

Dokumentart:	Dokumentbezeichnung:	Vertraulichkeitsklasse:	Anlagen:	Anzahl Seiten:
Richtlinie	RL1101	Medium (C2)	0	14
Erstellt durch:	Dokumentverantwortung:	Genehmigt von:	Version:	Gültig ab:
Daniel Fitzner	Herr Giesecking Leiter IT	Herr Landeck Geschäftsführung	1.0	01.07.2021

INFORMATIONSKLASSIFIZIERUNG, -KENNZEICHNUNG UND -HANDHABUNG

Zusammenfassung

Diese Richtlinie gibt einen Rahmen für die Klassifizierung von unstrukturierten Informationen (z.B. Office-Dokumente, E-Mails, PDF-Dateien usw.) auf der Grundlage ihrer Vertraulichkeitsstufe (Vertraulichkeit und Geheimhaltung) mit dem Ziel vor, die Stromnetz Berlin GmbH, deren Eigentümer, Mitarbeiter*innen, Partner, Kunden und die Gesellschaft, in der wir tätig sind, zu schützen.

Die Stromnetz Berlin GmbH klassifiziert, kennzeichnet und handhabt Informationen hinsichtlich drei verschiedener Perspektiven: um die Stromnetz Berlin GmbH, die Gesellschaft und den Einzelnen zu schützen. Alle Regeln zur Klassifizierung, Kennzeichnung und Handhabung geben diese Perspektiven wieder.

Die Klassifizierung von Informationen dient dazu, grundlegende Sicherheitsmaßnahmen für den Schutz von Informationen sowie Anweisungen für die Handhabung von Informationen festzulegen. Es ist wichtig, dass Informationen zutreffend, also für die richtige Stufe, klassifiziert werden. Eine Überklassifizierung, also die Klassifizierung für eine Stufe, die über derjenigen liegt, die eigentlich zutrifft, bedeutet höhere Kosten für die Stromnetz Berlin GmbH und sollte vermieden werden.

Dokumentbezeichnung:	Dokumenttitel:	Version:	Seitenzahl:
RL1101	Informationsklassifizierung, -kennzeichnung und -handhabung	<Nr.>	2 (12)

INHALT

1	Änderungshinweise.....	4
2	Ziel und Zweck.....	4
3	Geltungsbereich.....	4
4	Copyright	4
5	Klassifizierung, Kennzeichnung und Handhabung von Informationen.....	4
6	Funktionen und Zuständigkeiten	5
6.1	Management	5
6.2	Mitarbeiter*innen	5
6.3	Verfasser von Informationen.....	5
6.4	Business Information Security Officer (BISO)	5
6.5	Datenschutzbeauftragter	5
7	Klassifizierung von Informationen.....	6
7.1	Klassifizierungsstufen bezogen auf die geschäftliche Perspektive	6
7.2	Klassifizierungsstufen bezogen auf die individuelle Perspektive	6
8	Kennzeichnung von Informationen	7
9	Klassifizierungsmatrix	8
10	Handhabung von Informationen	9
10.1	Wer ist zum Zugriff auf die Informationen berechtigt?	9
10.2	Anweisungen für Handhabung von Informationen.....	10
	Anhang.....	12
I	Abkürzungen, Definitionen	12
II	Abbildungsverzeichnis	12
III	Tabellenverzeichnis	12
IV	Revisionsverzeichnis	12

Dokumentbezeichnung:	Dokumenttitel:	Version:	Seitenzahl:
RL1101	Informationsklassifizierung, -kennzeichnung und -handhabung	<Nr.>	3 (12)

1 Änderungshinweise

Alle Änderungshinweise aus älteren Versionen sind im Anhang IV Revisionsverzeichnis, Tabelle Anhang IV-1 Revisionsverzeichnis abgelegt.

