Deutsche Post DHL Group

DEUTSCHE POST DHL GROUP

INFORMATION SECURITY POLICY

Dokument-Eigentümer: DPDHL Group CISO

Version 2-2022 Spring

KEINE VERSCHLUSSSACHE

Bei dem vorliegenden Dokument handelt es sich um eine Übersetzung der „Information Security Policy“ aus dem Englischen. In Fragen der Auslegung und Bedeutungen der deutschen Übersetzung ist der „Chief Information Security Officer“ (CISO) hinzuzuziehen.

INHALTSVERZEICHNIS

1 LEITBILD FÜR INFORMATIONSSICHERHEIT BEI DEUTSCHE POST DHL GROUP

1.1 Verpflichtung zur Informationssicherheit

Der Konzernvorstand von Deutsche Post DHL Group verpflichtet sich in vollem Umfang, die Informationen von Deutsche Post DHL Group sowie die unserer Kunden, Partner und Mitarbeiter angemessen zu schützen.

Als weltweit führender Logistikanbieter setzen wir Maßnahmen zur Informations- und Cybersicherheit um, unser Geschäft rund um den Globus schützen. Dabei sind wir bestrebt Unterbrechungen des Geschäftsbetriebs und damit verbundene Schäden zu vermeiden, sowie die anzuwendenden Gesetze und Vorschriften einzuhalten.

Die Sicherung und der Schutz von Informationen unterstützen das Ziel von Deutsche Post DHL Group, „Anbieter erster Wahl", „Investment erster Wahl" und „Arbeitgeber erster Wahl" zu sein. Dies ermöglicht es Deutsche Post DHL Group, die Erwartungen unserer Kunden zu erfüllen, das Vertrauen unserer Investoren zu erhalten, das Wachstum in bestehenden und neuen Märkten zu fördern und die Informationen unserer Mitarbeiter vertraulich und sicher zu halten.

1.2 Ansatz zur Informationssicherheit

Der Konzernvorstand von Deutsche Post DHL Group stellt sicher, dass Informationssicherheit konzernweit einheitlich gefördert, implementiert und gemanagt wird, indem er eine eigene Informationssicherheitsorganisation einrichtet, die Standards und unterstützende Prozesse definiert, welche konzernweit eingeführt und umgesetzt werden.

Innerhalb von Deutsche Post DHL Group basiert die Informationssicherheit auf:

- Sicherstellung eines angemessenen Schutzniveaus durch Implementierung geeigneter Governance, Prozesse und Technologien nach einem risikobasierten Ansatz.
- Bezugnahme aller Aktivitäten der Informationssicherheit auf international anerkannte Verfahren und Standards.
- Förderung der kontinuierlichen Verbesserung der Informationssicherheitsaktivitäten unter Verwendung unserer First Choice-Methoden.
- Einbindung unserer Mitarbeiter als wesentlicher Teil unseres Schutzes.

1.3 Steuerung der Informationssicherheit

Der Konzernvorstand von Deutsche Post DHL Group hat beschlossen, dass die Informationssicherheit durch ein Informationssicherheits-Managementsystem geregelt wird, das im Information Security Target Model spezifiziert und dokumentiert ist und konzernweit umgesetzt wird.

Das Information Security Target Model liefert einen systematischen Ansatz für die Planung, Übernahme, Implementierung, Überwachung und Verbesserung von Aufgaben und Aktivitäten, die für den Schutz von Informationen erforderlich sind. Dies erfolgt unter Einbezug von Menschen, Prozessen und Informationssystemen sowie durch die Anwendung des Risikomanagementprozesses. Es behandelt folgende Komponenten:

1. Die Steuerung des Informationssicherheits-Managementsystems, um sicherzustellen, dass alle seine Aspekte konzernweit implementiert werden, um Anforderungen an die Informationssicherheit festzulegen und sicherzustellen, dass die Informationssicherheits-Organisation angemessen funktioniert.
2. Das Informationssicherheits-Risikomanagement zur Identifizierung, Bewertung und Reduktion von Risiken sowie Nutzung von Chancen anhand definierter Risikobewertungskriterien. Dies erfolgt mit eindeutig identifizierten Risikoeignern, die den Risikobehandlungsplan genehmigen und das Restrisiko akzeptieren.
3. Die Informationssicherheitsmessung und -berichterstattung zur Überwachung, Messung, Analyse und Bewertung der Effektivität des Informationssicherheits-Managementsystems. Um dem Management fundierte Entscheidungen zu ermöglichen, werden Metriken zur Verbesserung des Informationssicherheits-Managementsystems und der technologischen Umgebung verwendet.
4. Das Management von Informationssicherheits-Vorfällen zur Sicherstellung der effektiven Handhabung und Kommunikation von Informationssicherheits-Ereignissen und -Vorfällen. Dies dient der zeitnahen und möglichst störungsfreien Behebung, der erforderlichen Beweissicherung und der Verbesserung von Fähigkeiten, Prozesse und Technologien aus den gewonnenen Erkenntnissen.
5. Informationssicherheitsbewusstsein, Schulung, Training und Praxiserfahrung, um unsere Mitarbeiter in die Lage zu versetzen, Informationssicherheitsrisiken im besten Interesse von Deutsche Post DHL Group richtig zu erkennen und zu behandeln.

