

Globale Richtlinie von Getinge

Globale IT-Richtlinie

Dokumenteneigner Agneta Palmér

Version v2

Vom Verwaltungsrat verabschiedet 26. April 2023

1. Kurzdarstellung

Die Getinge Group ist bestrebt, Menschen und Informationen zu schützen und gleichzeitig das gesamte IT-Risiko zu mindern. Diese Gruppenrichtlinie definiert Getinges Standpunkte im Bereich der IT und klärt das Verhalten, das wir von Benutzern, Systemadministratoren, Management und IT-Sicherheitspersonal erwarten. Es setzt auch die Sicherheitsstandards für unser IT-System und unsere Anwendungen.

2. Definitionen (streichen Sie dieses Kapitel, falls nicht zutreffend)

In dieser globalen Richtlinie haben die folgenden Begriffe die folgende Bedeutung:

CFO	Finanzvorstand
CIO	Chief Information Office (Leiter des Informationsbüros)
CISO	Informationssicherheitsbeauftragter
DSGVO	Datenschutz-Grundverordnung (EU-Verordnung zum Schutz personenbezogener Daten)
BYOD	Bringen Sie Ihr eigenes Gerät mit – der persönliche PC, das Tablet oder das Mobiltelefon eines Benutzers
ITIL	

In: Information Technology Infrastructure Library. Eine Reihe detaillierter Praktiken für das IT-Servicemanagement, die sich darauf konzentrieren, IT-Services an den Anforderungen des Unternehmens auszurichten.

3. Geltungsbereich

Diese globale Richtlinie gilt für alle Getinge-Unternehmen, ihre Tochtergesellschaften und Joint Operations (gemeinsam "Getinge") und gilt für alle unsere Mitarbeiter und Direktoren sowie Berater und Agenturmitarbeiter, die in den Räumlichkeiten von Getinge oder unter der Leitung von Getinge arbeiten (alle in dieser globalen Richtlinie als "Mitarbeiter" bezeichnet).

Das Ziel dieser Richtlinie ist es, Leitlinien und Unterstützung für IT-Entscheidungen innerhalb von Getinge bereitzustellen. Es beschreibt Standards und Verfahren, die eine sichere und akzeptable Praxis auf der Grundlage anerkannter und aktueller Kenntnisse, Richtlinien und gängiger Praktiken widerspiegeln.

4. Grundsätze

Engagement und Erwartungen

Die IT-Struktur von Getinge bietet einen Mehrwert, indem sie dem Unternehmen den bestmöglichen Service bietet und Risiko und Rendite mit dem Return on IT-Investment ausgleicht.

Getinge ist bestrebt, Menschen und Informationen zu schützen und gleichzeitig das gesamte IT-Risiko zu mindern. Wir leiten und steuern unsere IT-Funktionen durch strukturiertes Management, einen konsistenten Prozess und durch den Aufbau starker Beziehungen zum Unternehmen.

Ziel dieser globalen Richtlinie ist es:

- Schutz von Personen und Informationen;
- Legen Sie die Regeln für das erwartete Verhalten von Benutzern, Systemadministratoren, Management- und IT-Sicherheitspersonal fest;
- Festlegung der Standards für das IT-System und die Anwendungen;
- Minderung des gesamten IT-Risikos.

Wir erwarten von allen Mitarbeitern und Auftragnehmern, die auf IT-Systeme oder Hardware von Getinge zugreifen, dass sie diese globale Richtlinie befolgen und ihre hohen Standards konsequent anwenden. Weitere Hinweise finden sich in den zugrunde liegenden Richtlinien und Anweisungen.

5. Informationssicherheitsrichtlinie

Informationssicherheit ist die Praxis, Informationen vor unbefugtem Zugriff, Verwendung, Offenlegung, Störung, Änderung, Durchsicht, Inspektion, Aufzeichnung oder Zerstörung zu schützen.

Die Getinge-Informationssicherheitsrichtlinie definiert, wie wir mit Getinge-Informationssicherheitsrisiken umgehen und die Sicherheitskontrollen einrichten, die zum Schutz von Getinge-Informationsressourcen erforderlich sind, unabhängig von der Form der Daten (z. B. elektronische oder physische Sicherungen).

Ziel dieser Informationssicherheitsrichtlinie ist es, Anleitungen zu geben, wie wir unter Sicherheits Gesichtspunkten sicherstellen,

- die Vertraulichkeit unserer Informationen
- den Zugang und die Verfügbarkeit unserer Systeme
- die Integrität unserer Daten.