Tabelle 1-1 Änderungsübersicht

Version	
Abschnitt	Thema

2 Ziel und Zweck

Der Zweck dieser Richtlinie besteht darin, die Klassifizierung, die Kennzeichnung und die Handhabung von Informationen bei der Stromnetz Berlin GmbH darzulegen, einschließlich des Aufbaus, Anwendungsbereichs, der Rollen und Zuständigkeiten. Durch die konsequente Verwendung geeigneter Verfahren für die Klassifizierung, Kennzeichnung und Handhabung von Informationen verringert die Stromnetz Berlin GmbH das Risiko, dass Informationen gegenüber einer nicht autorisierten Partei offengelegt werden.

3 Geltungsbereich

Diese Richtlinie gilt für alle Mitarbeiter*innen der **Stromnetz Berlin GmbH**. Verantwortlich für Erstellung bzw. Aktualisierung dieses Dokuments ist die IT (EXI) der SNB. Die förmliche In- und Außerkraftsetzung sowie wesentliche inhaltliche Änderungen obliegen der Geschäftsführung der Stromnetz Berlin GmbH.

4 Copyright

Alle Inhalte dieser Richtlinie inklusive der Abbildungen, Zeichnungen [Tabellen, Diagramme usw.] und Anlagen unterliegen, sofern nicht anders angegeben, urheberrechtlichem Schutz. Es ist untersagt, sie ganz oder teilweise ohne ausdrückliche vorherige schriftliche Zustimmung der Stromnetz Berlin GmbH zu vervielfältigen, zu verbreiten, zu bearbeiten oder umzugestalten.

5 Klassifizierung, Kennzeichnung und Handhabung von Informationen

Informationen sind ein Vermögenswert, der für die Stromnetz Berlin GmbH von entscheidender Bedeutung ist. Es sind angemessene und geeignete Schritte zu unternehmen, um Informationen zu identifizieren und zu schützen, die vom Unternehmen stammen, dem Unternehmen gehören oder dem Unternehmen von anderen anvertraut wurden.

Diese Richtlinie bildet einen Rahmen für die Klassifizierung, Kennzeichnung und Handhabung unstrukturierter Informationen (z.B. Office-Dokumente, E-Mails, PDF-Dateien usw.) auf der Grundlage ihrer Vertraulichkeitsstufe (Vertraulichkeit und Geheimhaltung). Diese Richtlinie betrifft alle unstrukturierten Informationen unabhängig von ihrem Format (schriftlich, elektronisch, mündlich).

Dokumentbezeichnung:	Dokumenttitel:	Version:	Seitenzahl:
RL1101	Informationsklassifizierung, -kennzeichnung und -handhabung	<Nr.>	4 (12)

Die richtige Klassifizierung, Kennzeichnung und Handhabung von Informationen fällt in den Zuständigkeitsbereich aller Mitarbeiter*innen des Unternehmens, einschließlich Leiharbeitnehmer sowie Berater und Auftragnehmer.

Die Stromnetz Berlin GmbH unterteilt Informationen nach drei verschiedenen Perspektiven: aus Sicht des Unternehmens, aus Sicht der Gesellschaft und aus Sicht des Einzelnen. Diese Richtlinie gilt für die Stromnetz Berlin GmbH und deren Mitarbeiter*innen beim Klassifizieren, Kennzeichnen und der Handhabung unstrukturierter Informationen unter allen drei Perspektiven.

6 Funktionen und Zuständigkeiten

6.1 Management

Die Geschäftsführung und die Bereichsleiter sind für die Umsetzung dieser Richtlinie sowie für deren Einhaltung zuständig. Das Management ist:

- dafür zuständig, zu gewährleisten, dass in seinem Zuständigkeitsbereich ausreichende Anleitungen für das Klassifizieren, Kennzeichnen und die Handhabung unstrukturierter Informationen vorhanden sind.

6.2 Mitarbeiter*innen

Alle Mitarbeiter*innen der Stromnetz Berlin GmbH sind dafür zuständig, dass Informationen im Rahmen ihrer täglichen Arbeit gemäß dieser Richtlinie klassifiziert und gehandhabt werden. Alle Mitarbeiter*innen der Stromnetz Berlin GmbH müssen:

- erstellte Informationen gemäß dieser Richtlinie klassifizieren,
- die Informationen ihrer Vertraulichkeitsstufe entsprechend kennzeichnen,
- die Informationen gemäß dieser Richtlinie zu handhaben.