Es gelten die folgenden Regeln zur Entscheidungs- und Durchführungsverantwortung:

	Gruppen-Ebene	**Unternehmensbereichs-Ebene**
Entscheidungs- und Durchführungsverantwortung für Geschäftsauswirkungen	Corporate Board	Fachseite
Entscheidungsverantwortung für die Informationssicherheit	IT Board	CIO des Unternehmensbereichs
Durchführungsverantwortung für die Informationssicherheit	Information Security Committee	CISO des Unternehmensbereichs

Die finanziellen, strategischen und operativen Erfordernisse von Deutsche Post DHL Group sowie rechtliche und ethische Standards bestimmen die Zielsetzungen, die durch die Informationssicherheit erreicht werden sollen. Die Erreichung der Zielsetzungen wird gemessen, um sicherzustellen, dass die beabsichtigten Ziele innerhalb des entsprechenden Zeitrahmens erreicht werden.

2 UMFANG DER INFORMATIONSSICHERHEIT

2.1 Bezug zu international anerkannten Kontrollstandards

Der Konzernvorstand von Deutsche Post DHL Group gibt die freiwillige Selbstverpflichtung ab, dass das Information Security Target Model den Anforderungen der Internationalen Norm ISO/IEC 27001:2013 entspricht.

2.2 Geltungsbereich

Die Informationssicherheit bei Deutsche Post DHL Group zielt darauf ab, alle organisationseigenen Werte (nachfolgend immer als „Assets“ bezeichnet) von Deutsche Post DHL Group vor informations- und cybersicherheitsbezogenen Bedrohungen zu schützen. Dazu gehören unter anderem Kundendaten, Finanzdaten und Mitarbeiterdaten, IT-Anwendungen, Speicher- und Datenverarbeitungsgeräte, Netzwerke und physische Assets.

Das Information Security Target Model ist für alle Mitarbeiter von Deutsche Post DHL Group sowie für Lieferanten und Partner gültig und verbindlich. Seine Anforderungen müssen erfüllt oder übertroffen werden. Das Information Security Target Model richtet sich außerdem an Kunden, Investoren, Behörden und die Öffentlichkeit.

2.3 Schutzziele

Der Schutz vor Bedrohungen in der Informationssicherheit bedeutet, die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen zu wahren, was wie folgt verstanden wird:

- **VERTRAULICHKEIT:** Sicherstellen, dass Informationen nur für autorisierte Personen, Informationssysteme oder Prozesse zugänglich sind.
- **INTEGRITÄT:** Sicherstellung der Richtigkeit und Vollständigkeit von Informationen über den gesamten Lebenszyklus.
- **VERFÜGBARKEIT:** Sicherstellen, dass autorisierte Personen, Informationssysteme oder Prozesse zu allen erforderlichen Zeitpunkten rechtzeitig und unterbrechungsfrei auf eine Information zugreifen können.

3 LEITPRINZIPIEN DER INFORMATIONSSICHERHEIT

Diese Leitprinzipien definieren, wie das Informationssicherheits-Managementsystem eingerichtet, implementiert, aufrechterhalten und kontinuierlich verbessert wird.

3.1 Verwaltung, Umsetzung und Unterstützung der Informationssicherheit

Das für die Informationssicherheit direkt verantwortliche Management stellt sicher, dass Personal mit entsprechender Kompetenz und in der erforderlichen Anzahl vorhanden ist und bleibt.

Rollen und Verantwortlichkeiten für die Informationssicherheit sind identifiziert, definiert und etabliert.

Die Mitarbeiter von Deutsche Post DHL Group müssen das Information Security Target Model kennen, wissen, wie sie das Informationssicherheits-Managementsystem unterstützen können und welche Konsequenzen es hat, wenn sie dessen Anforderungen nicht umsetzen. Dieses Bewusstsein und alle anderen Informationen, die für die erfolgreiche Implementierung des Informationssicherheits-Managementsystems relevant sind, müssen fortlaufend kommuniziert werden.