Die Informationssicherheitsrichtlinie gilt für alle Computerinformationssysteme, die die Geschäftsprozesse von Getinge unterstützen. Dazu gehören Anwendungsinfrastruktur (einschließlich Netzwerke und Kommunikation), bereitgestellte IT-Dienste, Desktop- und Laptop-

PCs, mobile Geräte (einschließlich Telefone, Tablets, Wearables) und persönliche Geräte, d. h. BYOD:s, die für Geschäfte im Zusammenhang mit Getinge verwendet werden.

Alle Fragen zur Informationssicherheit sind an den CISO von Getinge zu richten.

Weitere Hinweise finden Sie unter: *Informationssicherheitsrichtlinie*

6. Richtlinie über Cybersicherheitsvorfälle

Diese Globale Richtlinie lenkt und plant, wie auf Cyber-Vorfälle zu reagieren ist. Der Plan wurde entwickelt, um

- die Anforderungen und Erwartungen an die Reaktion auf Cybersicherheitsvorfälle zu beschreiben
- den Lebenszyklus und den Prozess der Reaktion auf Sicherheitsvorfälle festzulegen
- festlegung der Rollen und Verantwortlichkeiten der am Sicherheitsvorfall beteiligten Personen
- antwort
- definition von Parametern für die Meldung, Klassifizierung und Ermittlung von Vorfällen.

Weitere Hinweise finden Sie unter: *Richtlinie über Cybersicherheitsvorfälle*

7. IT-Nutzungsrichtlinie

Diese globale Richtlinie definiert die akzeptable Nutzung der IT-Ressourcen von Getinge, um die Nutzung aller IT-Eigenschaften effektiv zu verwalten und zu sichern. Dazu gehören nicht nur Computer und Handys, sondern auch die Nutzung elektronischer Informationssysteme (wie Software, Dateifreigaben), das Getinge-Netzwerk, der Internetzugang und das elektronische Postsystem.

Diese Systeme werden für geschäftliche Zwecke verwendet und dienen den Interessen des Unternehmens sowie unserer Kunden und Kunden im Rahmen des normalen Betriebs. Jede Nutzung muss in Übereinstimmung mit den geltenden Gesetzen, Verordnungen, Vorschriften und Regeln sowie gegebenenfalls mit Branchen- und Konsensstandards erfolgen.

Weitere Hinweise finden Sie unter: *IT Acceptable Use Directive*

8. IT-Governance-Richtlinie

Diese globale Richtlinie soll relevante IT-Governance-Prozesse skizzieren, um sicherzustellen, dass die IT weiterhin effiziente und sichere IT-Projekte und -Dienstleistungen liefern sowie die globale Lizenzkonformität und gute Einkaufspraktiken für IT-Geräte und -Dienstleistungen aufrechterhalten kann.

Diese Globale Richtlinie deckt die wichtigsten Bereiche der IT-Governance ab, die in der Regel miteinander verbunden sind, weshalb sie alle in diesem Dokument und nicht in separaten Richtlinien enthalten sind:

- Project Portfolio Management (PPM) beschreibt den Prozess, wenn Sie ein Projekt haben, bei dem die IT Aufgaben und/oder Dienstleistungen erbringen muss
- Das Project Management Office (PMO) beschreibt die Art und Weise, wie die IT Projekte in der Umsetzung verfolgt
- Business Relationship Management (BRM) beschreibt das Modell für die IT- /Business-Ausrichtung
- IT-Lizenzmanagement beschreibt, wie Group IT Lizenzen verwaltet und die lokale Verantwortung dafür
- IT-Beschaffungsmanagement beschreibt den Prozess für den Einkauf von IT-bezogener Software, Hardware und / oder Dienstleistungen.

Weitere Hinweise finden Sie unter: *IT-Governance-Richtlinie*

9. IT-Betriebsrichtlinie

Diese globale Richtlinie legt eine Grundlage für den IT-Betrieb fest, um ein gutes Sicherheitsniveau und bewährte Verfahren aufrechtzuerhalten, mit dem Ziel, stabile und effiziente IT-Services für unser Geschäft bereitzustellen. Diese globale Richtlinie deckt die wichtigsten IT-Betriebsbereiche ab, die in der Regel miteinander verbunden sind. Daher befinden sie sich alle in diesem Dokument und nicht in separaten Richtlinien:

- Netzwerksicherheitsmanagement
- Patch- und Schwachstellenmanagement
- Schutz vor bösartigem Code
- Protokollierung und Überwachung
- Personal Computer-Verwaltung
- Verwaltung mobiler Geräte

Weitere Hinweise finden Sie unter: *IT-Betriebsrichtlinie*

10. IT-Sicherungs- und Wiederherstellungsrichtlinie

Diese Globale Richtlinie gilt für die Sicherung und Wiederherstellung aller Daten, die elektronisch auf von Group IT verwalteten Servern gespeichert sind. Von Group IT verwaltete Server können sich intern oder extern befinden.

