizierung vorgenommen, so hat der (erste) Informationsbesitzer innerhalb des RWE Konzerns nach Übermittlung der Information die Einstufung vorzunehmen.
- Bei sensiblen Informationen muss der Informationseigentümer klar erkennbar aus dem Dokument hervorgehen.
- Beachten Sie, dass der Schutzbedarf einer Information sich im Laufe der Zeit verändern kann.

Kennzeichnung mittels Vertraulichkeitsklassen:

- Informationen müssen gemäß ihrem Schutzbedarf mit einer Vertraulichkeitsklasse gekennzeichnet werden. Es muss immer nur die höchste, zutreffende Kennzeichnung verwendet werden.
- Informationen der Schutzklasse „niedrig bis mittel“ sind mit „**Intern**“ zu kennzeichnen. Dafür gilt:
  - Dokumente sind mindestens auf der ersten Seite zu kennzeichnen.
- Informationen der Schutzklasse „hoch“ sind mit „**vertraulich**“ zu kennzeichnen, dafür gilt:
  - Dokumente sind auf jeder Seite zu kennzeichnen.
  - Beschriftung des Datenträgers/Umschlags ist notwendig.
- Informationen der Schutzklasse „sehr hoch“ sind mit „**streng vertraulich**“ in rot zu kennzeichnen, dafür gilt:
  - Dokumente sind auf jeder Seite zu kennzeichnen.

- Eine Beschriftung des Datenträgers/Umschlags ist notwendig.

- Eine Sonderrolle kommt Informationen zu, die zur Veröffentlichung gedacht sind, den sogenannten „**öffentlichen**“ Informationen. Diese müssen nicht gekennzeichnet, aber von den autorisierten Geschäftsfunktionen (z. B. Unternehmenskommunikation) eingestuft und veröffentlicht werden.
- Informationen ohne Kennzeichnung können als „**intern**“ betrachtet werden, wenn es sich nicht offensichtlich um sensible Informationen handelt. Die Kennzeichnung muss nachgeholt werden. Dies gilt nicht, wenn die Informationen offensichtlich „**öffentlich**“ sind (z. B. Werbebroschüren).
- Eine Anpassung der Kennzeichnung ist nur nach Abstimmung mit dem Informationseigentümer vorzunehmen.
- Der Informationseigentümer muss die Klassifikation bei Änderung des Schutzbedarfs anpassen.

Hinweis:

- Informationen der Schutzklassen „hoch“ und „sehr hoch“ bzw. „vertraulich“ und „streng vertraulich“ zusammenfassend als „**sensible Informationen**“ bezeichnet, wenn beide gemeint sind.
- „Intern“ ist die Kennzeichnung für die Dokumente mit der niedrigsten Schutzklasse. Diese Kennzeichnung sagt aus, dass diese Information ohne Beschränkung an RWE-Mitarbeiter weitergegeben werden darf. Im Anhang finden Sie die Arten von Informationen, die als „Intern“ eingestuft werden.
- Es wird pro Dokument immer nur eine Kennzeichnung vergeben. Dabei kommt immer die höchste zutreffende Kennzeichnung zum Einsatz. Ein Dokument kann folglich nicht mit „Intern Vertraulich“ gekennzeichnet sein.
- Die verschiedenen Schutzklassen mit ihren Kennzeichnungen haben aufeinander aufbauende Anforderungen, die im Folgenden erklärt werden.

5.1.2 Aufbewahren und Speicherung von Informationen

Auch bei der Aufbewahrung und Speicherung von Informationen müssen diese geschützt sein. Daher gelten folgende Regeln:

- Speichern und verwahren Sie nur Informationen, die Sie für die Erfüllung ihrer Tätigkeiten benötigen.
- Informationen müssen entsprechend ihres Schutzbedarfs vor unbefugtem Zugriff geschützt werden, unabhängig auf welchem Medium sie vorliegen (z. B. auf Papier, als E-Mail oder als Datei).
- Medien mit vertraulichen Informationen sind unter Verschluss aufzubewahren.
- Für die dauerhafte Aufbewahrung von Medien mit streng vertraulichen Informationen ist eine geeignete Aufbewahrungsmöglichkeit (z.B. Wertschutzschrank oder Stahlschrank) zu verwenden.
  Im Rahmen der täglichen Verwendung sind Medien mit streng vertraulichen Informationen unter Nutzung der verfügbaren technischen Möglichkeiten bestmöglich unter Verschluss zu halten.
- Sensible Informationen auf Laufwerken und Datenträgern sind zu verschlüsseln oder in bereitgestellten Secure Data Rooms zu speichern.

Hinweis:

- Kontaktieren Sie Ihren zuständigen RWE-Ansprechpartner, bei Fragen zur Verschlüsselung von Daten oder zur Nutzung von sicheren Datenräumen.
- Informieren Sie den RWE IT Service Desk, wenn Sie sensible Informationen auf einer zur Reparatur vorgesehenen IT-Komponente gespeichert haben, damit diese Informationen angemessen geschützt oder ggf. gelöscht werden können.
- Achten Sie darauf, dass das Schutzniveau bei der Übertragung auf einen anderen bzw. weiteren Speicher- oder Ablageort kontinuierlich erhalten bleibt.

