

- Leitlinie -

Zweck der Regelung	Festlegung der Informationssicherheitspolitik und -ziele des Unternehmens
Verantwortlich	Geschäftsführung
Bearbeiter	ISB
Geltungsbereich	Organisationsweit
Dokumentenstatus	Freigegeben
Einstufung	Öffentlich
Gültig ab	18. Februar 2019
Frist zur Überprüfung	Jährlich
Version	3.0
Ersetzt	2.0
Bezugsdokumente	-
Identifikationsnummer	ISMS-01-001
Dateiname	ISMS-01-001-Leitlinie_Policy_20230817_v3.0
Anzahl der Seiten <small>(inkl. Deckblatt)</small>	8

Inhaltsverzeichnis

Informationssicherheitspolitik.....	3
1 Zweck.....	5
2 Geltungsbereich.....	5
3 Unsere Informationssicherheitsziele.....	5
4 Unser Informationssicherheitsmanagementsystem.....	7
5 Unsere gemeinsame Verantwortung.....	7
6 Aktualisierung, Inkrafttreten.....	8
A Änderungsjournal.....	8
B Liste der mitgeltenden Dokumente.....	8

Informationssicherheitspolitik

Als führender IT-Lösungsanbieter für wertschöpfende Dienstleistungen und integrierte Produkte in der Prozessindustrie in der Downstream-Branche hat die Sicherheit und der Schutz von Informationen höchsten Stellenwert für Implico.

Informationssicherheit bedeutet für uns, dass:

- unsere Kunden und Mitarbeiter*innen alle für Geschäftsprozesse notwendigen Informationen best- möglich ohne Unterbrechungen oder Störungen nutzen können. Dies umfasst zum einen unsere internen Informationen und zum anderen Informationen von Kunden und Dritten, die auf unseren Systemen verarbeitet werden;
- wir die Integrität dieser Informationen aufrechterhalten und die Richtigkeit und Vollständigkeit gegen ungewollte Veränderungen schützen;
- die Vertraulichkeit der Informationen gewahrt wird und Informationen unserer Kunden, Mitarbeiter*innen und Dritter sowie die elektronische Kommunikation vor ungewollter Offenlegung abgesichert wird;
- wir regulatorische und gesetzliche Vorgaben einhalten, um die Compliance des Unternehmens in Bezug auf die relevante nationale und internationale Gesetzgebung zu gewährleisten und die entsprechenden Anforderungen zu erfüllen;
- wir die Sicherheit der Informationen auf Basis unserer Risikomanagement-Methode steuern;
- ein Business Continuity Management und entsprechende Vorkehrungen Unterbrechungen der Geschäftsprozesse entgegenwirkt und kritische Geschäftsprozesse vor Auswirkungen durch Großstörungen oder Desastern schützt. Geschäftsfortführungspläne werden regelmäßig überprüft und angepasst;
- unsere Mitarbeiter*innen durch regelmäßige Schulungen, Trainings und Awareness-Maßnahmen die notwendigen Kenntnisse zum Schutz und der Sicherheit von Informationen aufbauen und weiterbilden;
- alle tatsächlichen oder vermuteten Verstöße gegen die Sicherheit von Informationen den entsprechenden Verantwortlichen (insb. Incident Response) gemeldet und durch diese geprüft und nachverfolgt werden;
- wir durch ein rollenbasiertes Berechtigungskonzept grundsätzlich gewährleisten, dass Kunden, Mitarbeiter*innen und Dritte nur auf Informationen Zugriff haben, die sie im Rahmen ihrer Tätigkeit benötigen, und Informationen gegen ungewollten Zugriff geschützt sind;
- Richtlinien, Anweisungen und Verfahren unseren Mitarbeiter*innen auf einer Plattform zur Verfügung stehen, um die Informationssicherheitspolitik durchsetzen zu können;
- die internen Verantwortlichen für die Informationssicherheit ein Information Security Management System (ISMS) kontinuierlich weiterentwickeln. Dies umfasst auch die direkte Verantwortung zur Durchführung interner Audits und die Fortschreibung relevanter Richtlinien, Anweisungen und Verfahren;
- alle Implico-Mitarbeiter*innen die Vorgaben zur Informationssicherheitspolitik einhalten werden.
- Die jeweiligen Manager sind für ihren Bereich für die Implementierung und Einhaltung verantwortlich.

Die Geschäftsführung der Implico GmbH hat diese Informationssicherheitspolitik freigegeben und allen interessierten Parteien zugänglich gemacht.