6.3 Verfasser von Informationen

Die Person, die die Information erstellt, also der/die Verfasser/in, ist für die Klassifizierung und Kennzeichnung der Information zuständig.

6.4 Business Information Security Officer (BISO)¹

Der Business Information Security Officer (BISO) ist dafür zuständig sicherzustellen, dass die Richtlinie zum Klassifizieren, Kennzeichnen und zur Handhabung von Informationen angemessen sind und auf dem aktuellen Stand gehalten werden. Der BISO hat dabei insbesondere auch die gesetzlichen und regulatorischen Vorgaben zu beachten.

6.5 Datenschutzbeauftragter (DSB)

Der/Die Datenschutzbeauftragte ist dafür zuständig, seine jeweilige Rechtseinheit bei der Klassifizierung, Kennzeichnung und Handhabung von Informationen, die personenbezogene Daten enthalten, zu unterstützen. Aufgabe des DSB ist die Beobachtung und Nachverfolgung von Änderungen der Datenschutzgesetze, die sich auf die in dieser Richtlinie aufgestellten Grundsätze auswirken können. Weitere Informationen finden sich in der Richtlinie zum Datenschutz RL1015.

¹ Die Rolle des BISO wird provisorisch beibehalten und im Zuge des Aufbau eines ISMS abgelöst.

Dokumentbezeichnung:	Dokumenttitel:	Version:	Seitenzahl:
RL1101	Informationsklassifizierung, -kennzeichnung und -handhabung	<Nr.>	5 (12)

7 Klassifizierung von Informationen

7.1 Klassifizierungsstufen bezogen auf die geschäftliche Perspektive

Die Informationsklassifizierung muss auf den Auswirkungen für das Geschäft der Stromnetz Berlin GmbH, die sich aus einer absichtlichen oder unabsichtlichen Veröffentlichung der Informationen ergeben können, basieren.

Bei der Klassifizierung muss der Verfasser die möglichen Auswirkungen berücksichtigen, die die Stromnetz Berlin GmbH betreffen können, wenn Informationen absichtlich oder unabsichtlich gegenüber unbefugten Personen offengelegt werden. Dies betrifft die folgenden Aspekte und Auswirkungen:

- Reputationsrisiken (Markenwert, Betriebslizenz)
- Finanzen
- Umwelt, Gesundheit und Sicherheit
- Geschäftsbetrieb
- Recht, Compliance (Konformität mit internen und externen Vorgaben) oder Verträge

Auf der Grundlage des Vorstehenden sind alle Informationen für eine der folgenden Vertraulichkeitsstufen zu klassifizieren (für weitere Informationen siehe Kapitel 10)

- C1 – Public
- C2 – Internal
- C3 – Restricted
- C4 – Strictly Confidential

Wenn die Informationen wirtschaftlich sensible und/oder wirtschaftlich vorteilhafte Informationen enthalten, die DSO vertraulich behandeln muss, gilt die allgemeine Faustregel, die Informationen als „C3 – Restricted“ zu klassifizieren, es sei denn, sie wird in diskriminierungsfreier Weise veröffentlicht.

7.2 Klassifizierungsstufen bezogen auf die individuelle Perspektive

Die Informationsklassifizierung muss auf den Auswirkungen auf das Individuum, die sich aus einer absichtlichen oder unabsichtlichen Veröffentlichung der Informationen ergeben können, basieren. Personenbezogene Daten bezeichnen alle Angaben in Bezug auf eine identifizierte oder identifizierbare natürliche, lebende Person. Beispiele für personenbezogene Daten sind:

- Name
- Adresse
- IP-Adresse
- E-Mail-Adresse
- Standortdaten

Wenn die erstellten Informationen personenbezogene Daten enthalten, gilt die allgemeine Regel, die Informationen als „C3 – Restricted“ zu klassifizieren. Inhalt und Kontext der Verarbeitung personenbezogener Daten können sich jedoch auf die Klassifizierungsstufe auswirken.