5.1.3 Arbeiten mit Informationen

Auch bei der Arbeit mit Informationen muss deren Sicherheit gewährleistet sein. Daher sind die folgenden Regelungen zu beachten:

- Stellen Sie sicher, dass Unbefugte nicht auf Informationen an Ihrem Arbeitsplatz zugreifen können. Dies gilt besonders, wenn Sie den Arbeitsplatz verlassen.
- Halten Sie Ihren Arbeitsplatz aufgeräumt und vermeiden Sie es, sensible Informationen offen liegen zu lassen.
- Informationsträger (z. B. Bildschirme, Flipcharts) mit sensiblen Informationen müssen so platziert sein, dass sie von Unbefugten (etwa von außen) nicht einsehbar sind.
- Vermeiden Sie bei Desktopfreigaben (z. B. im Rahmen der Nutzung von Teams) die ungewollte Preisgabe von Informationen.
- Hinterlassen Sie keine sensiblen Informationen auf Anrufbeantwortern, Voice-Mail-Boxen oder in automatischen E-Mail Antworten.
- Für sensible Informationen nutzen Sie die Funktion „sicheres Drucken“.
- Unterstützt der bei Ihnen vorhandene Drucker noch nicht die Funktion „sicheres Drucken“, so ist Ihr Vorgesetzter dafür verantwortlich, eine Verfahrensweise festzulegen, wie beim Druck von sensiblen Informationen vorzugehen ist.
- Wenn Sie einen Auftrag trotz aller Sorgfalt an einen falschen Drucker gesendet haben, stellen Sie unverzüglich sicher, dass der Ausdruck vernichtet oder an Sie weitergeleitet wird.
- Holen Sie den Ausdruck umgehend vom Etagendrucker ab. Lassen Sie Ihre Ausdrucke und Kopien nicht unbeaufsichtigt liegen.
- Achten Sie auch dann auf einen sicheren Umgang mit Informationen, wenn Sie unterwegs oder zuhause Arbeiten.

Hinweis:

- Die technische Realisierung der Funktion „sicheres Drucken“ kann je nach Drucker und/oder RWE-Gesellschaft unterschiedlich komfortabel ausgelegt sein. An einigen Geräten startet der Ausdruck erst nach Identifikation über die RWE Service Card, andere Geräte starten den Ausdruck erst, wenn Sie am Gerät ein entsprechendes Kennwort eingeben.

5.1.4 Versenden und Weitergeben von Informationen

Für das Versenden und Weitergeben von Informationen gelten besondere Regeln, um den Schutz der Informationen zu gewährleisten.

- **Interne** Informationen dürfen
  - dürfen ausschließlich mit Mitarbeitenden der RWE-Gruppe geteilt werden.
- **Vertrauliche** Informationen dürfen
  - nur bei Bedarf (Need-to-Know Prinzip) weitergegeben werden
  - und dürfen nur mit relevanten RWE-Ansprechpartnern geteilt werden, nachdem eine Vertraulichkeitsvereinbarung unterzeichnet wurde.
- **Streng Vertrauliche** Informationen dürfen
  - nur bei Bedarf (Need-to-Know Prinzip) weitergegeben werden
  - und erst nach unterzeichnetem, spezifiziertem Geheimhaltungsvertrag an Externe weitergegeben werden.
  - Auf Wunsch des Informationseigentümers kann die Weitergabe auf einen benannten Personenkreis beschränkt werden. Dieser muss dann auf dem Deckblatt oder im Anhang aufgeführt werden.
- Nutzen Sie für den Versand und die Weitergabe nur von RWE zugelassene Kommunikationsmittel und die zugehörigen Sicherheitsmaßnahmen (z. B. Verschlüsselung).
- Das Versenden von sensiblen Informationen per E-Mail muss verschlüsselt erfolgen (z. B. mittels MIP, S/MIME).
- Beachten Sie Einschränkungen, die aus Vertraulichkeitserklärungen mit Dritten oder Urheberrechten resultieren.
- Sie müssen als Empfänger von Informationen sicherstellen, dass sensible Informationen nicht durch Unbefugte mitgelesen werden können (z. B. Sichtschutzfolie am Notebook).
- Sollten Sie Informationen erhalten, die nicht für Sie bestimmt sind, informieren Sie den Absender und löschen Sie diese Informationen.

Hinweis:

- Auch Informationen, die nicht sensibel sind, dürfen nur bei Bedarf an Externe kommuniziert und nicht ohne Genehmigung veröffentlicht werden.
- Die Information, ob eine Vertraulichkeitserklärung bzw. ein Geheimhaltungsvertrag vorliegt, muss Ihnen Ihr Vorgesetzter mitteilen.
- Informationen bzgl. zugelassener Kommunikationsmittel und Schutzmaßnahmen erhalten Sie von Ihrem Vorgesetzten.

5.1.5 Vernichten von Informationen

Das sorgsame Vernichten von Informationen und Daten am Ende des Lebenszyklus trägt dazu bei, dass sensible Information nicht in falsche Hände geraten.