Implico Information Security Policy Statement

As a leading IT solution provider of value-added services and integrated products in the process industry in the downstream sector, Implico attaches great significance to the security and protection of information.

For us, information security means that:

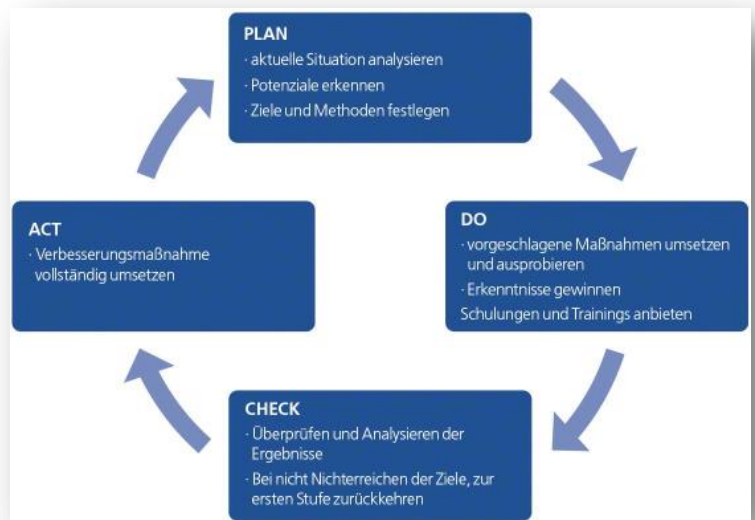
- our customers and employees should be able to use all the information required by business processes with minimal interruption or interference. This includes both our internal information and information on customers and third parties that is processed in our systems;
- we will maintain the integrity of this information and will protect its correctness and completeness against unwanted changes;
- the confidentiality of this information is preserved and information of our customers, employees and third parties as well as electronic communication will be secured against unwanted disclosure;
- we adhere to regulatory and legal requirements in order to ensure the company's compliance with respect to the relevant national and international laws and to fulfill the corresponding requirements;
- we manage the security of information on the basis of our risk management method;
- business continuity management and measures counteract interruptions in business processes and protect critical business processes against the effects of major disruptions or disasters. Business continuity plans are regularly checked and updated.
- our employees develop and extend the knowledge required for the protection and security of information through regular education, training sessions and awareness measures;
- all actual or suspected breaches of information security are reported to the respective responsible parties (especially Incident Response) and are investigated and tracked by them;
- we strictly guarantee, through a role-based access plan, that customers, employees and third parties only have access to information that they require in the context of their work, and that information is protected against unwanted access;
- guidelines, instructions, and procedures will be made available on a platform to our employees, in order to effectuate the information security policy;
- the parties internally responsible for information security continuously enhance the ISMS. This also includes the direct responsibility for conducting internal audits and the updating of relevant guidelines, instructions, and procedures;
- all Implico employees will comply with information security policy. The managers are responsible for implementation and compliance within their respective units.

The Board of Directors of Implico GmbH has approved this information security policy and made it available to all interested parties.

1 Zweck

Implico ist als führender IT-Lösungsanbieter für wertschöpfende Dienstleistungen und integrierte Produkte in der Prozessindustrie elementarer Beteiligter in der Downstream-Branche. Unsere Kunden vertrauen auf die Leistungen und Verlässlichkeit unseres Unternehmens. Vor dem Hintergrund der stetig steigenden Integration von IT-Systemen in unsere Geschäftstätigkeit und die Geschäftstätigkeit unserer Kunden nimmt die Sicherheit von Informationen einen sehr hohen Stellenwert für einen reibungslosen und effizienten Ablauf der Geschäftsprozesse ein. Es ist unerlässlich, Informationen unserer Kunden, Mitarbeiter*innen und unseres Unternehmens vor möglichen Risiken zu schützen und die Funktionsfähigkeit der Informations- und Kommunikationssysteme zu erhalten und zu verbessern. Negative Auswirkungen auf das Geschäft und damit verbundene Kosten sollen so minimiert und dadurch der Erfolg und das Ansehen von Implico nachhaltig gesichert werden. Dazu gehört auch der Schutz unseres Knowhows und Wissens im Unternehmen.

Vor diesem Hintergrund hat sich Implico dazu entschlossen, ein ISMS einzuführen, zu erhalten und kontinuierlich zu verbessern. Diese Leitlinie zur Informationssicherheit stellt den Rahmen für das ISMS dar und definiert die Ziele, an welchen sich alle Maßnahmen in Bezug auf die Sicherheit und den Schutz von Informationen orientieren sollen.