Dokumentbezeichnung:	Dokumenttitel:	Version:	Seitenzahl:
RL1101	Informationsklassifizierung, -kennzeichnung und -handhabung	<Nr.>	6 (12)

Die Datenschutz-Grundverordnung (DSGVO) definiert eine Untergruppe personenbezogener Daten, die als besondere Kategorien personenbezogener Daten bezeichnet werden. Dies sind personenbezogene Daten, aus denen Folgendes hervorgeht:

- rassische und ethnische Herkunft
- politische Meinungen
- religiöse oder weltanschauliche Überzeugungen
- Gewerkschaftszugehörigkeit
- genetische Daten
- biometrische Daten
- Gesundheitsdaten
- Sexualleben und sexuelle Orientierung

Die allgemeine Faustregel ist, dass die Verarbeitung besonderer Kategorien personenbezogener Daten mit einem höheren Risiko verbunden ist. Wenn die erstellten Informationen eine dieser Kategorien enthalten, muss mit gebotener Sorgfalt in Betracht gezogen und bewertet werden, ob die Informationen als „C4 – Strictly Confidential“ zu klassifizieren sind oder zusätzliche Sicherheitsmaßnahmen angewendet werden sollten.

Es ist wichtig, dass Informationen zutreffend, also für die richtige Stufe, klassifiziert werden. Eine Überklassifizierung, also die Klassifizierung für eine Stufe, die über derjenigen liegt, die eigentlich zutrifft, bedeutet höhere Kosten für die Stromnetz Berlin GmbH und sollte vermieden werden

8 Kennzeichnung von Informationen

Die Klassifizierung jeder Information muss ordnungsgemäß und deutlich sichtbar gekennzeichnet werden. Der/die Verfasser/in der Information ist für die Kennzeichnung zuständig. Jegliche Informationen müssen mit einer der folgenden Kennzeichnungen basierend auf der Informationsklassifizierung versehen werden:

- C1 – Public
- C2 – Internal
- C3 – Restricted
- C4 – Strictly Confidential

Die Informationskennzeichnung gewährleistet, dass die Empfänger oder Nutzer der Informationen darauf hingewiesen werden, mit welcher Vertraulichkeitsklasse die Informationen klassifiziert sind und wie sie zu handhaben sind.

Bei mündlichen Informationen, die C3 – Restricted, C4 – Strictly Confidential betreffen, muss der Sender den Empfänger vor dem Informationsaustausch über die Vertraulichkeitsstufe informieren.

Jegliche Abweichung von den Kennzeichnungsregeln muss dokumentiert und vom ISMS-Koordinator genehmigt werden.

Dokumentbezeichnung:	Dokumenttitel:	Version:	Seitenzahl:
RL1101	Informationsklassifizierung, -kennzeichnung und -handhabung	<Nr.>	7 (12)

9 Klassifizierungsmatrix

Tabelle 2: Klassifizierungsmatrix

Klassifizierung	Auswirkung	Mögliche Anwendungsbereiche / Beispiele
C1 – Public	Informationen, die aus öffentlichen Quellen erlangt wurden oder von der Stromnetz Berlin GmbH mit der Intention erstellt wurden, sie zu veröffentlichen. Eine Veröffentlichung dieser Informationen hätte keine Folgen für das Unternehmen. Der ungefähre Umfang des möglichen finanziellen Schadens ist unerheblich.	Allgemein zugängliche Informationen
C2 – Internal	Ein unautorisierter externer Zugriff auf diese Daten ist zu verhindern. Sollten diese Informationen jedoch öffentlich werden, sind die Folgen geringfügig.	„Normale“ Arbeitsdokumente, unkritische Betriebstagebücher, die meisten Dokumentvorlagen Für personenbezogene Daten (mindestens C2 – Internal): Daten wie Namen, Adressen, IP-Adressen, E-Mail-Adressen, Standortdaten
C3 – Restricted	Unbefugter Zugriff könnte sich auf die operative Effektivität des Unternehmens auswirken, zu einem bedeutenden finanziellen Verlust führen, einem Konkurrenten einen erheblichen Vorteil verschaffen oder zu einem starken Rückgang des Kundenvertrauens führen. Für personenbezogene Daten (C3 – Restricted, risikoorientierte Abwägung): Ein unbefugter (externer oder interner) Zugriff auf personenbezogene Daten (beispielsweise Kundendaten oder Mitarbeiter*innendaten) würde die Rechte und die Freiheit einer Einzelperson gefährden. Falsche Handhabung personenbezogener Daten kann zu Geldbußen, negativer Publicity	Verträge, Informationen über Expansionsvorhaben, Rechnungslegungsdaten, Ergebnisse von Risikobewertungen, Budget, Auditinformationen, Dokumentationen der IT-Architektur Für personenbezogene Daten (mindestens C3 – Restricted): Daten wie Gehaltsinformationen, Zählermessdaten, Bankdaten, Kundennummern.

