REINHAUSEN

Richtlinie
Klassifizierung und Handhabung von Informationen der REINHAUSEN Gruppe

Version 1.2 (01.04.2012)

Geltungsbereich:

Die vorliegende Richtlinie ist für alle Mitarbeiter der unten aufgeführten Gesellschaften (nachfolgend REINHAUSEN Gesellschaften) verbindlich. Sie richten sich ebenso an alle Lieferanten, an externe Dienstleister und Partnerunternehmen dieser Unternehmen, soweit dies nicht in den einzelnen Abschnitten anders angegeben ist.

Gesellschaft	Gültig ab
Maschinenfabrik Reinhausen GmbH	01.12.2009
Reinhausen Plasma GmbH	01.12.2009
Reinhausen Power Composites GmbH	01.12.2009
Highvolt Prüftechnik Dresden GmbH	14.06.2010
Messko GmbH	14.06.2010
MR China Ltd.	14.06.2010
MR do Brasil Ltd.	14.06.2010
MR Japan Corp.	14.06.2010
MR Manufacturing Inc.	14.06.2010
MR Russland (OOO MR)	14.06.2010
PT Reinhausen Indonesia (RID)	01.04.2012
Reinhausen 2e d.o.o. (RSI)	01.04.2012
Reinhausen Asia-Pacific Sdn Bhd.	14.06.2010
Reinhausen Australia Pty. Ltd.	14.06.2010
Reinhausen Canada Inc.	14.06.2010
Reinhausen Italia S.r.l.	14.06.2010
Reinhausen Korea Ltd.	14.06.2010
Reinhausen Luxembourg S.A.	14.06.2010
Reinhausen Manufacturing Inc.	14.06.2010
Reinhausen Middle East FZE	14.06.2010
Reinhausen South Africa (Pty) Ltd.	14.06.2010

Dokumentenverlauf

Version	Datum	Autor	Kommentare
0.10	06.09.2009	Andreas Schnitzer HvS-Consulting	1. Entwurf
0.20	07.09.2009	FID Dr. Bauer Andreas Schnitzer	Überarbeitung
0.30	14.09.2009	FID Dr. Bauer	Überarbeitung
1.00	04.11.2009	FID Dr. Bauer Andreas Schnitzer	Überarbeitung
1.10	11.05.2010	FID Dr. Bauer	Überarbeitung Abschnitte 4.2, 5.2 und 6.
1.20	28.03.2012	FID Dr. Bauer	Gesellschaft JEPC gelöscht, RSI und RID aufgenommen In Tabelle unter 4.2 Personenbezogene Daten gem. Bundesdatenschutzgesetz ergänzt Überarbeitung Abschnitt 6.

Freigabe

Version 1.0 wurde am 26.11.2009 von der Geschäftsleitung der MR für die REINHAUSEN Gruppe freigegeben.

Inhalt

1. Grundlagen zum Umgang mit Informationen 4
2. Geltungsbereich 4
3. Verantwortlichkeiten und Rollen 4
3.1. Informationsverantwortlicher 4
3.2. Verfasser 4
3.3. Nutzer 5
3.4. Kernnutzer 5
3.5. Technischer Sachbearbeiter 5
3.6. Prüfer und Ermittler 5
4. Klassifizierung von Informationen – Vertraulichkeitsklassen 5
4.1. Grundlagen 5
4.2. Schadensgrößen 6
4.3. Vertraulichkeitsklassen 6
4.4. Änderung der Klassifizierung / „Lebenslauf“ von Informationen 7
4.5. Angebote, Verträge 7
4.6. Informationen von Dritten 7
5. Kennzeichnung von Informationen 8
5.1. Explizite Kennzeichnung 8
5.2. Implizite Kennzeichnung 8
5.3. Dokumente im Entwurfsstadium 8
6. Ausdrückliche Verpflichtungserklärungen 8
7. Regeln zum Umgang mit Informationen 9