Lieferanten und Partner müssen angemessene und geeignete Informationssicherheitsmaßnahmen für die von ihnen gelieferten Produkte und/oder Dienstleistungen sicherstellen. Das erforderliche Niveau der Informationssicherheit wird durch eine Risikobewertung bestimmt, die von Mitgliedern der Informationssicherheitsorganisation beurteilt wird.

3.2 Überwachung und Messung der Effektivität der Informationssicherheit

Die Effektivität und Effizienz von Aktivitäten der Informationssicherheit innerhalb und außerhalb des Informationssicherheits-Managementsystems werden mit Hilfe geeigneter Methoden und Technologien kontinuierlich gemessen und überwacht.

Bewertungen der Informationssicherheit, die die Effektivität und Effizienz messen, werden nach einem definierten Plan durchgeführt, der Umfang, Methodik, Häufigkeit und Ziel detailliert beschreibt.

Die Ergebnisse der Messungen und Überwachung werden von der Informationssicherheitsorganisation ordnungsgemäß analysiert und liefern dem Management Informationen, die zu Änderungen der Technik, Organisation und Verfahren führen können.

Die Effektivität und Effizienz des Informationssicherheits-Managementsystems, die Analyse und Bewertung des aktuellen Risikoniveaus und der Bedrohungslage sowie die Ergebnisse der Verbesserungs- und Minderungsmaßnahmen werden an das Corporate Board und das IT Board von Deutsche Post DHL Group berichtet.

3.3 Arbeitsweise der Informationssicherheit

Informationen werden nach einem Risikobewertungsansatz klassifiziert und entsprechend ihrer Klassifizierung geschützt.

Risikomindernde Kontrollen werden zeitnah implementiert und überwacht, um ihre fortlaufende Funktionsfähigkeit sicherzustellen und um eine kontinuierliche Verbesserung zu unterstützen.

Informationen, die für das ordnungsgemäße Funktionieren des Informationssicherheits-Managementsystems erforderlich sind, werden gesammelt, zeitnah analysiert und darauf angemessen reagiert.

Änderungen am Informationssicherheits-Managementsystem und nachfolgender Dokumentation werden identifiziert und überwacht, um das erforderliche Niveau der Informationssicherheit zu gewährleisten. Diese Änderungen werden in einem Standardprozess erfasst, analysiert, geprüft, dokumentiert und von der entsprechenden Managementebene genehmigt.

Informationssicherheits-Ereignisse und -Vorfälle werden von Experten von Deutsche Post DHL Group angemessen behandelt.

3.4 Kontinuierliche Verbesserung der Informationssicherheit

Dem Ansatz von Deutsche Post DHL Group zur kontinuierlichen Verbesserung folgend, werden das Informationssicherheits-Managementsystem und die dazugehörige Dokumentation jährlich überprüft und bei Bedarf vom Information Security Committee aktualisiert.

Die Überprüfung berücksichtigt wesentliche Veränderungen im externen und internen Umfeld, die Strategie von Deutsche Post DHL Group sowie die Ergebnisse relevanter Messungen und Überwachungen im gesamten Konzern Deutsche Post DHL Group.

4 DOKUMENTEIGENSCHAFTEN

4.1 Übersicht der Dokumenteneigenschaften

Dokument-Eigentümer	Beschluss-gremium	Datum der Autorisierung	Aktuell freigegebene Version	Häufigkeit der Prüfung	Datum der letzten Überprüfung
Information Security Committee	IT Board	25 Juli 2013	1.00	n/a	n/a
Information Security Committee	Information Security Committee	22 Februar 2018	1.31	n/a	n/a
Information Security Committee	Information Security Committee	16 März 2020	2.00	Alle zwei Jahre	n/a
Information Security Committee	IT Board	24 März 2020	2.00	Alle zwei Jahre	n/a
Information Security Committee	Corporate Board	21 Juli 2020	2.00	Alle zwei Jahre	n/a
DPDHL Group CISO	Information Security Committee	19 Januar 2021	2.01	Spätestens alle zwei Jahre	n/a
DPDHL Group CISO	IT Board	4. Oktober 2021	V2 2021 Herbst	halbjährlich	4. Oktober 2021
DPDHL Group CISO	IT Board	12 April 2022	2 – Spring 2022	halbjährlich	12 April 2022

Tabelle 4.1-1 Übersicht der Dokumenteneigenschaften

Deutsche Post AG

dpdhl.de

Gültig ab 5. Oktober 2021