Dokumentbezeichnung:	Dokumenttitel:	Version:	Seitenzahl:
RL1101	Informationsklassifizierung, -kennzeichnung und -handhabung	<Nr.>	8 (12)

	<p>oder einer schwerwiegenden Verletzung von Rechtsnormen führen.</p> <p>Für wirtschaftlich sensible und/oder vorteilhafte Informationen gemäß den Entflechtungsvorschriften (C3 – Restricted):</p> <p>Die SNB muss die Vertraulichkeit sensibler Informationen, die sie im Rahmen der Ausübung der Geschäftstätigkeit zugehen, wahren und gleichzeitig verhindern, dass Informationen über eigene Aktivitäten, deren Offenlegung in diskriminierender Weise wirtschaftliche Vorteile bringen könnte, veröffentlicht werden. Die falsche Handhabung solcher Informationen kann zu negativer Publicity oder einer schwerwiegenden Verletzung von Rechtsnormen führen.</p>	<p>Für wirtschaftlich sensible und/oder vorteilhafte Informationen gemäß den Entflechtungsvorschriften (C3 – Restricted):</p> <p>Daten, die die SNB erlangt hat oder die von der SNB erstellt wurden, sind zum Beispiel: Informationen über Kunden, Preise, Vertragsbedingungen und Stromversorger.</p>
C4 – Strictly Confidential	<p>Ein unbefugter (externer oder interner) Zugriff auf Informationen hätte kritische Auswirkungen auf das Unternehmen. Wenn Informationen, die vertrauliche Daten enthalten, an Dritte weitergegeben werden, kann dies zu einem erheblichen finanziellen Verlust oder einem Kontrollverlust von Betriebsprozessen, unerwünschter negativer Publicity oder einer schwerwiegenden Verletzung von Rechtsnormen führen.</p>	<p>Informationen über Fusionen und Übernahmen, Einkaufspreise und Nachlässe, Geschäftspläne, Administratorpasswörter, Informationen über Personen mit geschützter Identität.</p>

10 Handhabung von Informationen

10.1 Wer ist zum Zugriff auf die Informationen berechtigt?

Basierend auf der Informationsklassifizierung gibt es verschiedene Anforderungen bezüglich der Frage, wie und mit wem die Informationen ausgetauscht werden können. Nachstehend finden Sie Vorschriften über die Handhabung von Informationen auf der Grundlage der Informationsklassifizierungsstufe:

- C1 – Public: Die Information wird als öffentliche Information behandelt und kann unter Befolgung der Kommunikationsrichtlinien ausgetauscht werden.
- C2 – Internal: Die Informationen werden als interne Informationen behandelt und dürfen nur innerhalb der Stromnetz Berlin GmbH ausgetauscht werden. Für den Austausch von Informationen der Stufe C2 mit externen Parteien sind geeignete Geheimhaltungsvereinbarungen (Non-Disclosure Agreements - NDA) erforderlich.