- Löschen bzw. vernichten Sie Informationen, wenn Sie diese nicht länger benötigen. Achten Sie dabei auf gesetzliche Aufbewahrungsfristen.
- Für die Vernichtung von **vertraulichen** und **streng vertraulichen** Informationen sollten Sie einen geeigneten Schredder / Aktenvernichter benutzen. Alternativ können Sie bei **vertraulichen** Informationen die auf-gestellten Datenschutztonnen verwenden.
- Für die **streng vertraulicher** Informationen müssen Sie eine angemessen sichere Methode zur Vernichtung nutzen.
- Verwenden Sie ein Verfahren zum sicheren Löschen von **streng vertraulichen** Informationen.
- Für die sachgerechte Vernichtung von Datenträgern wenden Sie sich an den RWE IT Service Desk.

Hinweis:

- Nicht sensible Informationen können über den normalen Papierkorb entsorgt werden.
- Für die Vernichtung von „**streng vertraulichen**“ Informationen kann z.B. einen Schredder/Aktenvernichter der Stufe 3 Cross-Cut oder höher (nach DIN 32757) verwendet werden.
- Kontaktieren Sie im Zweifelsfall Ihren RWE-Ansprechpartner, um Aufbewahrungsfristen und die sachgerechte Entsorgung von Informationen zu klären.
- Kontaktieren Sie den RWE IT Service Desk bei Fragen zum sicheren Löschen von Daten.

5.2 Sichere Kommunikation

Der Austausch von Informationen gehört zur täglichen Arbeit. Dabei muss allerdings auch die Sicherheit der Informationen gewährleistet werden. Es ist daher wichtig, bei jeglicher Kommunikation angemessene Maßnahmen zu beachten bzw. zu ergreifen.

5.2.1 E-Mails und Messenger

E-Mail-Verkehr dient nicht nur zur Kommunikation, vielmehr werden hierüber geschäftsrelevante und sogar geschäftskritische Vorgänge geregelt. Deshalb ist es notwendig, E-Mails mit sensiblen Informationen zu schützen.

- Nutzen Sie für betriebliche E-Mails ausschließlich das von RWE bereitgestellte E-Mail-Konto.
- Verwenden Sie in jedem Fall eine digitale Signatur bei zu übermittelnden Nachrichten und Daten, bei denen Ihre Identität als Absender oder die Unverfälschtheit der Nachricht zweifelsfrei feststehen muss.
- Sie müssen E-Mails mit sensiblen Informationen in jedem Fall verschlüsseln (MIP, S/MIME oder gleichwertige Verschlüsselungsprogramme).
- Nutzen Sie nur die in der RWE-Gruppe genehmigten Messenger für die Kommunikation dienstlicher Informationen. Es gelten die gleichen Anforderungen an die Verschlüsselung von vertraulichen Dokumenten, die auch für E-Mails gelten.

- Es ist Ihnen untersagt, eine automatische Weiterleitung von betrieblichen E-Mails an Nicht-RWE-Mailadressen einzurichten.

Hinweise:

- Sollte eine E-Mail bei der automatischen Prüfung einen SPAM-Verdacht ergeben, wird diese z. B. mit „SPAM“ in der Betreff-Zeile gekennzeichnet.
- Trotz aller Sorgfalt kann es vorkommen, dass „korrekte“ E-Mails fälschlicherweise als SPAM gekennzeichnet werden. Bitte prüfen Sie daher auch die mit SPAM gekennzeichneten E-Mails und ihren „Junk-E-Mail“ Ordner regelmäßig.
- Seien Sie kritisch, wenn Sie eine E-Mail z. B. mit einer Aufforderung erhalten, persönliche Daten einzugeben. Führen Sie keine Aktionen aus, zu denen Sie von Unbekannten über E-Mail aufgefordert werden. Verknüpfungen (Links) in solchen E-Mails leiten Sie häufig auf gefälschte Webseiten weiter und dienen zum Diebstahl der dort eingegebenen Informationen oder können Ihren Rechner mit einer Schadsoftware infizieren.
- Melden Sie verdächtige E-Mails über die Hoxhunt-Schaltfläche (sofern aktiviert) in Outlook oder schreiben Sie an spam@rwe.com bzw. csirt@rwe.com.

5.2.2 Telefon- und Videokonferenzen

Auch bei Telefon- und Videokonferenzen werden Informationen geteilt. Diese Konferenzen finden häufig mit mehreren Teilnehmern statt. Es ist daher wichtig, die Sicherheitsvorgaben einzuhalten.

- Sie müssen sicherstellen, dass bei Telefon- und Video-Konferenzen keine sensiblen Informationen an Unbefugte gelangen können (z. B. Einwahl mit PIN).
- Prüfen Sie vor einer Telefon- oder Videokonferenz den Teilnehmerkreis.

- Achten Sie darauf, dass keine unbefugten Personen während Besprechungen, bei Telefonaten, im Hotelzimmer, im Wartebereich am Flughafen, im Zug oder im Taxi mithören.

- Besprechungen von streng vertraulichen Informationen sind in der Öffentlichkeit nicht zu führen.

Hinweise:

- Kontaktieren Sie Ihren RWE IT Service Desk bei Fragen zu sicheren Telefon- und Videokonferenzlösungen.

- Wenn Ihr Gesprächspartner mit dem Vorgang vertraut ist, versteht er Sie auch, ohne dass Sie Details oder konkrete Namen nennen.