2 Geltungsbereich

Diese Leitlinie zur Informationssicherheit sowie alle ihr untergeordneten Dokumente gelten im Rahmen des Anwendungsbereichs des ISMS für alle Mitarbeiter: innen der Implico GmbH– unabhängig vom Arbeitsort –, sowie (sofern anwendbar) für externe Dienstleister und Lieferanten. Die Zertifizierung bezieht sich auf die Entwicklung, Integration und der Betrieb von Applikationen zur Optimierung von Logistik- und Geschäftsprozessen für Öl- und Gas-Unternehmen im Downstream- Bereich. Der Geltungsbereich ist in «Richtlinie Informationssicherheit» weiter spezifiziert. Die Implico, Inc. (USA) und die Implico B.V. (Niederlande) sind out of Scope.

3 Unsere Informationssicherheitsziele

Das Zusammenspiel der nachfolgend genannten Ziele ist für unseren weiteren Erfolg als Unternehmen im Öl- und Gassektor essenziell, um uns weiterhin auf dem globalen Markt zu behaupten. Wachsende Marktanforderungen, aber auch interne Anforderungen und selbst gesetzte Vorgaben, setzen den Fokus auf Vertraulichkeit, Integrität, Authentizität und nicht zuletzt Verfügbarkeit diejenigen zentralen Ziele, die für unseren Geschäftsbetrieb und die Weiterentwicklung unumgänglich sind. Die Informationssicherheitsziele der Implico sind im Einzelnen:

Verfügbarkeit

Informationen werden zur richtigen Zeit am richtigen Ort bereitgestellt.

Aus unserem eigenen Qualitäts- und Leistungsanspruch und aus den vertraglichen Verpflichtungen müssen wir gewährleisten, dass alle betriebsnotwendigen Daten und Informationen zur Verfügung stehen, um einen reibungslosen Geschäftsbetrieb unserer Kunden und der Implico selbst sicherstellen zu können.

Aufgrund der besonders auf Kundenseite gewachsenen Anforderungen an die Verfügbarkeit, ist eines der ständigen Ziele der Implico, die Verfügbarkeit von Daten und Informationen zu erhalten und stetig zu verbessern.

Integrität

Informationen bzw. Daten sind unversehrt (korrekt).

Wir haben aus unseren Leistungs- und Qualitätsansprüchen und aus den vertraglichen Verpflichtungen, sowohl das Interesse als auch die Pflicht, die Richtigkeit, Vollständigkeit und Nachvollziehbarkeit der Informationen sicherzustellen. Informationen der Öl- und Gasbranche sind besonders sensibel, so dass die Implico als zentraler Akteur die Integrität dieser Informationen sicherstellen und ausbauen muss, um weiterhin als kompetenter und vertrauenswürdiger Dienstleister für Kunden dieser Branche auftreten zu können. Die zunehmende Integration der IT und die fortschreitende technologische Weiterentwicklung werden zukünftig weitere Herausforderungen an die Integrität stellen, so dass dieses Ziel eine zentrale Bedeutung im Rahmen unserer Dienstleistungen erhalten wird.

Vertraulichkeit

Informationen sind nur für autorisierte Personen zugänglich.

In Bezug auf die Informationssicherheit ist eines der Ziele der Implico, die Vertraulichkeit von Informationen auf einem hohen Niveau zu gewährleisten und stetig zu verbessern. Dies ergibt sich aus zumeist vertraglichen Vorgaben, aber auch aus eigenen wirtschaftlichen Interesse. Die Alleinstellungsmerkmale insbesondere unserer Produkte auf dem Markt bedürfen einem speziellen Schutz, vor allem in Hinblick auf einem angestrebten weltweiten Unternehmenswachstum und der damit einhergehenden Gefahr der Industrie- und Wirtschaftsspionage.

Authentizität

Informationen wurden von der angegebenen Quelle erstellt.

Durch die wachsende Globalisierung, eine größere Zahl an Beteiligten (Kunden, Mitarbeiter*innen und Dritte) und zunehmend (rein) technischer Kommunikationswege sind besonders die Anforderungen in puncto Authentizität und Nachweis der Identität zentraler geworden. Die kontinuierliche Optimierung der Prozesse und Maßnahmen zur Sicherstellung der Authentizität von Akteuren, Informationen und anderen Objekten im Geschäftsumfeld der Implico ist elementar, um das bestehende Vertrauen zu erhalten und auszubauen.