1. Grundlagen zum Umgang mit Informationen

- Die REINHAUSEN Gruppe ist sich der Bedeutung des Schutzes von Informationen bewusst, da deren Missbrauch zu großen materiellen und immateriellen Schäden führen kann. Die Klassifizierung und angemessene Handhabung von Informationen ist ein wichtiger Baustein zur Vermeidung solcher Schäden.
- Informationen können in unterschiedlicher Form vorliegen – z.B. in elektronischer Form als Datei, in physischer Form als Ausdruck oder auch als gesprochenes Wort. Informationen werden anhand der Vertraulichkeit ihres Inhalts eingestuft. Der Grad der Vertraulichkeit spiegelt das Maß der Auswirkungen wider, falls Informationen missbräuchlich benutzt werden. Er bestimmt auch, wie mit Informationen umzugehen ist. Die Einstufung der Information ist unabhängig vom verwendeten Medium.
- Grundsätzlich sollen nur diejenigen Personen Zugriff zu unternehmenskritischen Informationen erhalten, die diese zur Erfüllung ihrer Aufgaben benötigen („need-to-know-Prinzip“).

2. Geltungsbereich

- Diese Richtlinie richtet sich an Mitarbeiter der REINHAUSEN Gruppe entsprechend des auf dem Deckblatt genannten Geltungsbereiches (nachfolgend REINHAUSEN Gesellschaften). Ebenso richtet sich diese Richtlinie an alle Lieferanten, an externe Dienstleister und Partnerunternehmen, soweit dies nicht in den einzelnen Abschnitten anders angegeben ist.
- Diese Richtlinie ist für jeden Mitarbeiter verbindlich und wird jedem Mitarbeiter zugänglich gemacht (u.a. im REINHAUSEN GroupNet).
- Jeder Mitarbeiter soll im Informationsaustausch mit einer externen Stelle (z.B. Geschäftspartner) darauf hinwirken, dass auch diese die Anforderungen der Richtlinie einhält.
- Verstöße gegen die Richtlinie können arbeits-, zivil- oder strafrechtliche Maßnahmen nach sich ziehen. Die zuständige Gesellschaft behält sich das Recht vor, die Einhaltung dieser Richtlinie regelmäßig zu überprüfen.

3. Verantwortlichkeiten und Rollen

3.1. Informationsverantwortlicher

- Der Informationsverantwortliche ist verantwortlich für die Klassifizierung von Informationen in seinem Verantwortungsbereich. Typischerweise gehört er der Bereichs-, Abteilungs- oder Projektleitung an oder hat übergreifende Aufgaben (z.B. Informationssicherheit, Arbeitsschutz, Datenschutz). Er legt den Kreis der Nutzer (interne und ggf. externe Personen) namentlich oder über Rollen sowie deren Berechtigungen fest. Die Verantwortlichkeit zur Klassifizierung von Informationen kann durch ihn auch an andere Mitarbeiter delegiert werden.
- Für bestimmte Gruppen von Informationsnutzern, bestimmte Arten des Informationsaustauschs oder für Einzelfälle kann von dem Informationsverantwortlichen aus sachlichen Gründen von den Bestimmungen der Richtlinie abgewichen werden. Jede Abweichung muss bekannt gegeben und dokumentiert werden.

3.2. Verfasser

- Der Verfasser arbeitet im Auftrag des Informationsverantwortlichen und übernimmt die Einstufung der Information von diesem. Bezüglich der Weitergabe besitzt er keine Sonderrechte.

3.3. Nutzer

- Nutzer einer Information sind alle Personen, die berechtigt sind, diese Information zu erhalten. Der Nutzer handelt gemäß den Regeln dieser Richtlinie, sofern der Informationsverantwortliche nicht Abweichendes vorgegeben hat.

3.4. Kernnutzer

- Der Informationsverantwortliche legt die Kernnutzer fest. In der Regel wird der Kernnutzerbereich abteilungsübergreifend alle Mitarbeiter umfassen, die innerhalb eines Prozesses bestimmte Informationen regelmäßig bearbeiten. Kernnutzern einer Information ist der Umgang mit diesen Informationen vertraut; sie sind vom Informationsverantwortlichen dafür entsprechend geschult und sensibilisiert.
- Beispiele für Kernnutzer einer Information sind die Mitarbeiter der Personalabteilung bezüglich Personalakten oder abteilungsübergreifende Projektteams – auch mit externen Beratern – bezüglich Projektdaten.
- Das Kernnutzerkonzept reduziert den Kennzeichnungsaufwand (s. 5.2 Implizite Kennzeichnung).

