ORGANISATIONS-
ANWEISUNG

LEITLINIE INFORMATIONSSICHERHEIT

Gültig: Dürr Gruppe

Fachliche Freigabe:	Jan Steinbrenner, Corporate Security, Dürr AG	4.5.2023 Datum
Qualitätsfreigabe:	Fabian Mock, Corporate Internal Audit, Dürr AG	4.5.2023 Datum
Gesamtfreigabe:	Dr. Jochen Weyrauch, CEO, Dürr AG	8.5.23 Datum

Änderungsdienst-Zustand

Änderungsdienst

[ ] Dieses Dokument unterliegt derzeit keinem Änderungsdienst.

[X] Corporate Internal Audit (CIA) - unterhält für dieses Dokument einen Änderungsdienst.

[X] Die jeweils aktuelle Version dieses Dokuments ist im DÜRRnet abrufbar.

Änderungszustand

Version des Gesamtdokuments: 2.0 vom 19.04.2023. Die folgende Tabelle listet die bisherigen Versionen des Dokuments.

Version	Datum	Änderung/Grund
1.0	24.08.2020	Erstausgabe
2.0	19.04.2023	Dokumentenreview (Anpassung Zuständigkeiten, Format)

Inhalt

1 Leitgedanke und Stellenwert der Informationssicherheit 4

2 Umsetzung eines angemessenen Informationssicherheitsniveaus .. 6

3 Verantwortung des Managements 7

4 Schlussbestimmungen und Geltungsbereich 8

1 Leitgedanke und Stellenwert der Informationssicherheit

Als weltweit führender und innovativer Technologiekonzern hat im Dürr-Konzern spezifisches Know-how eine herausragende Bedeutung und unterliegt deshalb einem besonderen Schutzbedarf. Nur durch den wirksamen Schutz dieser Informationen kann der wirtschaftliche Erfolg nachhaltig gesichert werden.

Darüber hinaus ist unser Unternehmen auch gegenüber unseren Kunden in der Verantwortung. Von Geschäftspartnern übergebene geheimhaltungsbedürftige Informationen werden vertraulich behandelt und nur für den vereinbarten Zweck verwendet. Getroffene Verpflichtungen und Vereinbarungen zur besonderen Geheimhaltung werden jederzeit beachtet.

Ein wirksamer und umfassender Schutz dieser Informationen basiert auf einer umfassenden Risikobetrachtung und eines ebenso umfassenden Schutzkonzepts, dass nicht nur IT technische Maßnahmen beinhaltet, sondern alle relevanten Konzernbereiche einbezieht.

Ziel eines integrierten Informationssicherheitsmanagementsystems ist es den wirksamen Schutz schutzbedürftiger Informationen bereichsübergreifend sicherzustellen.
Die Etablierung des ISMS basiert auf folgenden Leitgedanken:

- Geschäftsbasierter Ansatz
  - Der Informationsschutz des Dürr-Konzerns basiert auf den geschäftlichen Verpflichtungen und Erfordernissen des Unternehmens. Er sichert den wirtschaftlichen Erfolg und reduziert Risiken für die Unternehmensgruppe.
- Risikobasierter Ansatz
  - Schwerpunkte werden so gesetzt, dass Risiken nach ihrem Schadenspotential und Eintrittswahrscheinlichkeit identifiziert und reduziert werden.
- Einheitlicher Ansatz
  - Alle Mitarbeiterinnen und Mitarbeiter im Dürr-Konzern sind für die Informationssicherheit mitverantwortlich. Durch einheitliche Standards und Prozesse wird die Durchgängigkeit eines wirksamen Informationsschutzes garantiert.
- Prozessbasierter Ansatz
  - Das ISMS folgt dem in der ISO/IEC 27001 empfohlenen kontinuierlichen Verbesserungsprozess auf Basis des PDCA-Modells (Plan, Do, Check, Act). Ziel ist es, nachweislich und regelmäßig die Angemessenheit, Vollständigkeit, Nachhaltigkeit, Effektivität und Effizienz der implementierten Informationssicherheitsprozesse und Schutzmaßnahmen innerhalb der Dürr-Gruppe sicherzustellen.

Um diesem Ziel und den Leitgedanken gerecht zu werden, wird durch das ISMS ein erforderliches, geeignetes sowie angemessenes Schutzniveau in Bezug auf die

- Vertraulichkeit – Schutz von wertvollen oder sensitiven Informationen vor unautorisiertem Zugriff/ Veröffentlichung;

- Integrität (Korrektheit) – Schutz von wertvollen oder sensitiven Informationen vor absichtlicher oder unabsichtlicher Verfälschung, um Richtigkeit und Vollständigkeit sicherzustellen;

- Verfügbarkeit – Sicherstellung, dass die Verarbeitungsvorgänge von Informationen gemäß den zeitlichen Anforderungen von Mitarbeitern und Geschäftspartnern zur Verfügung gestellt werden;

von Geschäftsprozessen, Daten, Informationen und IT-Systemen definiert.

