Informationen zum Unternehmen Sicherheitspolitik

Inhaltsübersicht

Dokumentenkontrolle

Inhaltsübersicht

1. Übersicht
2. Zweck
3. Umfang
4. Politik
5. Einhaltung der Politik
6. Zugehörige Normen, Richtlinien und Prozesse
7. Definitionen und Begriffe
8. Geschichte der Revision

Dokumentenkontrolle

Name des Dokuments	Unternehmenspolitik zur Informationssicherheit
Klassifizierung	INTERNE
Revisionsnummer	3.5
Datum der Überarbeitung	05/12/2024
Verwahrstelle	Manager für Unternehmenssicherheit
Zulassung	Einblicke IS Forum
Prüfung	Jährlich: Sicherheitsmanager für Unternehmen
Nächste Überprüfung	Dezember 2025

1. Überblick

Diese Richtlinie basiert auf ISO 27001:2022, dem anerkannten internationalen Standard für Informationssicherheit. Diese Norm gewährleistet, dass die Insights die folgenden Sicherheitsgrundsätze einhalten:

Vertraulichkeit	Alle sensiblen Informationen werden vor unbefugtem Zugriff oder Offenlegung geschützt.
Integrität	Alle Informationen werden vor versehentlichen, böswilligen und betrügerischen Änderungen oder Zerstörungen geschützt,
Verfügbarkeit	Die Informationsdienste werden zu den mit den Nutzern vereinbarten Zeiten zur Verfügung stehen und gegen zufällige oder böswillige Beschädigung oder Denial-of-Service geschützt sein.

2. Zweck

Zweck dieser Richtlinie ist es, das Engagement von Insights Learning and Development für die Sicherheit der Daten, für die es verantwortlich ist, zu demonstrieren und die Kontrollen und Verantwortlichkeiten aufzuzeigen, die zur Unterstützung des Informationssicherheits-Managementsystems (ISMS) vorhanden sind, dessen wichtigster Rahmen die ISO 27001:2022 ist.

3. Geltungsbereich

Der Geltungsbereich dieser Richtlinie erstreckt sich auf alle internen und externen Parteien und unterstützt Insights kontinuierliches Engagement für ISO 27001:2022.

4. Politik

4.1 Verantwortlichkeiten der Exekutive

Die Geschäftsleitung von Insights verpflichtet sich, alle anwendbaren Anforderungen im Rahmen dieser Richtlinie zu erfüllen und das Informationssicherheitsmanagementsystem (ISMS) kontinuierlich zu verbessern, und hat daher diese Informationssicherheitsrichtlinie erstellt, um

- sie dem Zweck von Insights angemessen ist;
- Sie enthält Ziele für die Informationssicherheit und bietet den Rahmen für die Festlegung kontinuierlicher Ziele für die Informationssicherheit.

Diese Informationssicherheitspolitik muss als dokumentierte Information verfügbar sein, innerhalb von Insights kommuniziert werden und gegebenenfalls interessierten Parteien zur Verfügung stehen.

Die Einhaltung dieser Politik und aller anderen Sicherheitsmaßnahmen und -verfahren ist für alle Mitarbeiter verbindlich.

Der CEO genehmigt diese Politik. Das Informationssicherheitsforum ist dafür verantwortlich, dass die Politik in allen Geschäftsbereichen, die in den Geltungsbereich des ISMS fallen, umgesetzt und befolgt

wird.

4.2 Führungsqualitäten und Engagement

Die Exekutive wird weiterhin Führungsstärke und Engagement in Bezug auf das ISMS demonstrieren, indem sie:

- Gewährleistung, dass die Informationssicherheitspolitik und die Informationssicherheitsziele festgelegt werden und mit der strategischen Geschäftsausrichtung von Insights vereinbar sind;
- Gewährleistung der Integration der ISMS-Anforderungen in die Prozesse von Insights;
- Sicherstellung, dass die für das ISMS erforderlichen Ressourcen zur Verfügung stehen;
- Vermittlung der Bedeutung eines wirksamen Informationssicherheitsmanagements und der Einhaltung der Anforderungen des ISMS ;
- Sicherstellung, dass das ISMS seine beabsichtigten Ergebnisse erreicht;
- Anweisung und Unterstützung von Personen, die zur Wirksamkeit des ISMS beitragen;
- Förderung der kontinuierlichen Verbesserung und Unterstützung anderer relevanter Managementfunktionen bei der Demonstration ihrer Führungsqualitäten in ihren Verantwortungsbereichen.

