Leitlinie zur Informationssicherheit bei der MELOS GmbH

Dokumenteninformationen

Aktuelle Version	Stand, Datum	Klassifikations-stufe	Verteiler-kreis	Status	Freigabe	Veröffentlicht am
3.0	08.02.2022	Öffentlich	Extern	Freigegeben	08.02.2022 (am)	14.02.2022 (sk)

Fachbereich

Arbeitssicherheit		Datenschutz	x	IT-Sicherheit	x	Allgemein	x

Dokumentenverlauf

Version	Datum	Autor	Kommentare
0.1	31.05.2021	Sara Kneißl	Überführung Entwurf
0.2	28.07.2021	Sara Kneißl	Überarbeitung
1.0	03.08.2021	Andreas Manntz	Freigabe
1.1	26.10.2021	Sara Kneißl	Ergänzungen
2.0	26.10.2021	Andreas Manntz	Freigabe
2.1	31.01.2022	Sara Kneißl	Einarbeitung Kommentare DataGuard
3.0	08.02.2022	Andreas Manntz	Freigabe

Geltungsbereich

Dieses Dokument gilt für den gesamten Anwendungsbereich des Informationssicherheits-Managementsystems (ISMS) der MELOS GmbH.

Inhalt

Dokumenteninformationen 1
Dokumentenverlauf 1
Geltungsbereich 2
Referenzdokumente 3
Vorwort der Geschäftsleitung 4
Leitgedanken und Stellenwert der IT, Informationssicherheit 5
Bedeutung der Informationssicherheitsleitlinie 5
Anforderungen an Informationssicherheit 6
Maßnahmen zur Informationssicherheit 6
Unser Fachwissen, unser Vorsprung - Sorgfalt und Genauigkeit im Umgang mit Informationen 6
- Least Privilege-Prinzip 6
- Richtiger Umgang mit Dokumenten und Datenträgern 6
- Technische Sicherheit 6
- Eigenverantwortung 6

Umsetzung 7
Verantwortung des Managements 7
Dokumentenstruktur im ISMS 7
Kommunikation 7
Umgang mit Verstößen 8
Schlussbestimmungen 8

Referenzdokumente

- ISO/IEC 27001 Standard, Abschnitte 5.2 und 5.3
- Dokument zum ISMS-Anwendungsbereich
- Methodik zur Risikoeinschätzung und Risikobehandlung
- Erklärung zur Anwendbarkeit
- Dokumente des Qualitätsmanagement SharePoints

Vorwort der Geschäftsleitung

Informationssicherheit ist heute mehr denn je unverzichtbar für Unternehmen jeder Größe. Für die wirksame und vor allem nachhaltige Umsetzung von Informationssicherheit ist eine strukturierte Herangehensweise unumgänglich. Wir haben hierzu im Unternehmen ein **I**nformations**S**icherheits**M**anagement**S**ystem (**ISMS**) implementiert, dass die Aufgabe hat, in einem ständigen Verbesserungsprozess Informationssicherheit zu schaffen, zu erhalten und vor allem zu verbessern.

Hierfür haben wir klare Verantwortlichkeiten für die Informationssicherheit definiert und notwendige Ressourcen für den Wissensaufbau, sowie Personal und Budget bereitgestellt.

Die Stabsstelle "Beauftragter des integrierten Managementsystems (IMB)" ist bei uns im Haus zentraler Ansprechpartner für alle Fragen zum Thema des Integrierten Management Systems. Die Rolle des Informationssicherheitsbeauftragten (ISB) ist der zentrale Ansprechpartner im Bereich Informationssicherheit und initiiert, plant, überwacht und steuert alle Tätigkeiten in diesem Bereich. Derzeit wird diese Stellung durch einen externen ISB begleitet. Intern wird dieser durch den Koordinator der Informationssicherheit unterstützt. Der ISB und der interne Koordinator der Informationssicherheit unterstützen die Fachbereiche, ihre Prozesse konform zu den Vorgaben zur Informationssicherheit zu gestalten.

Die Leitlinie zur Informationssicherheit ist dabei zentral für den gesamten Informationssicherheitsprozess. Neben der Verpflichtung der Geschäftsführung zur Informationssicherheit werden darin Ziele und der Stellenwert der Informationssicherheit mit den jeweiligen Verantwortlichkeiten definiert. Unterstützend kommen Richtlinien zum Einsatz, die gemeinsam mit den Fachbereichen erstellt und im Unternehmen ausgerollt werden. Die Zusammenarbeit zwischen Geschäftsleitung, Fachbereich, IMB, ISB und interne Koordination Informationssicherheit, ermöglicht eine praxisnahe und gelebte Informationssicherheit.

Informationssicherheit ist ein wichtiger Bestandteil zur Sicherung des Fortbestands unseres Unternehmens und hat deshalb einen hohen Stellenwert in unserem Unternehmen. Unsere Mitarbeitenden sind angehalten, die Vorgabe, Leitlinien und Richtlinien zur Informationssicherheit zu beachten und einzuhalten.