Dokumentbezeichnung:	Dokumenttitel:	Version:	Seitenzahl:
RL1101	Informationsklassifizierung, -kennzeichnung und -handhabung	<Nr.>	9 (12)

- C3 – Restricted: Die Informationen werden als eingeschränkte Informationen behandelt und dürfen nur mit einer eingeschränkten Gruppe von Einzelpersonen mit eingeschränktem Zugang ausgetauscht werden, sofern sie über diese Kenntnisse zur Erfüllung Arbeitsaufgaben verfügen müssen („need-to-know“). Für den Austausch von Informationen der Stufe C3 mit externen Partnern sind geeignete Geheimhaltungsvereinbarungen (Non-Disclosure Agreements - NDA) erforderlich.
- C4 – Strictly Confidential: Die Informationen werden als geheime Informationen behandelt und dürfen nur unter außerordentlicher Vorsicht mit nur wenigen, zuvor ausgewählten Einzelpersonen ausgetauscht werden. Über die Personen, mit denen Informationen ausgetauscht werden, sind Aufzeichnungen zu führen. Für den Austausch von Informationen der Stufe C4 mit externen Parteien sind geeignete Geheimhaltungsvereinbarungen (Non-Disclosure Agreements - NDA) erforderlich.

Für den Austausch wirtschaftlich sensibler und/oder wirtschaftlich vorteilhafter Informationen gemäß den Entflechtungsvorschriften sind Geheimhaltungsvereinbarungen (Non-Disclosure Agreements - NDA) mit den betreffenden Partnern unerlässlich. Solche Informationen dürfen jedoch niemals mit Wettbewerbsbereichen ausgetauscht werden.

Zusätzlich zu den vorstehenden Vorschriften bestehen die folgenden allgemeinen Grundsätze für klassifizierte Informationen:

- Der Informationseigentümer entscheidet, mit wem und wie die Informationen ausgetauscht werden können.
- Eine Person ist zum Zugriff auf die Informationen befugt, wenn sie
 - die Informationen zur Durchführung ihrer Arbeitsaufgaben benötigt (need-to-know)
 - ausreichende Kenntnis darüber besitzt, wie die Informationen zu handhaben sind

10.2 Anweisungen für Handhabung von Informationen

Für die Handhabung von Informationen sind die folgenden Instruktionen festgelegt:

- Für die Handhabung von Informationen, die als C1 – Public klassifiziert sind, bestehen keine Sicherheitsbeschränkungen bezüglich der Vertraulichkeit. Mitarbeiter*innen müssen jedoch stets die entsprechenden Kommunikationsrichtlinien befolgen.
- Die Handhabung von Informationen, die als C3 oder höher klassifiziert sind, richtet sich stets nach dem Prinzip der Erforderlichkeit für den Anwendungsbereich („need-to-know“) und ist gemäß den in der nachstehenden Tabelle beschriebenen Anweisungen zu handhaben.
- Für bestimmte Finanzinformationen, wie Unternehmensberichte oder vertrauliche Informationen zu Bepreisungen, gelten spezielle Offenlegungsanforderungen.