4.3 Ziele der Informationssicherheit

Es wurden Ziele für die Informationssicherheit festgelegt, die mit der strategischen Ausrichtung von Insights vereinbar sind. Das Hauptziel besteht darin, im Einklang mit den unten aufgeführten Abschnitten der Best-Practice-Norm ISO 27001:2022 zu arbeiten.
Darüber hinaus werden die Sicherheitsziele vom Informationssicherheitsforum als ständige Aufgabe und bei den ISMS Management Review Meetings festgelegt.

4.4 Kontinuierliche Verbesserung des ISMS-Rahmens

Insights ist bestrebt, das Managementsystem für die Informationssicherheit im Einklang mit einem PLAN-DO-CHECK-ACT-Ansatz kontinuierlich zu verbessern, um die in das ISMS eingebetteten Prozesse zu verbessern.

Die Bedeutung, die der Informationssicherheit beigemessen wird, zeigt sich in der Existenz des Informationssicherheitsforums; dessen Funktion wird im Folgenden beschrieben

- Überprüfung und Weiterentwicklung von strategischen Sicherheitsfragen;
- Aufbau von Beziehungen außerhalb von Insights zu anderen Sicherheitsberatern;
- die Bewertung der Auswirkungen neuer gesetzlicher oder behördlicher Anforderungen, die uns auferlegt werden;
- Überwachung der Wirksamkeit des ISMS, z. B. anhand der Ergebnisse der Berichte der Innenrevision und der Berichte über Sicherheitsvorfälle;
- Empfehlung/Befürwortung von Änderungen am ISMS.

Das Informationssicherheitsforum tritt regelmäßig zusammen, um sich mit den oben genannten Aktivitäten zu befassen und so die kontinuierliche Wirksamkeit des ISMS von Insights zu gewährleisten. Das Überprüfungsverfahren ist in der "Information Security Forum Management Review Policy" festgelegt.

Diese Unternehmenspolitik zur Informationssicherheit bestätigt das Engagement von Insights für eine kontinuierliche Verbesserung und hebt die Schlüsselbereiche (als "Themen" bezeichnet) für einen wirksamen Schutz seiner Informationen hervor, nämlich

- Organisatorische Kontrollen
- Personenkontrollen
- Physikalische Kontrollen
- Technologische Kontrollen

4.5 Organisatorische Kontrollen

Organisatorische Kontrollen fallen in den Zuständigkeitsbereich des Informationssicherheitsforums und betreffen die folgenden Bereiche:

- Strategische Informationssicherheitspolitik - die diese Politik, die Politik der Sicherheitsziele und die Kommunikationspolitik umfasst.
- Rollen und Zuständigkeiten - der Sicherheitsbeauftragte des Unternehmens führt den Vorsitz im

Informationssicherheitsforum.

- Identitäts- und Zugriffsmanagement - der Enterprise Security Manager bzw. die Teamleiter sind für die Einrichtung und Aufrechterhaltung robuster logischer Zugriffskontrollen verantwortlich. Es gibt eine entsprechende Richtlinie, die von allen Mitarbeitern und externen Parteien befolgt werden muss.
- Asset Management - Insights-Informationen müssen entsprechend ihrer Sensibilität klassifiziert und einem Informationseigentümer zugeordnet werden. Der Enterprise Security Manager führt ein Inventar der Informationsbestände, das regelmäßig entsprechend dem Risikoprofil aktualisiert und entsprechend geschützt wird.
- Beziehungen - Die Anforderungen an die Informationssicherheit zur Minderung des Risikos, das mit dem Zugang des Lieferanten zu Insights-Vermögenswerten verbunden ist, müssen mit dem Lieferanten vereinbart und dokumentiert werden.
- Vereinbarungen mit Cloud-Anbietern müssen festgelegt, dokumentiert und laufend überprüft werden.
- Management von Sicherheitsvorfällen - Die Aufzeichnungen zum Management von Sicherheitsvorfällen müssen zentral gepflegt, aktualisiert und laufend überwacht werden. Alle Mitarbeiter müssen wissen, was ein tatsächlicher oder potenzieller Sicherheitsvorfall ist, wie ein Vorfall zu melden ist und an wen der Vorfall zu melden ist. Die Verantwortung für die Überwachung aller Sicherheitsverstöße liegt beim Sicherheitsbeauftragten des Unternehmens.
- Business Continuity Management - Einblicke müssen einen konsistenten und effektiven Ansatz für das Management größerer Informationssicherheitsvorfälle gewährleisten, einschließlich der Kommunikation über Sicherheitsereignisse und -schwächen und die Auswirkungen auf das Business Continuity Management.