Aus Gründen der besseren Lesbarkeit wird im Weiteren auf eine geschlechterspezifische Unterscheidung verzichtet. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung aller Geschlechter.

Gessertshausen, März 2022

Andreas Manntz	Christoph Duelli	Dr. Jens Riedel
Geschäftsführung	Geschäftsführung	Geschäftsführung

Informationssicherheit: Grundbegriffe

Vertraulichkeit – die Eigenschaft von Informationen, dass sie lediglich berechtigten Personen oder Systemen verfügbar gemacht werden

Integrität – die Eigenschaft von Informationen, dass sie lediglich von berechtigten Personen oder Systemen auf genehmigte Weise abgeändert werden können

Verfügbarkeit – die Eigenschaft von Informationen, dass sie lediglich berechtigten Personen zugänglich sind, wenn ein solcher Zugang notwendig ist

Informationssicherheit - Aufrechterhaltung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen

Informationssicherheits-Managementsystem – jener Teil des gesamten Managementprozesses, der sich mit Planung, Implementierung, Instandhaltung, Überprüfung und Verbesserung von Informationssicherheit befasst

Leitgedanken und Stellenwert der IT, Informationssicherheit Bedeutung der Informationssicherheitsleitlinie

Die Ideen und das Fachwissen unserer Mitarbeitenden sind das Fundament unseres Erfolgs. Der Geschäftserfolg der MELOS GmbH ist abhängig von vertraulichen, verfügbaren und integren Geschäftsinformationen, die MELOS mit Kunden, Zulieferern, Kooperationspartnern, Geldinstituten und anderen Institutionen austauscht. Die Informationstechnik ist die essenzielle Ressource unseres Geschäfts und unserer Arbeiten in allen Abteilungen.

Eine funktionsfähige Informationstechnik und ein sicherheitsbewusster Umgang mit ihr sind wesentliche Voraussetzungen für die Einhaltung unserer Informationssicherheitsziele: Verfügbarkeit, Integrität und Vertraulichkeit von Informationen.

Dem erklärten Unternehmensziel, zentrale Geschäftsprozesse mitsamt dort benötigten Informationswerten und IT-Systemen effektiv zu schützen, wird durch die Schaffung global gültiger Sicherheitsstandards und die Integration von Informationssicherheit in interne Prozesse entsprochen. Die definierten Informationssicherheitsziele tragen dabei zur Erreichung der Unternehmensziele bei.

Ein stets vorhandenes Bewusstsein im Bereich Informationssicherheit bei allen täglich anfallenden Aktivitäten wird von jedem Mitarbeitenden erwartet. Jeder Vorgesetzte ist verpflichtet, die Einhaltung der Vorschriften zur Informationssicherheit durch seine Mitarbeitenden sicherzustellen und zu kontrollieren. Jeder Mitarbeitende, der Schwachstellen im Bereich der Informationssicherheit erkennt, ist verpflichtet, diese seinem Vorgesetzten oder dem Informationssicherheitsbeauftragten mitzuteilen.

Anforderungen an Informationssicherheit

Diese Leitlinie und das gesamte ISMS müssen sowohl den rechtlichen und gesetzlichen Anforderungen als auch den vertraglichen Verpflichtungen entsprechen, die für die Organisation auf dem Gebiet der Informationssicherheit, Datengeheimnis, Geschäftskontinuität, Schutz persönlicher Daten und dem Schutz von Gesundheitsdaten maßgeblich sind.

Eine detaillierte Auflistung aller vertraglichen und rechtlichen Anforderungen wird mit der Liste der rechtlichen, amtlichen und vertraglichen Verpflichtungen künftig bereitgestellt.

Maßnahmen zur Informationssicherheit

Der Prozess bei der Auswahl von Maßnahmen (Sicherheitsmaßnahmen) ist in der Methodik zur Risikoeinschätzung und Risikobehandlung definiert.
Die gewählten Maßnahmen und deren Implementierungsstatus sind in der Erklärung zur Anwendbarkeit (Statement of Applicability = SOA) aufgeführt.

Unser Fachwissen, unser Vorsprung - Sorgfalt und Genauigkeit im Umgang mit Informationen

Least Privilege-Prinzip

Berechtigungen und Informationen werden restriktiv und nur an die Personen und Stellen vergeben, die diese auch benötigen. Den beteiligten Personen muss dabei klar sein, wie vertraulich Informationen sind und für wen sie bestimmt sind. Das gilt natürlich auch für Berechtigungen in IT-Systemen und für Zutrittsrechte.

Richtiger Umgang mit Dokumenten und Datenträgern

Der Umgang mit Dokumenten und Datenträgern mit vertraulichem Inhalt ist ein zentraler Punkt beim Schutz von Informationen. Sparsamkeit beim Ausdrucken von sensiblen Informationen, die sichere Aufbewahrung von Dokumenten und Speichermedien in verschlossenen Bereichen sowie die ordnungsgemäße Entsorgung liegen in der Verantwortung eines jeden Mitarbeitenden.