5.2.3 Besprechungen

Bei Besprechungen werden Informationen mit anderen Personen ausgetauscht. Daher sind folgende Sicherheitsmaßnahmen zu beachten.

- Bei Besprechungen sind sensible Informationen nur unter den berechtigten Teilnehmern auszutauschen.
- Sie müssen den Teilnehmerkreis kennen, insbesondere sollten Sie wissen, wer RWE-Mitarbeiter ist und wer nicht.
- Besprechungsräume, in denen sich sensible Informationen befinden, müssen abgeschlossen sein, wenn sie nicht benutzt werden.

- Am Ende einer Besprechung hat der Sitzungsleiter/Organisator dafür zu sorgen, dass keine Unterlagen, Informationen auf Whiteboards oder Flipcharts sowie keine mitgebrachten mobilen IT-Komponenten zurückbleiben.
- Als Organisator und Sitzungsleiter müssen Sie prüfen, ob in Veranstaltungen **„streng vertrauliche“** Informationen ausgetauscht werden. Wenn ja, so sind hierfür Räume zu nutzen, die von außen nicht einsehbar sind und das mithören erschweren (z.B. geschlossene Tür).

- Achten Sie darauf, dass Teilnehmer keine externen IT Komponenten (z. B. mobile Geräte, USB Sticks etc.) mit der RWE Infrastruktur (z. B. RWE Notebook oder Netzwerk) verbinden. Die Nutzung von RWE Beamern und Bildschirmen ist von dieser Regelung nicht betroffen.

Hinweise:

- Achten Sie darauf, dass in Besprechungspausen die Räume nicht unbeaufsichtigt sind.
- Kontaktieren Sie Ihren zuständigen RWE-Ansprechpartner bei Fragen zu geeigneten sicheren Räumen.

5.2.4 Internet

Das Verhalten der Mitarbeiter bei der Nutzung des Internets trägt entscheidend zum Schutz der Informationen bei.

- Sie sind verpflichtet, das Internet ausschließlich über die dafür vorgesehenen und mit Schutzeinrichtungen (u. a. Firewall) gesicherten Zugangswege Ihres RWE IT-Dienstleisters zu nutzen.

- Es ist Ihnen untersagt, die von Ihrem RWE IT-Dienstleister eingerichtete Konfiguration zur Nutzung des Internets zu verändern. Nur dieser hat die Berechtigung, die Internet-Zugriffssoftware zu installieren und zu konfigurieren.

Hinweise:

- Der Abruf oder die Speicherung bestimmter Inhalte (z.B. jugendgefährdende Inhalte, Glücksspiel) im Internet kann strafrechtlich verfolgt werden. Bedenken Sie, dass dies arbeitsrechtliche Konsequenzen nach sich ziehen kann.

- Wenn Sie bei der Nutzung Ihres Browsers auf RWE-eigener Infrastruktur (z. B. RWE-Laptop oder -Netzwerk) Unregelmäßigkeiten feststellen, informieren Sie bitte den RWE IT Service Desk.

5.2.5 Social Media

Die in Social Media (z. B. Facebook und Instagram) eingestellten Informationen sind einem größeren Personenkreis öffentlich zugänglich. Oftmals ist es für Außenstehende nicht erkennbar, ob es sich um berufliche / private Meinungsäußerungen handelt.

- Kennzeichnen Sie private Äußerungen zu RWE deutlich als Ihre persönliche Meinung (z. B. „ich meine“ oder „meine persönliche Meinung hierzu ist …“).

- Geben Sie niemals betriebliche Informationen in Sozialen Medien preis. Dies gilt auch für nicht sensible Informationen. Diese können Auswirkungen auf das Unternehmen haben und beispielsweise den Aktienkurs der RWE AG beeinflussen.
- Teilen Sie keine Bilder oder Videos, auf denen Sicherheitseinrichtungen (z. B. Umzäunung, Kameratechnik, Schrankenanlagen etc.) erkennbar sind.
- Kommunizieren Sie keinesfalls sensible Informationen in Social Media.

Hinweise:

- Bedenken Sie, dass z. B. Beleidigungen/Verleumdungen in Bezug auf den Arbeitgeber arbeitsrechtliche Konsequenzen nach sich ziehen können. Gleiches gilt für die Verletzung von Betriebs- und Geschäftsgeheimnissen.
- Seien Sie wachsam, wenn Sie persönliche Informationen veröffentlichen! Angreifer können versuchen, diese Informationen auszuspähen, um sie für einen Angriff (z. B. Phishing) zu verwenden.

5.3 Sicherer Umgang mit IT-Komponenten und Zugängen

Eine Arbeit ohne IT-Komponenten und den Zugängen zu diesen ist heute nur noch schwer vorstellbar. Es ist daher umso wichtiger, die Sicherheit dieser Komponenten aufrechtzuerhalten.

5.3.1 Kennwörter und Zugriffsschutz

Kennwörter dienen der Identifizierung des Nutzers. Der Zugriffsschutz ist ein wichtiges Mittel, um die Vertraulichkeit von Informationen zu gewährleisten.