3.5. Technischer Sachbearbeiter

- Technische Sachbearbeiter (z.B. Administratoren, Archivare) haben aufgrund ihrer besonderen Rolle Umgang mit klassifizierten Informationen. Sie sind nicht berechtigt, diese Informationen außerhalb ihrer funktionsbezogenen Aufgabe (z.B. Monitoring, Auswertung für Verrechnungszwecke) zu verwenden.

3.6. Prüfer und Ermittler

- Dieser Personenkreis hat expliziten Zugriff auf Informationen zum Zwecke der Ermittlung oder Prüfung. Zum Personenkreis zählen z.B. öffentliche Regierungsstellen (Polizei, Staatsanwaltschaft, etc.) oder Steuer- und Wirtschaftsprüfer.

4. Klassifizierung von Informationen – Vertraulichkeitsklassen

4.1. Grundlagen

- Die in der REINHAUSEN Gruppe vorhandenen Informationen werden nach ihrer Vertraulichkeit klassifiziert. Die Vertraulichkeit ist abhängig von ihrer Bedeutung für die Geschäftsprozesse oder dem potentiellen Schaden bei falschem Umgang mit ihnen.
- Informationen werden in folgende Klassen eingestuft:
    - Offen
    - Intern
    - Vertraulich
    - Streng vertraulich

Beispiele für die Einstufungen einzelner Dokumente in die Vertraulichkeitsklassen finden Sie im GroupNet unter Sicherheitsmanagement.

4.2. Schadensgrößen

Für die korrekte Einstufung von Informationen in die jeweiligen Vertraulichkeitsklassen ist das Wissen um den potentiellen Schaden bei unerwünschter Offenlegung oder Weitergabe an Dritte wichtig.

Schadensgröße	Schaden für das Unternehmen	Klasse dt./engl.	Beispiele
Groß bis existenzgefährdend	• Betroffen ist das gesamte Unternehmen • Sehr schwerer Schaden für die Geschäftszwecke und Ziele des Hauses • Gravierende rechtliche Konsequenzen bis hin zu Haftstrafen • Erheblicher Verlust von Ansehen und Vertrauen bei mehreren Kunden oder Lieferanten	Streng vertraulich / Strictly confidential	• Strategieunterlagen • Daten von gravierenden Störfällen • Ergebnisse Technik-Benchmark • Passwörter • Brief an Lieferanten mit Daten zu Neuproduktentwicklung, …
Mittel	• Betroffen ist ein Unternehmensbereich • Erheblicher finanzieller Schaden • Rechtliche Konsequenzen bis hin zu Ordnungswidrigkeiten und Geldstrafen • Verärgerung und Imageverlust bei einzelnen Kunden oder Lieferanten • Personenbezogene Daten gem. Bundesdatenschutzgesetz	Vertraulich / Confidential	• Informationen, die im Rahmen von Vertraulichkeitsvereinbarungen erlangt wurden • Daten des CRM-Systems • Kalkulationen • Unterlagen von Bewerbern • Arbeitsverträge • Mitarbeiterbeurteilung • Monatsbericht einer Gesellschaft, …
Gering	• Keine weit reichenden Konsequenzen	Intern / Internal	• Organigramme • Adressänderung eines Mitarbeiters, …
Kein	• Kein Schaden, da Information für Öffentlichkeit bestimmt	Offen / Public	• Freigegebene Produktflyer • Referenzlisten, …

4.3. Vertraulichkeitsklassen

Im Folgenden werden die vier Vertraulichkeitsklassen und die grundlegenden Regeln bezüglich Kennzeichnung, Weitergabe und Absicherung sowie das Schadenspotential bei unsachgemäßem Umgang dargestellt.

„Offen“

- Diese Informationen bedürfen keiner Kennzeichnung. Ein Schaden für das Unternehmen kann in keinem Fall entstehen. Für die Handhabung offener Informationen existieren keine Einschränkungen.
- Über die Veröffentlichung eines Dokumentes entscheidet der jeweilige Informationsverantwortliche.

„Intern“

- Für diese Informationen genügt die implizite Kennzeichnung (siehe 5).
- Interne Informationen können ohne Einschränkungen an Mitarbeiter von REINHAUSEN Gesellschaften oder an externe Stellen übermittelt werden, sofern dienstlich benötigt.
- Schaden für das Unternehmen bei einem unsachgemäßen Umgang: gering.