Wissen und Mitwirkung aller Beteiligten

Da diese vier Ziele eine zentrale Bedeutung für das Unternehmen haben, ergibt sich daraus als weiteres und fünftes Ziel, dass das Wissen zur Informationssicherheit, die Umsetzung von Richtlinien und Prozessen und

das Leben dieser Ziele von allen Kunden, Mitarbeiter*innen und Lieferanten der Implico aktiv mitgetragen wird.

4 Unser Informationssicherheitsmanagementsystem

Implico verfügt über ein an der DIN ISO / IEC 27001 ausgerichtetes ISMS.

Der Anwendungsbereich des ISMS ist in «Richtlinie -Informationssicherheit» in der jeweils gültigen Fassung spezifiziert. Für das ISMS sind Rollen und Prozesse definiert und Verantwortliche benannt.

Neue Prozesse und Technologien, neue Bedrohungen und Gefahren, gesetzliche Neuregelungen, geänderte Anforderungen auf Kundenseite und das weitere Wachstum der Implico machen einen kontinuierlichen Überprüfungs- und Verbesserungsprozess notwendig. Um diesen Prozess dauerhaft zu etablieren, sind Richtlinien, Prozesse und Regelungen zur Informationssicherheit regelmäßig zu prüfen, ggf. zu überarbeiten und zu verbessern. Alle Maßnahmen zur Aufrechterhaltung und Verbesserung der Informationssicherheit ist regelmäßig zu auditieren. Das ISMS insgesamt ist einer regelmäßigen Bewertung durch das oberste Management zu unterziehen und kontinuierlich zu verbessern.

5 Unsere gemeinsame Verantwortung

Grundlage für die erfolgreiche Umsetzung und Ausgestaltung unserer Informationssicherheitsziele sind die Integration in unser Werte- und Normenverständnis und in alle alltäglichen Abläufe und Tätigkeiten der Implico. Dies setzt die Unterstützung der Geschäftsführung voraus, beinhaltet aber auch das Mitwirken aller Mitarbeiter*innen.

Gemeinsam tragen wir alle eine große Verantwortung für den richtigen Umgang mit Informationen und Informationstechnologien von der Entstehung, Weitergabe, Speicherung und Verarbeitung bis hin zur Vernichtung. Die Technologien und notwendigen Ressourcen werden durch die Geschäftsführung bereitgestellt, Mitarbeiter*innen durch Qualifizierungs- sowie Sensibilisierungsmaßnahmen unterstützt, um unsere Informationssicherheitsziele einhalten zu können.

Dadurch leisten wir gemeinsam einen entscheidenden Beitrag, dass Implico als vertrauenswürdiger und verlässlicher Geschäftspartner wahrgenommen wird und weiterhin als konkurrenzfähiger Marktteilnehmer agieren kann. Zudem stellen wir sicher, dass unsere Unternehmenswerte geschützt werden, der zukünftige Geschäftsbetrieb langfristig gewährleistet wird und Implico der führende IT-Lösungsanbieter in der Downstream-Branche bleibt.

6 Aktualisierung, Inkrafttreten

Im Rahmen der Fortentwicklung der Informationssicherheit sowie technologischer oder organisatorischer Veränderungen wird dieses Dokument regelmäßig auf einen Anpassungs- oder Ergänzungsbedarf hin überprüft.

Dieses Dokument tritt mit Freigabe in Kraft und ist ab dem auf dem Deckblatt verzeichneten Datum anzuwenden. Die Mitarbeiter*innen sind in geeigneter Art und Weise über die geänderten Vorgaben in Kenntnis zu setzen.

A Änderungsjournal

Version	Datum	Bearbeiter	Synopse
1.0	18.12.2018	SBuhre	Freigabe GF
2.0	18.02.2019	SBuhre	Freigabe SB
2.0	11.02.2020	FHetmank	GF: Review, Dokument hat ohne Änderungen Bestand
2.0	22.02.2023	MPoelckow	Review im Managementreview, Dokument hat ohne Änderungen Bestand
3.0	17.08.2023	LMoussa	Review; Aktualisierung des neuen CI, Ergänzung des Geltungsbereichs und PDCA-Zyklus, Aktualisierung des Dateinamens
3.0	18.08.2023	EBille	Freigabe und Review

B Liste der mitgeltenden Dokumente

ID	Titel	Link
ISMS-02-001	Richtlinie Informationssicherheit	