- Compliance - Insights muss Verstöße gegen rechtliche, gesetzliche, behördliche oder vertragliche Verpflichtungen in Bezug auf die Informationssicherheit und gegen Sicherheitsanforderungen vermeiden. Insights muss technische und organisatorische Maßnahmen ergreifen, um personenbezogene Daten vor versehentlicher oder unrechtmäßiger Zerstörung, versehentlichem Verlust oder versehentlicher Änderung sowie vor unbefugter Weitergabe oder unbefugtem Zugriff zu schützen. Insbesondere sollte Insights Maßnahmen ergreifen, die sicherstellen sollen, dass:

    - Jeder, der personenbezogene Daten verwaltet und verarbeitet, weiß, dass er vertraglich für die Einhaltung einer guten Datenschutzpraxis verantwortlich ist.
    - alle Personen, die personenbezogene Daten verwalten und bearbeiten, entsprechend geschult sind; und
    - Alle Personen, die personenbezogene Daten verwalten und bearbeiten, werden angemessen beaufsichtigt.

4.6. Personen-Kontrollen

Die Personalkontrollen fallen in den Zuständigkeitsbereich der Personalabteilung und betreffen die folgenden Bereiche:

- Alle Mitarbeiter müssen das Mitarbeiterhandbuch unterzeichnen, in dem sie verpflichtet werden, alle Richtlinien und Verfahren einzuhalten, die auch spezifische Anforderungen an die Informationssicherheit enthalten.
- Eine Sicherheitsrichtlinie für personenbezogene Daten stellt sicher, dass die Mitarbeiter darauf aufmerksam gemacht werden, dass sie verpflichtet sind, bewährte Verfahren zur Informationssicherheit zu befolgen.
- Es gibt auch ein Verfahren für alle Mitarbeiter, die Insights verlassen (einschließlich Zeit- und Vertragsangestellte), um ihr Netzwerkkonto zu deaktivieren und alle Gegenstände zurückzuholen.
- Alle neuen Mitarbeiter (Festangestellte, Zeitarbeiter und Auftragnehmer) müssen im Rahmen ihres Einführungsprogramms in den oben beschriebenen Bereichen geschult werden. Laufende Schulungen müssen in Form eines Programms regelmäßiger Aktualisierungen und Schulungen durch das Forum für Informationssicherheit erfolgen.

4.7 Physische Kontrollen

Die physischen Kontrollen fallen in den Zuständigkeitsbereich des Einrichtungsteams und betreffen die folgenden Bereiche:

- Das Personal muss die detaillierten Maßnahmen, Kontrollen und Verfahren kennen und befolgen,

die zur Gewährleistung einer angemessenen Kontrolle der physischen Sicherheit bestehen. Dazu gehören:

- Gebäudealarm- und CCTV-Systeme
- beschränkter Zugang zum Gebäude und weiterer beschränkter Zugang innerhalb des Gebäudes
- sichere Schließfächer, Schubladen, Tresore und Lagerräume, feuersichere Lagerung
- sichere Offsite-Backups und Archivierung
- übersichtlicher Schreibtisch und übersichtliche Bildschirmanordnung
- Verfahren für die Ausgabe von Medien aller Art
- die Notwendigkeit einer ständigen Überwachung aller physischen Sicherheitsmaßnahmen

4.8. Technologische Kontrollen

Die technologischen Kontrollen fallen in den Zuständigkeitsbereich des Teams für Unternehmenstechnologie und -sicherheit und betreffen die folgenden Bereiche:

- Alle Endgeräte müssen angemessen geschützt und gegebenenfalls verschlüsselt sein.
- Identitäts- und Zugriffsmanagement - IT-Systemadministratoren (privilegierte Nutzer) stellen sicher, dass die vereinbarten Zugriffskontrollen und -verfahren im Einklang mit der festgelegten Politik verwaltet werden.
- Kryptographie - Für den Fall, dass kryptographische Kontrollen von Insights eingesetzt werden, wurde eine Richtlinie für den Einsatz kryptographischer Kontrollen zum Schutz von Informationen entwickelt und umgesetzt.
- IT-Betriebssicherheit - Insights gewährleistet den ordnungsgemäßen und sicheren Betrieb von Informationsverarbeitungsanlagen. Das Enterprise Technology & Security Team führt eine laufende Überwachung aller IT-Betriebsaktivitäten durch.
- IT-Kommunikationssicherheit - Das Personal muss sich darüber im Klaren sein, dass die Nutzung von Technologie und Kommunikation vom Sicherheitsbeauftragten des Unternehmens festgelegt, kontrolliert und verwaltet wird. Er ist dafür verantwortlich, dass die entsprechenden Sicherheitsmaßnahmen und -prozesse vorhanden sind. Insights stellt sicher, dass die Sicherheit des Netzwerks, der Endpunkte und der Fernarbeit angemessen geschützt ist.
- Sicherheit bei der Entwicklung von IT-Systemen - der Sicherheitsbeauftragte des Unternehmens stellt sicher, dass die entsprechenden Verfahren zur Informationssicherheit in alle Projekte einbezogen werden. Ein sicheres Entwicklungskonzept einschließlich Richtlinien, Verfahren, Umgebung und Tests ist vorhanden.

4.9. Zeitraum für die Überprüfung der Politik

Das Informationssicherheitsforum wird diese Politik mindestens einmal jährlich überprüfen.

5. Einhaltung der Politik

Messung der Einhaltung: Das Sicherheitsteam und/oder das Informationssicherheitsforum überprüft die Einhaltung der
diese Politik durch verschiedene Methoden, einschließlich, aber nicht beschränkt auf, regelmäßige Begehungen, Videoüberwachung,
Business-Tool-Berichte, interne und externe Audits und Feedback an den Eigentümer der Police.

Ausnahmen: Alle Ausnahmen von dieser Richtlinie müssen von dem für die Richtlinie zuständigen Verwalter und Genehmiger genehmigt werden. In
Abwesenheit, wie z. B. Jahresurlaub, fällt dies in die Zuständigkeit eines Mitglieds der Kustodie und/oder
Zustimmendes Linienmanagement oder Informationssicherheitsforum

Nichteinhaltung: Ein Mitarbeiter, der gegen diese Richtlinie verstoßen hat und dadurch den Ruf von Insights beeinträchtigt
Lernen und Entwicklung oder die Insights-Gruppe im weiteren Sinne können disziplinarische Maßnahmen ergriffen werden, die bis zu
einschließlich der Beendigung des Arbeitsverhältnisses.

6. Zugehörige Normen, Richtlinien und Prozesse

Artikel	Int oder	Titel des Dokuments

	Ext	
1	Intern	ISMS-Dokumentenverwaltungssystem
2		
3		
4		
5		
6		

7. Definitionen und Begriffe

Nicht zutreffend

8. Revision Geschichte

Revision	Datum	Geändert durch	Beschreibung
2.0	09/01/2020	Graham Watson	Politik vom CEO genehmigt
2.1	24/09/2021	Kevin McAuley	Geringfügige Änderungen aufgrund von Änderungen der Rollen und der Struktur
3.0	30/11/2021	Kevin McAuley	Vom Exekutivausschuss genehmigte Politik
3.1	13/02/2023	Dave McClure	Aktualisierung der Politik durch Hinzufügen neuer Politiken
3.2	06/03/2023	Dave McClure	Rollen und Zuständigkeiten wurden in die neue Richtlinie aufgenommen
3.3	05/04/2023	Ian Gowen	Interne Referenztabelle hinzugefügt
3.4	28/04/2023	Ian Gowen	Die Reihenfolge der internen Referenzen wurde geändert
3.5	05/12/2024	Andy Moore	Jährliche Überprüfung und Unterzeichnung durch den CEO

Unterschrieben:

Datum: 5th Dezember 2024

Fiona Logan
Geschäftsführender Direktor