- Ändern Sie umgehend Standard- und Initialkennwörter.
- Nutzen Sie unterschiedliche Kennwörter für verschiedene Systeme und Anwendungen. Dies gilt nicht, sollten die unterschiedlichen Systeme oder Anwendungen ein sogenanntes Single Sign-on verwenden und kein einzelnes Anmeldeverfahren verlangen.
- Notieren Sie sich keine Kennwörter im Klartext (z. B. unverschlüsselt in einer Datei).
- Ihre Kennwörter müssen mindestens zwölf Zeichen lang sein.
- Verwenden Sie keine Tastaturmuster, Namen, Datumsangaben oder Begriffe aus Wörterbüchern. Nutzen Sie stattdessen etwa die Anfangsbuchstaben eines Satzes.
- Verwenden Sie – sofern technisch möglich – mind. drei der nachfolgenden Zeichentypen: Großbuchstaben, Kleinbuchstaben, Sonderzeichen und Ziffern.
- Achten Sie bei der Kennworteingabe darauf, dass niemand den Bildschirm oder die Tastatur einsehen kann.
- Sollten der Verdacht bestehen, dass Ihr Kennwort kompromittiert wurde, ändern Sie dieses unverzüglich und wenden Sie sich ggf. an den RWE IT Service Desk und oder ihren zuständigen RWE-Ansprechpartner.
- Sollten Sie bemerken, dass Ihnen fälschlicherweise Zugriff auf Daten, IT-Komponenten oder Anwendungen gewährt wird, so informieren Sie umgehend Ihren zuständigen RWE-Ansprechpartner.

- Versuchen Sie nicht, vorsätzlich Zugriff auf Daten zu erlangen, zu denen Sie keine Zugriffsberechtigung haben.

- Geben Sie Ihre Kennwörter niemals an andere Personen weiter. Hierzu zählen auch Kollegen, Ihre RWE-Ansprechpartner und der RWE IT-Dienstleister bzw. der RWE IT Service Desk.
- Überlassen Sie Ihre Zugänge niemals anderen Personen.
- Geben Sie Kennwörter niemals auf Ihnen unbekannte Webseiten oder in unbekannten Anwendungen ein.
- Verwenden Sie Zugangsdaten, wie Benutzername oder Kennwörter, die Sie im betrieblichen Umfeld nutzen, nicht außerhalb von RWE (z. B. im Internet).

Hinweise:

- Eine Möglichkeit zur Erstellung eines Kennworts besteht darin, ein Grundkennwort z. B. aus den Anfangsbuchstaben eines Satzes zu bilden. Der Satz „Im Sommer ist es meistens 30 Grad warm“ ergibt das Grundkennwort „ISiem30Gw“. Die anderen Kennwörter können dann systematisch davon abgeleitet werden, z. B. für SAP „ISiem30GwSAP“.
- Bitte denken Sie daran, ein anderes Grundkennwort, als das in diesem Beispiel genannte zu verwenden.

5.3.2 Nutzung von IT-Komponenten

Die für Ihre Arbeit zur Verfügung gestellten IT-Komponenten (Computer, Notebook, Smartphone, Tablets etc.) erfüllen die Vorgaben der Cybersecurity. Dieser Schutz kann nicht gewährleistet werden, wenn Sie Änderungen daran vornehmen oder andere Komponenten nutzen.

- Nutzen Sie bereitgestellte IT-Komponenten nur für betriebliche Tätigkeiten.

- Richten Sie ein Zugriffs- oder Gerätekennwort ein und aktivieren Sie eine vorhandene Bildschirm- bzw. Tastatursperre und schützen Sie den Zugang mit einem Kennwort.
- Verwenden Sie nur ordnungsgemäß lizensierte Standard-/Anwendungssoftware oder Daten (z. B. keine unberechtigten Kopien lizensierter Programme).
- Sie müssen eigenverantwortlich Systemupdates zeitnah installieren, wenn Sie dazu eine Aufforderung Ihres RWE IT-Dienstleisters erhalten.
- Sie müssen beim Verlassen Ihres Arbeitsplatzes durch Sperren des Rechners sicherstellen, dass kein Unberechtigter Ihren PC benutzen kann.
- Lassen Sie mobile IT-Komponenten niemals unbeaufsichtigt außerhalb Ihres Arbeitsplatzes liegen (z. B. in Meeting-Räumen oder der Bahn)
- Sichern sie Ihr Gerät gegen Diebstahl. Nutzen Sie dazu den bereitgestellten Diebstahlschutz (z. B. Kensington-Schloss) oder verschießen Sie das Büro beim Verlassen.
- Im Falle eines Verlustes, Diebstahls oder dem Verdacht einer nicht autorisierten Nutzung Ihrer IT-Komponenten, informieren Sie umgehend den RWE IT Service Desk.
- Für den Fernzugriff (Remote-Zugriff) müssen Sie eine verschlüsselte Anbindung (z. B. „VPN“ oder RWE VDI-Lösungen) zum Unternehmensnetz nutzen.
- Nutzen Sie öffentliche Netzwerke (z. B. WLAN) nur in Ausnahmefällen.
- Bei erforderlicher Reparatur oder Entsorgung von IT-Komponenten müssen Sie Ihren RWE IT Service Desk einschalten.
- Achten Sie darauf, dass die SIM-Karte entfernt wird (falls vorhanden) und die Daten gelöscht werden, wenn Sie eine mobile IT-Komponente zur Reparatur geben.