Technische Sicherheit

Das Sicherheitsniveau kann durch technische Mittel maßgeblich gestärkt werden. Zielgerichtete Investitionen in die Absicherung sowie eine sichere Konzeption unserer IT und unserer Gebäude gehören deshalb ebenfalls zur Strategie der Absicherung. Dabei liegt uns besonders am Herzen, unsere wichtigsten und sensibelsten Einrichtungen zu schützen.

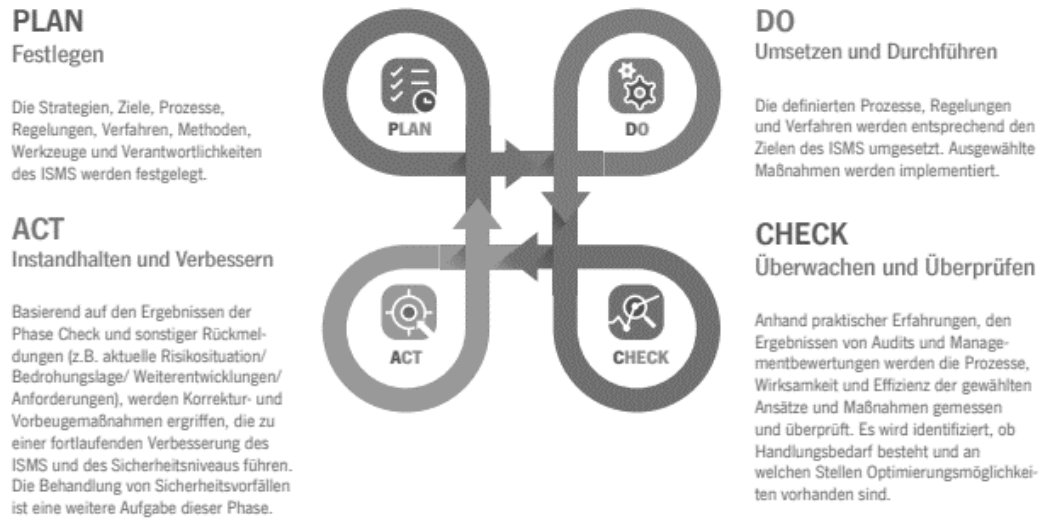
Eigenverantwortung

Jeder Mitarbeitende steht in der Verantwortung, Schwachstellen, verdächtige Situationen und Vorfälle zu melden. Das Kennen und Beachten von Vorgaben durch unsere Mitarbeitenden werden dabei als Voraussetzung gesehen und von jedem Mitarbeitenden erwartet.

Umsetzung

Die MELOS GmbH setzt zur Sicherstellung der Umsetzung von Informationssicherheitsanforderungen ein Informationssicherheits-Managementsystem (ISMS) in Anlehnung an den internationalen Standard ISO/IEC 27001:2015, ISO/IEC 9001:2015 und in der Produktlinie „MDN High Security Level“ TISAX® sowie an die relevanten gesetzlichen und branchenspezifischen Vorgaben ein.

Das ISMS folgt dem dort 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 sicherzustellen.



Verantwortung des Managements

Die Unternehmensleitung ist innerhalb des Unternehmens für die Informationssicherheit verantwortlich und verpflichtet sich dazu, 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 des vorhandenen Sicherheitsbewusstseins ihrer Mitarbeitenden hinsichtlich der Informationssicherheit verantwortlich.

Dokumentenstruktur im ISMS

Diese Leitlinie ist das oberste Dokument des ISMS. Ihr untergeordnet sind auf der Ebene zwei Richtlinien sowie auf der Ebene drei Arbeitsanweisungen und Prozessbeschreibungen.

Kommunikation

Die Geschäftsführung hat sicherzustellen, dass alle Mitarbeitenden der MELOS GmbH sowie entsprechenden externen Parteien (siehe oben Anwendungsbereich) mit dieser Leitlinie und allen untergeordneten Dokumenten vertraut sind.

Umgang mit Verstößen

Verstöße gegen diese Leitlinie und alle untergeordneten Richtlinien und Arbeitsanweisungen können arbeits-, zivil- oder strafrechtliche Maßnahmen nach sich ziehen. Die MELOS behält sich das Recht vor, die Einhaltung dieser Leitlinie und aller untergeordneten Dokumente regelmäßig zu überprüfen.

Schlussbestimmungen

Diese Vorstellung der Informationssicherheit bei der MELOS GmbH wird durch eine interne Leitlinie Informationssicherheitsstrategie und weitere Richtlinien und Prozessbeschreibungen ergänzt, die aus detaillierten Organisations- und Sicherheitsregeln bestehen und daher der internen Verwendung vorbehalten sind.