PUBLIC
TLP:CLEAR

Leitlinie
Informationssicherheitspolitik
pit-cup GmbH

Eigner:	ISB
Geprüft durch:	ISMS-Team
Freigabe durch:	Geschäftsführung
Version:	1.0
Gültig ab:	13.08.2025
Status:	FREIGEGEBEN

Dokumenthistorie

verändert am	Version*	DRAFT / REVIEW / FREIGEGEBEN durch	Detaillierte Beschreibung	Status (DRAFT / REVIEW / FREIGEGEBEN)
14.07.2025	1.0	ISB	Erstellung, Formatierung pit CI	REVIEW
13.08.2025	1.0	ISB, GF	Überprüfung und Freigabe durch ISB und GF	FREIGEGEBEN

*Versionskontrolle:
v1.0x Geringe Änderungen (z.B. Formatierung, Rechtschreibung, Grammatik) durch den Eigner selbst
v1.x0 Mittlere Änderungen (z.B. Adaptierung an neue Erfahrungen aus Audits, Rückmeldungen von Reviewern)
vx.00 Große Änderungen (z.B. wesentliche inhaltliche Änderungen)

pit-cup GmbH
Palo-Alto-Platz 11
D-69124 Heidelberg
Tel. +49 6221 5393-0
Fax +49 6221 5393-11

info@pit.de | www.pit.de
GF: R. Umshaus, J. Messner
Registergericht Mannheim
HRB 335193

D-10178 Berlin
D-01157 Dresden
D-19057 Schwerin

Tel. +49 30 84711869-0
Tel. +49 351 407905-20
Tel. +49 385 48504-0

Inhaltsverzeichnis

pit-cup GmbH
Palo-Alto-Platz 11
D-69124 Heidelberg
Tel. +49 6221 5393-0
Fax +49 6221 5393-11

info@pit.de | www.pit.de
GF: R. Umshaus, J. Messner
Registergericht Mannheim
HRB 335193

D-10178 Berlin
D-01157 Dresden
D-19057 Schwerin

Tel. +49 30 84711869-0
Tel. +49 351 407905-20
Tel. +49 385 48504-0

1 Zweck

Informationssicherheit und der damit einhergehende Schutz sensibler Daten und Informationen ist für die pit-cup GmbH von essenzieller Bedeutung im täglichen Handeln. Um ein angemessenes Schutzniveau zu erreichen und sowohl gesetzlichen als auch wirtschaftlichen Anforderungen gerecht zu werden, ist es erforderlich, entsprechende Anforderungen zu definieren.
Aus diesem Grund hat die pit-cup GmbH ein Informationssicherheitsmanagementsystem (ISMS) gemäß ISO 27001:2022 eingeführt. Die vorliegende Politik beschreibt demnach die strategische Bedeutung des ISMS und bildet den Rahmen für Richtlinien, Prozesse, Tätigkeiten und Ziele. Dies ermöglicht die strukturierte Identifizierung, Bewertung und Behandlung von Sicherheitsrisiken, die kontinuierliche Verbesserung unserer Informationssicherheit und die Erhaltung der Geschäftskontinuität.
Mit dieser Politik möchten wir alle interessierten Parteien sowie die Öffentlichkeit über die Bedeutung der Informationssicherheit in der pit-cup GmbH informieren und darstellen, auf welche Weise wir den Anforderungen nachkommen.

2 Anwendungsbereich

Der Anwendungsbereich dieser Informationssicherheitspolitik wird aus dem Kontext der Organisation, den internen und externen Anforderungen, identifizierten Risiken, zu schützenden Prozessen und Prozesswechselwirkungen sowie und den unterliegenden Einflüssen hergeleitet und umfasst:

- das gesamte Unternehmen inklusive aller Führungskräfte, Mitarbeiter, Geschäftspartner, Standorte in Deutschland, Informationswerte, Prozesse und Leistungen. Dies inkludiert Homeoffice- und Telearbeitsplätze der betroffenen Personengruppen.

The scope of this information security policy is derived from the organization’s context, internal and external requirements, identified risks, processes to be protected and their interactions, as well as the underlying influencing factors, and includes:

- the entire company, including all executives, employees, business partners, locations in Germany, information assets, processes, and services. This also includes home office and teleworking workplaces of the affected groups of persons.

3 Grundsätze

Die Unternehmensleitung verabschiedet die Informationssicherheitspolitik als Bestandteil der Unternehmensstrategie und unterstützt alle Ziele und Prinzipien der Informationssicherheit. Demnach trägt die **Unternehmensleitung** die Gesamtverantwortung für die Informationssicherheit in der pit-cup GmbH und bekennt sich ausdrücklich zur kontinuierlichen Verbesserung sowie der Förderung und Unterstützung aller notwendigen Aktivitäten und Maßnahmen. Darüber hinaus sind jede Führungskraft, jeder Mitarbeiter und jede Person, die Daten und Informationen der pit-cup GmbH verarbeitet, verpflichtet, die entsprechenden Sicherheitsbestimmungen zu beachten und einzuhalten.