„Vertraulich“

- Für diese Informationen genügt die implizite Kennzeichnung (siehe 5), sofern die Informationen den Kreis der Kernnutzer nicht verlassen.
- Vertrauliche Informationen können bestimmten, d.h. von dem Informationsverantwortlichen benannten Nutzern (namentlich oder Rollen) übermittelt werden, sofern dienstlich benötigt.
- Werden sie anderen als Kernnutzern übermittelt, so sind sie vorher explizit als „vertraulich“ zu kennzeichnen.
- Schaden für das Unternehmen bei einem unsachgemäßen Umgang: mittel.

„Streng vertraulich“

- Diese Informationen bedürfen stets einer expliziten Kennzeichnung (siehe 5.1).
- Sie dürfen nur an bestimmte von dem Informationsverantwortlichen namentlich benannte Nutzer übermittelt und von jedem Empfänger nur mit ausdrücklicher Einwilligung des Informationsverantwortlichen an andere Nutzer weitergeleitet werden.
- Unabhängig davon ist der Kreis der Nutzer möglichst klein zu halten.
- Schaden für das Unternehmen bei einem unsachgemäßen Umgang: groß bis existenzgefährdend.
- Unberührt von dieser Richtlinie bleiben die Sonderfälle der Geheimhaltungsbedürftigkeit gemäß § 79 BetrVG, § 96 SGB IX (Bekanntgabe von Betriebs- und Geschäftsgeheimnissen gegenüber BR, JAV und Schwerbehindertenvertretung).

4.4. Änderung der Klassifizierung / „Lebenslauf“ von Informationen

- Eine Information kann verschiedene Stufen an Vertraulichkeit durchlaufen. So können für eine Veröffentlichung vorgesehene Informationen noch als vertraulich einzustufen und zu behandeln sein, solange sie nicht veröffentlicht sind (z.B. Entwurf technischer Dokumente → Veröffentlichung der technischen Dokumente).
- Eine Änderung der Klassifizierung kann nur durch den Informationsverantwortlichen erfolgen.

4.5. Angebote, Verträge

- Angebote und Verträge zu Geschäften über allgemein angebotene Leistungen zu allgemein bekannten Gegenleistungen ohne besondere Nebenabreden werden in die Vertraulichkeitsstufe „Intern“ eingestuft. Andere Angebote und Verträge sind je nach Inhalt als „Vertraulich“ oder „Streng vertraulich“ einzustufen.
- Weitergehende Anforderungen (z.B. des Vergaberechts) bleiben unberührt.

4.6. Informationen von Dritten

- Die REINHAUSEN Gruppe wahrt die Vertraulichkeit von Kunden- und Lieferanteninformationen und trifft dafür entsprechende Vorkehrungen. Die gesetzlichen und vertraglichen Bestimmungen werden beachtet.
- Grundsätzlich gelten für Informationen, die der REINHAUSEN Gruppe überlassen und mit einer Vertraulichkeitsklasse gekennzeichnet wurden, die gleichen Regelungen wie für interne Informationen der REINHAUSEN Gruppe.

5. Kennzeichnung von Informationen

5.1. Explizite Kennzeichnung

- Sind Informationen explizit als „Vertraulich“ oder „Streng vertraulich“ zu kennzeichnen, so ist der Träger der Information (z.B. Papierbogen, DVD) deutlich erkennbar mit der Kennzeichnung „Vertraulich“ bzw. „Streng vertraulich“ zu versehen.
- Mehrseitige Dokumente in Papier- oder Dateiform sind auf jeder Seite in der Mitte der Kopf- oder Fußzeile in Fettdruck entsprechend zu kennzeichnen; die Gesamtseitenzahl muss erkennbar sein.
- Bei „vertraulichen“ Informationen ist der Empfängerkreis auf dem Informationsträger zu benennen, z.B. „Abteilung XY“.
- Bei „streng vertraulichen“ Informationen ist der Empfängerkreis NAMENTLICH (Verteilerliste) auf dem Informationsträger zu bezeichnen.
- „Vertrauliche“ Informationen in Papierform sind bei internem Versand in der Hauspostmappe mit Klebestreifen zu verschließen und darauf ein Handzeichen des Absenders anzubringen, bei externem Versand im verschlossenen Kuvert ist der Empfänger mit dem Zusatz „persönlich“ zu benennen. Wenn bei „vertraulichen“ Informationen das Risiko der Öffnung durch nicht befugte Dritte besteht und bei „streng vertraulichen“ Informationen generell sind Kuvertierungen doppelt auszuführen (Ausnahmen davon legt der Informationsverantwortliche fest); die innere ist mit der Kennzeichnung der Vertraulichkeitsklasse zu versehen, die äußere darf keinen Hinweis auf die Vertraulichkeit enthalten.
- Die explizite Kennzeichnung hat immer Vorrang vor der impliziten.