- Sie dürfen nicht eigenständig Hard- oder Software auf betrieblichen Komponenten installieren. Das ist Aufgabe des RWE IT-Dienstleisters.

- Es ist Ihnen nicht gestattet, Änderungen an IT-Komponenten (insbesondere sicherheitstechnische Einstellungen) vorzunehmen.
- Betriebsfremde IT-Komponenten (z. B. Notebooks) dürfen nicht an die RWE IT-Infrastruktur angeschlossen werden.
- Die Verarbeitung von Unternehmensdaten auf Smartphones ist nur mit Geräten gestattet, auf denen die RWE Mobile-Device-Management-(MDM)-Lösung installiert ist.
- Die Synchronisation von betrieblichen Daten zu anderen Geräten/IT-Komponenten oder in nicht vom Unternehmen lizensierte Cloud-Services ist nicht erlaubt.
- Nicht vom Unternehmen lizensierte und freigegebene Cloud-Speicher-Services (etwa Storage-Angebote wie „Dropbox“ oder „Google Drive“ etc.) dürfen Sie nicht verwenden.

Hinweis:

- Wenn Ihnen ein RWE-Laptop zugewiesen wurde, berechtigt Sie der Status als „lokaler Administrationsbenutzer“ nicht dazu, die von dem RWE IT-Dienstleister festgelegten Schutzmaßnahmen zu ändern.
- Sie können Ihren Rechner u. a. mit Hilfe der Tastenkombination „Windows-Taste + L“ sperren.

5.3.3 Schutz vor Schadprogrammen

Schadprogramme stellen eine Gefahr für die Cyber Security dar. Ihre Verbreitung erfolgt über das Internet, per E-Mail oder über mobile Datenträger.

- Öffnen Sie keine Dateien aus nicht vertrauenswürdigen Quellen – z. B. von Anhängen aus E-Mails unbekannter Herkunft oder von mobilen Datenträgern – und geben sie diese nicht weiter.
- Kontaktieren Sie sowohl bei Verdacht, als auch bei identifiziertem Schadprogrammbefall, umgehend den RWE IT Service Desk.

- Es ist Ihnen untersagt, die Schutzmaßnahmen des RWE IT-Dienstleisters gegen Schadprogramme außer Kraft zu setzen, zu modifizieren oder zu umgehen.

Hinweise:

- Prüfen Sie Informationen/Daten, die Sie aus externer Quelle erhalten vor dem ersten Öffnen z. B. mit dem Virenscanner Ihres Arbeitsplatzrechners. Ihr RWE IT Service Desk unterstützt Sie gerne.
- Unerklärliches Systemverhalten einer IT-Komponente (häufige Fehlermeldungen, Programmabstürze, Rechnerabstürze etc.) kann ein Hinweis auf einen Befall durch Schadprogramme sein. Auch wenn beispielsweise gehäuft Popup-Fenster mit zweifelhaften Werbeangeboten erscheinen, informieren Sie unmittelbar den RWE IT Service Desk.
- Melden Sie verdächtige E-Mails über die Hoxhunt-Schaltfläche (sofern aktiviert) in Outlook oder schreiben Sie an spam@rwe.com bzw. csirt@rwe.com.

5.3.4 Verwendung von Apps auf Smartphones und Tablets

Als App wird eine Softwareapplikation für Mobilgeräte wie Smartphones und Tablets bezeichnet.

- Auf Dienstgeräten des RWE-Konzerns ist die Installation und nicht-dienstliche Nutzung von Installationsplattformen/App Stores nur dann erlaubt, wenn Unternehmensdaten durch geeignete technische/organisatorische Maßnahmen geschützt sind (z. B. durch die Verwendung von Intune).
- Die Installation ist dabei nur aus regulären Installationsplattformen/App Stores erlaubt.
- Es dürfen nur lizensierte oder lizenzfreie Anwendungen genutzt werden.
- Halten Sie installierte Apps auf dem aktuellen Stand, insbesondere bei sicherheitsrelevanten Updates vom Softwarehersteller.

- Die Installation oder Nutzung von Tools oder Werkzeugen, die die Systemsicherheit mobiler IT-Komponenten in Frage stellen (z. B. Jailbreak, Root-Modus) ist verboten.
- Die Installation oder Nutzung von Apps, die die Sicherheit des Geräts gefährden oder gefährden können, ist untersagt.

Hinweis:

- Bei Fragen zu Mobile Device Management (z. B. MobileIron) wenden Sie sich bitte an den RWE IT Service Desk.

5.3.5 Mobile Datenträger

Bei Informationen auf mobilen Datenträgern ist die Vertraulichkeit durch Verlust, Diebstahl oder Weitergabe gefährdet.

- Nutzen Sie ausschließlich mobile Datenträger (z. B. USB-Sticks) die Ihnen von RWE bereitgestellt wurden.
- Nutzen Sie mobile Datenträger nur, wenn es keine sinnvolle Alternative dazu gibt („Minimalprinzip“).
- Sie müssen sicherstellen, dass bei Weitergabe von Informationen auf mobilen Datenträgern keine weiteren Daten auf den Datenträger vorhanden sind.
- Daten auf mobilen Datenträgern sind vor unerlaubten Zugriffen zu schützen (z. B. durch den Einsatz von Verschlüsselung).
- Beim Erhalt/Versand von mobilen Datenträgern mit integriertem Kennwortschutz müssen Sie das Kennwort über einen separaten Kommunikationskanal übermitteln (z. B. über eine verschlüsselte E-Mail).
- Sensible Informationen dürfen nur auf verschlüsselten mobilen Datenträgern gespeichert werden.
    - Für den Austausch von Informationen mit RWE muss ein sicherer Dokumentenaustausch (sicherer Datenraum) verwendet werden.