Damit einher geht die Verpflichtung, Anforderungen aus dem ISMS in die bestehenden Geschäftsstrukturen zu integrieren, um Informationssicherheit im täglichen Tun zu berücksichtigen. Zudem werden ausreichend Ressourcen zur Aufrechterhaltung des Systems zur Verfügung gestellt, welche den Informationssicherheitsbeauftragten und relevante Rollen unterstützen, um gemeinsam zur Wirksamkeit, Erfüllung und Verbesserung des Managementsystems beitragen zu können.
Der Missbrauch jeglicher Daten, der wirtschaftlichen Schaden oder Haftungsrisiken für uns oder unsere Partner verursachen kann, wird strikt abgelehnt. Dementsprechend unterstützen die Mitarbeiter der pit-cup GmbH bei der

pit-cup GmbH
Palo-Alto-Platz 11
D-69124 Heidelberg
Tel. +49 6221 5393-0
Fax +49 6221 5393-11

info@pit.de | www.pit.de
GF: R. Umshaus, J. Messner
Registergericht Mannheim
HRB 335193

D-10178 Berlin
D-01157 Dresden
D-19057 Schwerin

Tel. +49 30 84711869-0
Tel. +49 351 407905-20
Tel. +49 385 48504-0

Verhinderung unberechtigten Zugriffs auf bzw. unbefugter Änderung und Übermittlung von Informationen. Jedem Mitarbeiter ist bewusst, dass schützenswerte unternehmenseigene Informationen nicht illegal genutzt oder offenbart werden dürfen, um die Reputation und Geschäftsfähigkeit der pit-cup GmbH nicht zu gefährden.

4 Ziele

Die hier beschriebenen allgemeinen Sicherheitsziele des ISMS leiten sich aus allgemeinen Anforderungen an ein ISMS ab. Insbesondere die angemessene Realisierung der Schutzziele „Verfügbarkeit“, „Vertraulichkeit“ und „Integrität“ von Informationen, Daten und Systemen sowie die Gewährleistung des Schutzes von personenbezogenen Daten sind grundlegende Ziele unserer Informationssicherheit und schaffen die Voraussetzung dafür, Verantwortung und Vertrauen gegenüber unseren Mitarbeitern, Kunden, Partnern, Lieferanten und der Gesetzgebung zu schaffen:

- Vertraulichkeit: Vertrauliche Daten, Informationen und Systeme stehen ausschließlich autorisierten Personen zur Verfügung und werden vor unbefugter Preisgabe geschützt.
- Integrität: Informationen und Daten sind vollständig und korrekt und werden vor Veränderung, Manipulation und Verlust ausreichend geschützt. Vollständigkeit bedeutet, dass alle Teile der Information verfügbar sind. Korrekt sind Informationen, wenn sie den bezeichneten Sachverhalt unverfälscht wiedergeben.
- Verfügbarkeit: Die Informationen und Betriebsmittel stehen den berechtigten Personen im vorgesehenen Umfang und zum richtigen Zeitpunkt zur Verfügung.
- Authentizität: Informationen, Daten und Kommunikationspartner sind real, vertrauenswürdig und vor Manipulation geschützt.
- Konformität: Alle relevanten gesetzlichen, regulatorischen und unternehmensinternen Vorgaben zum Schutz von Informationen und Daten werden eingehalten.

Zur Erreichung der Schutzziele kontrollieren wir im Rahmen des Informationssicherheitsmanagementsystems die Einhaltung aller internen und externen Anforderungen und überwachen Vorbeuge- und Korrekturmaßnahmen. Zur besseren Überwachung werden angemessene Messgrößen der Ziele festgelegt und jährlich gemessen. Zudem werden alle Prozesse, Maßnahmen und Strategien in Bezug auf die Informationssicherheit zur Stärkung der Sicherheitslage regelmäßig überprüft und optimiert.

5 Leitsätze

Abgeleitet von unseren Zielen hat die pit-cup GmbH folgende Leitsätze entwickelt, um ein hohes Sicherheitsbewusstsein und Informationssicherheitsniveau zu erlangen.