Sie gilt auch für jeden IT-Business-/ technischen Systemeigentümer, wobei der Systemmanager von Getinge für eine Software verantwortlich ist, die auf einer computergestützten Lösung von Getinge ausgeführt wird.

Elektronische Daten, die in firmeneigenen Personalcomputern, Notebooks, Laptops, mobilen Geräten oder anderen Speichergeräten gespeichert sind, fallen nicht in den Anwendungsbereich dieser Richtlinie.

Weitere Hinweise finden Sie unter: *IT-Betriebsrichtlinie*

11. IT-Cloud-Richtlinie

Cloud Computing ist die Bereitstellung von Computing-Dienstleistungen - Server, Speicher, Datenbanken, Netzwerke, Software, Analysen und mehr - über das Internet („die Cloud“).

Diese globale Richtlinie beschreibt, was vor der Auswahl, Implementierung und dem Betrieb von Cloud-Lösungen oder Cloud-Diensten zu beachten ist:

- Klärung der Hauptmerkmale von Cloud Computing, Servicemodellen und Bereitstellungsmodellen.
- Must-haves, Best Practices und verbotene Dinge im Bereich Cloud.
- Empfehlungen und Erläuterungen, warum die IT so früh wie möglich in Cloud-Einkaufsprozesse eingebunden werden muss.

Weitere Hinweise finden Sie unter: *IT-Cloud-Richtlinie*

12. Rollen und Verantwortlichkeiten

Alle Mitarbeiter von Getinge sind individuell dafür verantwortlich, diese globale Richtlinie zu lesen, zu verstehen und einzuhalten. Jeder Mitarbeiter ist dafür verantwortlich, in Übereinstimmung mit dieser globalen Richtlinie zu handeln,

Jeder Vorgesetzte ist dafür verantwortlich, sicherzustellen, dass jedes Teammitglied Zugang zu dieser Globalen Richtlinie und den damit verbundenen Globalen Richtlinien, Globalen Anweisungen und Richtlinien hat.

Die tägliche Verstärkung, einschließlich regelmäßiger Informationen und Schulungen im Bereich IT sowie Compliance-Follow-up, gehört mit Unterstützung der IT-Abteilung zur Verantwortung eines jeden Managers.

Verstöße gegen die Konzernrichtlinie können zu Disziplinarmaßnahmen bis hin zur Kündigung führen.

13. Verstöße gegen die globale Richtlinie – Speak Up

Zögern Sie nicht, Bedenken zu äußern. Von jedem Getinge-Mitarbeiter, der Verstöße gegen diese globale Richtlinie vermutet, wird erwartet, dass er sich zu Wort meldet und das Problem seinem Vorgesetzten, dem Ethik- und Compliance-Büro oder der Getinge Speak Up Line vorlegt. Die Getinge Speak Up Line ist auf internen und externen Getinge-Webseiten verfügbar. Bei Getinge akzeptieren wir keine Form von Vergeltungsmaßnahmen gegen jemanden, der sich äußert und Bedenken oder Meinungen äußert.

Siehe weiter: Global Speak Up and Non Retaliation Directive (Globale Richtlinie über Äußerung und Nichtvergeltung)

14. Beratung und Unterstützung

Wenn Sie Fragen zu dieser globalen Richtlinie haben, wenden Sie sich bitte an Pelle Nilsson, CIO.

Wenn es einen Grund für die Nichteinhaltung eines Teils der globalen IT-Richtlinie oder der globalen IT-Richtlinien gibt (z. B. rechtlich, behördlich, finanziell oder technisch), muss ein Ausnahmeantrag ausgefüllt und an den Chief Information Security Officer von Getinge gesendet werden. Abhängig von der Risikostufe können zusätzliche Genehmigungen erforderlich sein.

Alle Ausnahmegenehmigungen müssen zeitlich und in ihrem Umfang begrenzt sein.

Zugehörige Dokumente

- Informationssicherheitsrichtlinie
- Richtlinie über Cybersicherheitsvorfälle
- IT-Nutzungsrichtlinie
- IT-Governance-Richtlinie
- IT-Betriebsrichtlinie
- IT-Sicherungs- und Wiederherstellungsrichtlinie
- IT-Cloud-Richtlinie
- Antrag auf IT-Sicherheitsausnahme