- Sensible Informationen müssen sicher gelöscht werden.

- Ohne weitergehende Überprüfung, nach Herkunft und Virenscan, dürfen Sie mobile Datenträger nicht an betriebliche IT-Komponenten anschließen. Kontaktieren Sie im Zweifelsfall Ihren RWE IT Service Desk.

Hinweis:

- Der Versand mobiler Datenträger sollte nur in Ausnahmefällen und ausschließlich an berechtigte Personen (z. B. Mitglieder in einem Projekt) erfolgen.
- Bei Fragen zur sicheren Löschung von Daten wenden Sie sich an den RWE IT Service Desk.

5.3.6 Datensicherung

Der Schutz gesicherter Daten muss gewährleistet sein. Dies gilt insbesondere für sensible Informationen, um potentiellem Schaden vorzubeugen.

- Speichern Sie Ihre Daten auf einem operativen Server sowie auf Laufwerken, die von Ihrem zuständigen RWE-Ansprechpartner bereitgestellt oder freigegeben wurden. Dort sichert der RWE IT-Dienstleister diese automatisch und fachgerecht.
- Sie sind für die Datensicherung von lokal gespeicherten Informationen selbst verantwortlich.
- Datensicherungen auf Datenträgern mit **sensiblen** Informationen müssen unter Verschluss aufbewahrt werden.
- Daten, die nur auf mobilen IT-Komponenten gespeichert sind, sollten Sie regelmäßig – am besten wöchentlich – sichern. Die Datensicherung ist gegen Zugriff mit einem Kennwort zu schützen und zu verschlüsseln. Beachten Sie bei der Sicherung von Daten die gesetzlichen Aufbewahrungsfristen.

- Die Sicherung von betrieblichen und sensiblen Informationen in nicht vom Unternehmen lizensierten und freigegebenen Cloud-Services ist nicht erlaubt. Wenden Sie sich im Zweifelsfall an Ihren RWE IT Service Desk.

Hinweise:

- Kontaktieren Sie Ihren zuständigen RWE-Ansprechpartner, um Aufbewahrungsfristen und die sachgerechte Entsorgung von Informationen zu klären.

5.4 Sicherheit auf Dienstreisen

Auf Dienstreisen sind IT-Komponenten und Informationen einem erhöhten Risiko ausgesetzt. Es ist daher unerlässlich, die folgenden Maßnahmen umzusetzen, um dadurch einen erhöhten Schutz zu gewährleisten.

5.4.1 Während der Reise

Auf Dienstreisen ist der achtsame Umgang mit mobilen IT-Komponenten und sensiblen Informationen notwendig.

- Wenn Sie von unterwegs arbeiten, müssen Sie sicherstellen, dass Unbefugte Informationen nicht „mitlesen“ können (z. B. Sichtschutzfolie am Notebook).
- Transportieren Sie mobile IT-Komponenten, sensible Informationen und Daten immer im Handgepäck.
- Schalten Sie Ihr Notebook immer vollständig aus und sichern Sie es physisch vor Diebstahl (z. B. mit einem Kensington Lock an stationären Gegenständen).
- Bewahren Sie mobile IT-Komponenten und sensible Informationen, wenn möglich, im Zimmersafe des Hotels auf.
- Nutzen Sie nur verschlüsselte Verbindungen für den Zugriff auf das RWE-Netzwerk, z. B. die RWE VPN-Verbindung mit Ihrem Notebook, denn

hiermit können Sie gefahrlos in WLAN-Netzwerken arbeiten. Verzichten Sie auf die Nutzung öffentlicher, ungesicherter WLAN-Netzwerke.

- Werden Sie zur Abgabe von Handy, Smartphone oder Tablet im Rahmen von Terminen mit Geschäftspartnern aufgefordert, schalten Sie vor Abgabe Ihr Gerät vollständig aus und entfernen Sie die SIM-Karte.
- Sensible Informationen müssen auch auf Dienstreisen sicher vernichtet werden. Entsorgen Sie diese im Zweifelsfall nach Ende der Reise im Büro auf dem üblichen Weg.

- Es ist Ihnen untersagt, mobile IT-Komponenten dem Hotelpersonal zu überlassen.
- Verwahren Sie mobile IT-Komponenten nicht offen sichtbar (z. B. im Hotelzimmer).

Hinweise:

- Sollte kein Zimmersafe verfügbar sein, verstauen Sie Ihre sensiblen Informationen im verschlossenen Reisegepäck.

5.4.2 Nach der Reise

Auch nach Ende der Reise sind Maßnahmen zum Schutz der IT-Komponenten und Informationen umzusetzen.

- Sie müssen umgehend – sofern es Ihnen während der Reise nicht möglich war – sicherheitsrelevante Vorfälle oder Beobachtungen an den RWE IT Service Desk melden.