Tabelle 3: Anweisungen für die Handhabung von Informationen

ANWEISUNGEN FÜR DIE HANDHABUNG VON INFORMATIONEN					
	Fall	C1 – Public	C2 – Internal	C3 – Restricted	C4 – Strictly Confidential
Dokumente	Drucken von Dokumenten	✓	„Follow Me Print“ verwenden	„Follow Me Print“ verwenden	„Follow Me Print“ verwenden
	Scannen/Fotografieren/Kopieren von Dokumenten	✓	✓	Unter ständiger Aufsicht „Follow Me Print“ verwenden, wo möglich	Nicht erlaubt
	Papierdokumente im Büro	✓	Clear-Desk- (aufgeräumt) und Clear-Screen-Policy nach Büroschluss	Informationen nicht unbeaufsichtigt lassen (verschlossen in Büroschränken)	Verschlossen im Sicherheitsschrank/Safe mit eingeschränktem Zugang
	Papierdokumente/Geräte/Medien außerhalb des Büros (Telearbeit, Reisen)	✓	Unter Aufsicht	Unter ständiger Aufsicht, verschlossen in einem persönlichen Schrank/Safe	Unter ständiger Aufsicht, verschlossen im Privat- oder Hotelzimmersafe
	Zerstörung von physischen Medien (z. B. Papier, CD/DVD)	✓	Papierkorb/ Recyclingcontainer	Verschlossener Papierkorb/ Recyclingcontainer	Mithilfe eines Aktenvernichters vernichten
Kommunikation	Internes Versenden von E-Mails oder ² Textnachrichten	✓	✓	✓	Verschlüsselung verpflichtend
	Externes Versenden von E-Mails, Textnachrichten oder Faxnachrichten	✓	✓	Verschlüsselung verpflichtend	Verschlüsselung verpflichtend
	Physische Postsendungen	✓	Verschlossener Umschlag	Verschlossener Umschlag	Einschreiben (mit Rückschein)
	Video- und Web-Konferenzen	✓	✓	Risiko für Belauschung und Beobachtung bewerten	Verschlüsselung verpflichtend oder eigene, vom Unternehmen genehmigte Dienste
	Mündliche Kommunikation in Räumlichkeiten der Stromnetz Berlin	✓	✓	Risiko für Belauschung und Beobachtung bewerten	Risiko für Belauschung und Beobachtung bewerten
	Mündliche Kommunikation in der Öffentlichkeit	✓	Vermeiden	In der Öffentlichkeit vermeiden, Risiko für Belauschung bewerten	In der Öffentlichkeit vermeiden, Risiko für Belauschung bewerten
	Telefongespräch	✓	In der Öffentlichkeit vermeiden, Risiko für Belauschung bewerten	In der Öffentlichkeit vermeiden, Risiko für Belauschung bewerten	Von Group genehmigtes Verschlüsselungssystem verwenden
Elektronische Speicherung oder Übertragung	Speichern von Dateien bei intern genehmigten Diensten (beispielsweise SharePoint, OneDrive, Livelink)	✓	✓	✓	Nur zugriffsgeschützte und verschlüsselte Dateiablage (secure file share) verwenden ¹
	Speicherung von Dateien bei externen, nicht genehmigten Diensten (beispielsweise kommerzielle Cloud-Dienste wie Dropbox, Google Drive, Amazon Web Services)	✓	Vermeiden	Nicht erlaubt	Nicht erlaubt
	Speicherung von Dateien auf externen Medien einschließlich privater Geräte	✓	✓	Vom Unternehmen genehmigte Anwendung auf Mobilgeräten und Verschlüsselung auf USB-Sticks verwenden	Nur auf vom Unternehmen zur Verfügung gestellten und verschlüsselten USB-Sticks
	Dateiübertragung	✓	Verschlüsselung für externe Übertragung	Sichere Dateiübertragungsmöglichkeiten verwenden, Verschlüsselung für externe Übertragung	Verschlüsselung verpflichtend

² Die automatische externe Weiterleitung von E-Mails über das Internet ist nicht gestattet.

Anhang

I Abkürzungen, Definitionen

DSK	Datenschutzkoordinator
DSB	Datenschutzbeauftragter
DSO	Distribution System Operator (Verteilungsnetzbetreiber)
DSGVO	Datenschutz-Grundverordnung
ISK	ISMS-Koordinator
ISMS	Informationssicherheits-Managementsystem

II Abbildungsverzeichnis

Es konnten keine Einträge für ein Abbildungsverzeichnis gefunden werden.

III Tabellenverzeichnis

Tabelle 1-1 Änderungsübersicht	4
Tabelle 2: Klassifizierungsmatrix.....	8
Tabelle 3: Anweisungen für die Handhabung von Informationen	12
 Tabelle Anhang IV-1 Revisionsverzeichnis	 13
Tabelle Anhang IV-2 Übersicht Erstellung, Verantwortlicher, Prüfung und Genehmigung	14

IV Revisionsverzeichnis

Tabelle Anhang IV-1 Revisionsverzeichnis

Version n	
Abschnitt	Thema
Version n-1	
Abschnitt	Thema

Dokumentbezeichnung:	Dokumenttitel:	Version:	Seitenzahl:
RL1101	Informationsklassifizierung, -kennzeichnung und -handhabung	<Nr.>	12 (12)

Tabelle Anhang IV-2 Übersicht Erstellung, Verantwortlicher, Prüfung und Genehmigung

	Erstellt:	Verantwortet:	Genehmigt:
Datum:	25.06.2021	25.06.2021	28.06.2021
Durch:	Hr. Fitzner	Herr Giesecking	Herr Landeck