5.2. Implizite Kennzeichnung

- Die implizite Kennzeichnung stellt innerhalb eines Kernnutzerbereiches (siehe 3.4) eine Erleichterung für die tägliche Arbeit dar. Die Informationen oder Informationsträger sind nicht selbst gekennzeichnet; der Nutzer kennt die Klassifizierung anhand der Art der Information und wurde vom Informationsverantwortlichen entsprechend geschult und sensibilisiert.
- Die implizite Kennzeichnung ist maximal für vertrauliche Informationen möglich, solange diese den Kernnutzerbereich nicht verlassen. Wenn vertrauliche Informationen den Kernnutzerbereich verlassen sowie bei streng vertraulichen Informationen ist generell eine explizite Kennzeichnung mit der Vertraulichkeitsklasse erforderlich.
- Bei neu erstellten Dokumenten sind die aktuellen Vorlagen für Microsoft Office-Dateien zu verwenden, sobald diese durch OI bereitgestellt werden. Wenn die Vorlage die Angabe einer Vertraulichkeitsklasse fordert, hat die Klassifizierung entsprechend Abschnitt 4. zu erfolgen.

5.3. Dokumente im Entwurfsstadium

- Dokumente, die sich noch im Entwurfsstadium (engl.: Draft) befinden, sind als solche mit dem Hinweis „Entwurf“ oder „Draft“ zu kennzeichnen.
- Dies entbindet aber nicht von der Einstufung des Dokuments in die jeweilige Vertraulichkeitsklasse.

6. Ausdrückliche Verpflichtungserklärungen

- Jeder externe Dienstleister und Lieferant muss sich zur Verschwiegenheit verpflichten, sofern er potentiell Zugriff auf Daten oder Informationen der REINHAUSEN Gruppe hat. Das kann bereits vor

Abschluss eines Vertrags, z.B. im Rahmen von Verhandlungen, der Fall sein. Dann hat er zuvor eine Erklärung zur Verschwiegenheitspflicht (Non Disclosure Agreement, NDA) zu unterschreiben. Daneben ist darauf zu achten, dass ein mit ihm später geschlossener Vertrag ebenfalls eine Verschwiegenheitspflicht enthält.

- NDAs für Lieferanten oder Dienstleister erstellt die Einkaufsabteilung. Für alle sonstigen Empfängergruppen erstellt sie die Rechtsabteilung. Der jeweilige Auftraggeber ist verantwortlich dafür, mit dem zuständigen Informationsverantwortlichen den Schutzbedarf der Daten zu klassifizieren und danach die Abteilung zu informieren, die das NDA ausstellt.

7. Regeln zum Umgang mit Informationen

Die Regeln zum Umgang mit Informationen werden in Anlage 1 zusammengefasst.

Wie wird gekennzeichnet?	Offen	Intern	Vertraulich	Streng vertraulich
Kennzeichnung von Informationen in Papierform	Keine	Implizit (d.h. der Nutzer ist mit der Art der Information vertraut und erkennt daraus die Vertraulichkeits-klasse, ohne dass diese auf dem Informationsträger vermerkt ist)	Implizit innerhalb der Kernnutzer. Explizit wenn die Information den Kreis der Kernnutzer verlässt: – mit „Vertraulich“ auf jeder Seite in Kopf- oder Fußzeile und ggf. im Betreff – Verteilerkreis auf erster Seite – Seitenangabe mit „Seite x von y“.	Explizit: – mit „Streng vertraulich“ auf jeder Seite in Kopf- oder Fußzeile und ggf. im Betreff – Verteilerkreis namentlich benannt auf erster Seite – Seitenangabe mit "Seite x von y"
Kennzeichnung von elektronischen Informationen	Keine	Implizit	Implizit innerhalb der Kernnutzer. Explizit mit "Vertraulich" wenn die Information den Kreis der Kernnutzer verlässt.	Explizit: – mit "Streng vertraulich"