- Es ist Ihnen nicht erlaubt, mobile IT-Komponenten zu nutzen, wenn Sie den begründeten Verdacht haben, dass diese manipuliert worden sind. Nehmen Sie unbedingt und unmittelbar Kontakt mit Ihrem RWE IT Service Desk auf.

5.5 Meldungen von Sicherheitsvorfällen

Durch das Melden und Auswerten von Sicherheitsvorfällen kann die Sicherheitslage besser eingeschätzt werden. Hierdurch können notwendige Anpassungen an den Regeln erkannt und vorgenommen werden.

- Wenn Sie einen Sicherheitsvorfall feststellen (z. B. Verlust sensibler Daten, Diebstahl von Hardware mit sensiblen Informationen, verdächtiges Verhalten Ihrer IT-Komponenten) oder einen möglichen Social-Engineering-Vorfall vermuten, melden Sie dies umgehend dem RWE IT Service Desk und informieren Sie Ihren zuständigen RWE-Ansprechpartner.
- Melden Sie verdächtige E-Mails über die Hoxhunt-Schaltfläche (sofern aktiviert) in Outlook oder schreiben Sie an spam@rwe.com bzw. csirt@rwe.com.

6 Außer Kraft gesetzte / Mitgeltende Konzernregelungen

6.1 Außer Kraft gesetzte Konzernregelungen

-/-

6.2 Mitgeltende Konzernregelungen

– Konzernrichtlinie Cyber Security (GDI_008)

7 Anhänge

Anhang 1: Klassifikation des Schutzbedarfs einer Information

Anhang 1: Klassifikation des Schutzbedarfs einer Information

Klassifizierung	Öffentlich (Public)	Intern (Internal)	Vertraulich (Confidential)	Streng vertraulich (Strictly confidential)
Schutzbedarf	Kein Schutzbedarf	Niedrig bis Mittel	Hoch	Sehr Hoch
Mögliche Auswirkungen	Keine	– Sehr geringe Auswirkungen auf RWE, die Beschäftigten und seine Kunden und Geschäftspartner	– Verletzung von Persönlichkeitsrechten – Erhebliche Störung / Abbruch einer wertwichtigen Geschäftsbeziehung – Wichtige Aufgaben können nur noch eingeschränkt wahrgenommen werden	– Massive Verletzung von Persönlichkeitsrechten, schwerer Ansehensverlust. – Erhebliche Störung / Abbruch einer wertwichtigen Geschäftsbeziehung mit Auswirkungen auf andere Geschäftsbeziehungen. – Wichtige Aufgaben können nicht mehr wahrgenommen werden.
Beispiele	– Produktinformationen – Pressemitteilungen – Externe Stellenanzeigen – Namen und dienstliche Kontaktinformationen von Mitarbeitern mit Verbindungen zur Öffentlichkeit (z. B. Ansprechpartner Recruiting, Referenten, Pressesprecher)	– Kommunikation in der RWE-Gruppe – Interne Richtlinien – Prozessbeschreibungen – Adressbücher – Organigramme – Personalnummer & R-UI	– Technische Dokumentationen – Kundendaten – Einsatzpläne – Sicherheitskonzept (z.B. für die HV) – unveröffentlichte Sicherheitsvorfälle – Persönliche Informationen zum Beschäftigungsverhältnis (z. B. Gehaltsdaten) – Bankverbindungsdaten	– M&A Projekte – Geschäftsentwicklungsprojekte – Geschäftsgeheimnisse (z.B. Patentanträge) – Compliance Sachverhalte – Daten der Arbeitsmedizin – Biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person – Daten zum Sexualleben oder der sexuellen Orientierung – Strafrechtliche Verurteilungen und Straftaten

Klassifizierung	Öffentlich (Public)	Intern (Internal)	Vertraulich (Confidential)	Streng vertraulich (Strictly confidential)
Weitergabe	Informationen in dieser Kategorie unterliegen keiner Einschränkung.	Informationen in dieser Kategorie dürfen nur innerhalb der RWE-Gruppe und mit relevanten externen Geschäftspartnern verwendet werden.	Informationen in dieser Kategorie dürfen ausschließlich Instanzen und/oder Mitarbeitern zugänglich gemacht werden, die diese Daten zur Erledigung ihrer Aufgaben benötigen.	Informationen in dieser Kategorie dürfen nicht nach außen gelangen und sind ausschließlich nach dem „Need-to-Known“ Prinzip weitergegeben werden.
Kennzeichnung	Öffentliche Informationen müssen nicht gekennzeichnet, aber nur von den autorisierten Geschäftsfunktionen (Unternehmenskommunikation) eingestuft und veröffentlicht werden.	Interne Informationen müssen mindestens auf dem Deckblatt mit dem Hinweis "Intern" oder "nur für den internen Gebrauch" gekennzeichnet werden.	Vertrauliche Informationen müssen auf jeder Seite oder auf jedem Teil der Information eindeutig mit dem Hinweis "vertraulich" gekennzeichnet werden. Datenträgers müssen entsprechend gekennzeichnet werden.	Streng vertrauliche Informationen müssen auf jeder Seite oder auf jedem Teil der Information eindeutig mit dem Hinweis "streng vertraulich" gekennzeichnet werden.