Wir schützen verarbeitete Daten und Informationen

- Wir gehen mit sämtlichen Informationen und Daten, insbesondere mit jenen, die als personenbezogen, sensibel oder vertraulich klassifiziert sind, sorgsam um und verarbeiten diese entsprechend den geltenden Gesetzen, Vorschriften und internen Anweisungen.
- Wir betrachten Informationen und Daten von der Erstellung bis zur Vernichtung entsprechend den Schutzzielen der Informationssicherheit.
- Unsere Systeme unterstützen den Schutz von verarbeiteten Informationen und Daten.
- Wir setzen das Need-To-Know-Prinzip ein, sodass nur autorisierte Personen Informationen und Daten verarbeiten.
- Wir verwenden das Least-Privilege-Prinzip, um zu gewährleisten, dass Personen über so geringe Zutritts- bzw. Zugriffsrechte auf Informationen und Daten verfügen, dass sie ausschließlich ihrer zugeordneten

pit-cup GmbH
Palo-Alto-Platz 11
D-69124 Heidelberg
Tel. +49 6221 5393-0
Fax +49 6221 5393-11

info@pit.de | www.pit.de
GF: R. Umshaus, J. Messner
Registergericht Mannheim
HRB 335193

D-10178 Berlin
D-01157 Dresden
D-19057 Schwerin

Tel. +49 30 84711869-0
Tel. +49 351 407905-20
Tel. +49 385 48504-0

Tätigkeiten durchführen können.

- Wir legen IT- und Informationssicherheitsmaßnahmen risikoorientiert fest und berücksichtigen dabei den aktuellen Stand der Technik.
- Wir erheben den Business Impact unserer Geschäftsprozesse und der zugehörigen Informationswerte und schaffen Transparenz über entsprechende Risiken.

Wir erhöhen die Informationssicherheit

- Wir fördern ein umfassendes Bewusstsein hinsichtlich Informationssicherheit und erreichen einen hohen Abdeckungsgrad erfolgreich durchgeführter Sensibilisierungsschulungen. Hierzu erhalten alle Mitarbeiter und Führungskräfte Schulungen, um das Bewusstsein und Verständnis für Informationssicherheit zu fördern, um Risiken zu minimieren und sicherheitsbewusstes Verhalten zu gewährleisten.
- Wir stellen sicher, dass Mitarbeiter mit sicherheitsrelevanten Aufgaben die erforderlichen Kenntnisse und Fähigkeiten besitzen, um Maßnahmen, die das ISMS verbessern, erfolgreich umzusetzen.
- Regelmäßige strukturierte Prüfungen geben Rückschlüsse auf den Umsetzungsgrad und unterstützen kontinuierlich die Eignung, Angemessenheit und Wirksamkeit des Informationssicherheitsmanagementsystems.
- Wir orientieren uns an Good-Practice-Ansätzen (ISO 27001, ITIL, BSI-Grundschutz, etc.) um dem Stand der Technik zu entsprechen.
- Durch gezielte Maßnahmen und eine vitale Fehlerkultur wird eine kontinuierliche Verbesserung des Informationssicherheitsmanagementsystems angestrebt.

Wir schaffen Verlässlichkeit

- Unsere Mitarbeiter melden sämtliche erkannte Verletzungen der Informationssicherheit. Dadurch werden Informationssicherheitsvorfälle rasch erkannt und notwendige und angemessene Maßnahmen veranlasst.
- Wir legen bei der Zusammenarbeit mit unseren jahrelangen Partnern Wert auf ein hohes Niveau an Informationssicherheit und fordern auch von ihnen ein Mindestmaß an umgesetzten technischen und organisatorischen Maßnahmen.

6 Umsetzung

Informationssicherheit ist nicht nur eine Verantwortung der Unternehmensleitung. Es sind alle Mitarbeiter verpflichtet, Informationen zu schützen und den nötigen Mehraufwand für die Einhaltung der festgelegten Sicherheitsmaßnahmen zu Gunsten der unternehmerischen Gesamtsicht in Kauf zu nehmen. Insbesondere sind Führungskräfte in ihrem Bereich für die Einhaltung von etablierten Richtlinien und Verfahren verantwortlich.

Die Informationssicherheitspolitik ist in der pit-cup GmbH eingeführt und verpflichtend einzuhalten. Die Umsetzung der Informationssicherheitspolitik erfolgt durch spezifische Richtlinien und Verfahrensanweisungen. Die Einhaltung wird regelmäßig und anlassbezogen überprüft. Eine Nichteinhaltung kann sowohl disziplinäre als auch zivil- und strafrechtliche Folgen haben.

Johannes Meßner-Haidenthaler
Geschäftsführer
pit-cup GmbH

pit-cup GmbH
Palo-Alto-Platz 11
D-69124 Heidelberg
Tel. +49 6221 5393-0
Fax +49 6221 5393-11

info@pit.de | www.pit.de
GF: R. Umshaus, J. Messner
Registergericht Mannheim
HRB 335193

D-10178 Berlin
D-01157 Dresden
D-19057 Schwerin

Tel. +49 30 84711869-0
Tel. +49 351 407905-20
Tel. +49 385 48504-0