Was mache ich bei …?		Offen	Intern	Vertraulich	Streng vertraulich
Vervielfältigung mittels Kopierer, Drucker		Keine Einschränkungen	Keine Einschränkungen	Beaufsichtigung des Vervielfältigungsvorgangs	Nur nach Freigabe durch den Informations-verantwortlichen, Beaufsichtigung des Vervielfältigungsvorgangs
Weitergabe		Keine Einschränkungen	An alle Mitarbeiter von REINHAUSEN Gesellschaften bzw. beauftragte Dienstleister oder Kunden - sofern dienstlich benötigt	Weitergabe an Kernnutzer oder an vom Informationsverantwortlichen definierte Nutzer (namentlich oder Rollen), sofern dienstlich benötigt. Bei externen Dienstleistern muss eine Vertraulichkeitsvereinbarung vorliegen.	Weitergabe nur an namentlich vom Informationsverantwortlichen definierte Nutzer. Vom Empfänger dürfen streng vertrauliche Informationen nur nach expliziter Freigabe des Informationsverantwortlichen weitergegeben werden. Bei externen Dienstleistern muss eine Vertraulichkeitsvereinbarung vorliegen.
Übermittlung auf d. Postweg	**Intern**	Keine Einschränkungen	Hauspostmappe	Hauspostmappe mit Klebestreifen verschließen und darauf Handzeichen anbringen; bei Risiko der Öffnung durch unbefugte Dritte Kuvertierung doppelt ausführen.	Kuvertierung doppelt ausführen; die innere ist mit der Kennzeichnung der Vertraulichkeitsklasse zu versehen, die äußere darf keinen Hinweis auf die Vertraulichkeit enthalten.
	Extern	Keine Einschränkungen	Normaler Brief	Verschlossener Umschlag, Empfänger mit Zusatz „persönlich“ benennen; bei Risiko der Öffnung durch unbefugte Dritte Kuvertierung doppelt ausführen.	Per Übergabe-Einschreiben, Kuriersendung; Empfänger mit Zusatz „persönlich“ benennen; Kuvertierung doppelt ausführen; die innere ist mit der Kennzeichnung der Vertraulichkeitsklasse zu versehen, die äußere darf keinen Hinweis auf die Vertraulichkeit enthalten.
Übermittlung per E-Mail (Tabelle zur internen oder externen Anbindung der	**Intern**	Keine Einschränkungen	Keine Einschränkungen	Mit der Nachrichtenoption „Vertraulich“ zu versenden	Mit der Nachrichtenoption „Vertraulich“ zu versenden
Töchter im GroupNet unter Sicherheitsmanagement)	**Extern**	Keine Einschränkungen Anlagen üblicherweise als PDF-Dokument	Keine Einschränkungen Anlagen üblicherweise als PDF-Dokument	Inhalt als Anlage mit WINZIP verschlüsselt (Anleitung im GroupNet), Anlagen üblicherweise als PDF-Dokument	Inhalt als Anlage mit WINZIP verschlüsselt (Anleitung im Group-Net), Anlagen üblicherweise als PDF-Dokument
Übermittlung per Fax	**Intern**	Keine Einschränkungen	Keine Einschränkungen	Nur nach Vorankündigung	Nur nach Vorankündigung
	Extern	Keine Einschränkungen	Deckblatt mit Anzahl der Seiten	Nur nach Vorankündigung Deckblatt mit Anzahl der Seiten	Verboten
Verbale Weitergabe		Keine Einschränkungen	Nur erlaubt, wenn keine Unberechtigten zuhören können.	Nur erlaubt, wenn keine Unberechtigten zuhören können.	Nur erlaubt, wenn keine Unberechtigten zuhören können. Nicht auf Anrufbeantworter / Mailbox hinterlassen. Identität des Gesprächspartners sicherstellen.
Vernichtung von Informationen in Papierform		Keine Einschränkungen	Papierkörbe am Arbeitsplatz; nicht bei personenbezogenen Daten	Gesicherte Vernichtung z. B. im Datenschutz-Container	Schreddern