Um die Vertraulichkeit zu garantieren werden:
- Schutzbedürftige Informationen identifiziert und klassifiziert
- Der Zugang zu den Informationen beschränkt (Need to know Prinzip)
- Ausreichende Schutzmaßnahmen getroffen (je kritischer die Information desto intensiver der Schutz)

Um die Integrität zu garantieren werden:
- Daten vor unberechtigter / ungewollter Veränderung mittels technischer und organisatorischer Sicherheitsmaßnahmen geschützt
- Zugriffsrechte- und Rollen definiert und eingehalten
- Die Richtigkeit von Informationen regelmäßig überprüft

Um die Verfügbarkeit zu garantieren werden:
- Redundanzen geschaffen wo diese notwendig sind
- IT-Systeme nach dem Stand der Technik gesichert
- Schwachstellen identifiziert und eliminiert

2 Umsetzung eines angemessenen Informationssicherheitsniveaus

Sämtliche Überlegungen zum ISMS basieren auf der Grundlage des im Konzern geltenden integrierten Managementsystems in der Verantwortung der jeweiligen Führungskräfte.

Die Dürr-Gruppe setzt zur Sicherstellung der Umsetzung von Informationssicherheitsanforderungen ein global implementiertes Informationssicherheitsmanagementsystem (ISMS) in Anlehnung an den internationalen Standard ISO/IEC 27001 ein.

Gesellschaftsspezifische Informationssicherheitsanforderungen werden unter Berücksichtigung global definierter Vorgaben und Standards zur Informationssicherheit in den lokal etablierten Organisationen und Prozessen der Gesellschaften behandelt und umgesetzt.

Die Umsetzung des prozessbasierten Ansatzes erfolgt auf der Grundlage des PDCA-Zyklus, der wie folgt hinterlegt wird:

PLAN - Festlegen des ISMS: Die Strategien, Ziele, Prozesse, Regelungen, Verfahren, Methoden, Werkzeuge und Verantwortlichkeiten des ISMS werden festgelegt.

DO - Umsetzen und Durchführen des ISMS: Die definierten Prozesse, Regelungen und Verfahren werden entsprechend den Zielen des ISMS umgesetzt. Ausgewählte Maßnahmen werden implementiert.

CHECK - Überwachen und Überprüfen des ISMS: Anhand praktischer Erfahrungen, den Ergebnissen von Audits und Managementbewertungen werden die Prozesse, Wirksamkeit und Effizienz der gewählten Ansätze und Maßnahmen gemessen und überprüft. Es wird identifiziert, ob Handlungsbedarf besteht und an welchen Stellen Optimierungsmöglichkeiten vorhanden sind.

ACT - Instandhalten und Verbessern des ISMS: Basierend auf den Ergebnissen der Phase Check und sonstiger Rückmeldungen (z.B. aktuelle Risikosituation / Bedrohungslage / Weiterentwicklungen / Anforderungen), werden Korrektur- und Vorbeugemaßnahmen ergriffen, die zu einer fortlaufenden Verbesserung des ISMS und des Sicherheitsniveaus führen.

3 Verantwortung des Managements

Der Vorstand der Dürr AG, die Vorstände der Teilkonzerne sowie alle Geschäftsführer der Konzerngesellschaften sind in ihrem jeweiligen Zuständigkeitsbereich für die Informationssicherheit verantwortlich und dazu verpflichtet, die erforderlichen personellen, organisatorischen und finanziellen Ressourcen bereitzustellen, um ein angemessenes Informationssicherheitsniveau zu etablieren, aufrechtzuerhalten und weiterzuentwickeln.

Im Rahmen ihrer Managementaufgaben und Vorbildfunktion sind alle Führungskräfte in besonderem Maß für die Förderung und Aufrechterhaltung des Bewusstseins und der Disziplin ihrer Mitarbeiter hinsichtlich der Informationssicherheit verantwortlich.

4 Schlussbestimmungen und Geltungsbereich

Diese Leitlinie wird durch weitere Managementprozesse und Richtlinien ergänzt. Hierzu zählen detaillierte Organisations- und Sicherheitsregeln für Bereiche mit unterschiedlichen Anforderungen zur Informationssicherheit sowie länder- bzw. standortspezifische gesetzliche und organisatorische Regelungen.

Weitere Hinweise hierzu sind im Dokument „Geltungsbereich des Informationssicherheitsmanagementsystems (ISMS)“ beschrieben.