Informationen in IT-Systemen	*Offen*	*Intern*	*Vertraulich*	*Streng vertraulich*
Speicherung in IT-Systeme / Anwendungen der REINHAUSEN Gesellschaften	Keine Einschränkungen	Speicherung unter Berücksichtigung der Zugriffsrechte, ggf. explizite Vergabe von Zugriffsrechten	Speicherung unter Berücksichtigung der Zugriffsrechte, ggf. explizite Vergabe von Zugriffsrechten	Speicherung unter Berücksichtigung der Zugriffsrechte, regelmäßig Prüfung der aktuellen Zugriffsrechte, ggf. explizite Vergabe von Zugriffsrechten
Mobile Geräte (Notebooks, MDAs)	Keine Einschränkungen	Keine Einschränkungen	Bei Notebooks Verschlüsselung erforderlich. Bei anderen mobilen Geräten Speicherung vertraulicher Daten vermeiden.	Bei Notebooks Verschlüsselung erforderlich. Bei anderen mobilen Geräten Speicherung streng vertraulicher Daten verboten.
Mobile Datenträger (CD, DVD, USB-Stick)	Keine Einschränkungen	Keine Einschränkungen	Verschlüsselung erforderlich z. B. mit WINZIP (Anleitung im GroupNet)	Verschlüsselung erforderlich z. B. mit WINZIP (Anleitung im GroupNet)
Bereitstellung im Internet (Blogs, Foren)	Keine Einschränkungen	Verboten	Verboten	Verboten
Löschen von elektronischen Informationen	Löschen in Filesystem	Löschen in Filesystem	Löschen in Filesystem	Löschen in Filesystem
Entsorgung / Vernichtung von Hardware und mobilen Daten-trägern (CD, DVD, USB-Stick)	Keine Einschränkungen	Hardware: Abgabe bei OISC oder ggf. lokaler IT Mobile Datenträger: physische Vernichtung	Abgabe bei OISC oder ggf. lokaler IT zur Vernichtung	Abgabe bei OISC oder ggf. lokaler IT zur Vernichtung

Physische Aufbewahrung und Ablage von Informationen	*Offen*	*Intern*	*Vertraulich*	*Streng vertraulich*
Allgemein	Keine Einschränkungen	Unbefugten Zugriff durch Dritte über einfache Mittel verhindern. Eine angemessene technische Umsetzung ist durch den Informationsverantwortlichen im Einzelfall in Abhängigkeit von den Gefährdungen zu gewährleisten.	Zugriff durch unbefugte Dritte verhindern. Eine angemessene technische Umsetzung ist durch den Informationsverantwortlichen im Einzelfall in Abhängigkeit von den Gefährdungen zu gewährleisten.	Zugriff durch unbefugte Dritte verhindern. Eine angemessene technische Umsetzung ist durch den Informationsverantwortlichen im Einzelfall in Abhängigkeit von den Gefährdungen zu gewährleisten.
In Firmengebäuden der REINHAUSEN Gesellschaften	Keine Einschränkungen	Absperren des Büros wo möglich. Bei physisch extra abgesicherten Bereichen sind Sonderregelungen möglich.	Absperren des Büros, wo möglich. Falls gewährleistet ist, dass niemand außer dem Schlüsselbesitzer das Büro betreten kann, ist diese Maßnahme ausreichend. Sonst: Bei längerer Abwesenheit (> 30 Minuten) Wegsperren der Informationen. Bei physisch extra abgesicherten Bereichen sind Sonderregelungen möglich.	Absperren des Büros, wo möglich. Falls gewährleistet ist, dass niemand außer dem Schlüsselbesitzer das Büro betreten kann, ist diese Maßnahme ausreichend. Sonst: Bei physisch extra abgesicherten Bereichen bei längerer Abwesenheit (> 30 Minuten) Wegsperren der Informationen. Bei physisch nicht gesondert abgesicherten Bereichen Wegsperren der Informationen bei einer Abwesenheit von mehr als 10 Minuten.
Unterwegs (z. B. Hotel) oder Zuhause	Keine Einschränkungen	Abgesperrter Raum, z. B. Hotelzimmer, Heimbüro	Vor Zugriff sicher aufbewahren (Verschlüsseln und z. B. Wegsperren in Hotelsafe)	Vor Zugriff sicher aufbewahren (Verschlüsseln und z. B. Wegsperren in Hotelsafe)