KISTERS
Leitlinie zu
Informationssicherheit, Datenschutz und Business Continuity

v.4.1, 2025-09-22

Verantwortlich:
KISTERS CEO

Inhaltsverzeichnis

1 Einleitung

Die KISTERS Gruppe, bestehend aus der KISTERS AG mit Hauptsitz in Aachen, Deutschland, und ihren nationalen und internationalen Tochterunternehmen, ist ein weltweit erfolgreicher Anbieter von Software- und Hardwarelösungen und Dienstleistungen. Das Portfolio von KISTERS umfasst Lösungen für nachhaltiges Ressourcenmanagement von Energie, Wasser, Wetter und Umwelt, für Arbeits- und Umweltschutz und Compliance, Sicherheit und Logistik, Softwarelösungen für 3D-Viewing, IT-Hardware wie Großformatdrucker (3D/2D) und Scanner sowie Dienstleistungen im Umweltconsulting (Siedlungswasserwirtschaft, Tiefbau, Erschließung, Wasserbau und -Wirtschaft). KISTERS bietet außerdem Dienstleistungen zur Ergänzung seiner Hardware- und Softwarelösungen an, einschließlich des Betriebs der KISTERS-Softwarelösungen in der KISTERScloud.

2 Motivation und Ziele

Informationen und ihre Verarbeitung sind der Schlüssel für die Durchführung unserer Geschäftsaktivitäten. Daher ist der Schutz dieser Informationen, insbesondere personenbezogener Daten, vor unbefugtem Zugriff, unrechtmäßiger Änderung oder Verbreitung sowie nicht tolerierbarer Nichtverfügbarkeit von wesentlicher Bedeutung.
Alle unsere wesentlichen strategischen und operativen Funktionen und Aufgaben werden maßgeblich durch IT-Systeme unterstützt. Ein Ausfall oder eine Kompromittierung dieser Systeme muss vermieden oder zumindest kurzfristig so kompensiert werden, dass der Geschäftsbetrieb aufrechterhalten oder schnellstmöglich wiederhergestellt werden kann.
Als Anbieter von Softwarelösungen und KISTERScloud-Diensten übernehmen wir nicht nur die Verantwortung für unsere eigene Informationssicherheit, sondern auch für die Informationssicherheit unserer Kunden und Partner. Daher ist es notwendig, unsere Lösungen und KISTERScloud-Dienste entsprechend den Sicherheitsanforderungen unserer Kunden und Partner zu entwickeln und die Entwicklungsprozesse, Werkzeuge und Umgebungen entsprechend zu gestalten. Dies gilt insbesondere für Softwarelösungen, die zur Verarbeitung personenbezogener Daten oder als kritische Komponenten im Bereich der kritischen Infrastrukturen eingesetzt werden.

Daher hat der Vorstand der KISTERS AG diese Richtlinie zur Informationssicherheit verabschiedet, um Informationssicherheit, Datenschutz und Geschäftskontinuität als wichtige Bestandteile unserer Unternehmensstrategie zu verankern.

2.1 Informationssicherheit

Das Ziel der Informationssicherheit bei KISTERS ist die Unterstützung der Absicherung unseres Unternehmens und unserer geschäftlichen Aktivitäten durch

- die Gewährleistung von Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität in unseren Informationen, Prozessen und Systemen,
- den Schutz unserer Interessen und der Vertrauenswürdigkeit bei unseren Kunden durch die Sicherung unserer Arbeitsfähigkeit in Bezug auf unsere IT-Systeme, Programme, Daten sowie Produkte und Dienstleistungen,

- den Schutz der Interessen unserer Kunden und Partner durch die sichere und kontinuierliche Bereitstellung unserer Softwarelösungen, Systeme und Dienstleistungen sowie die vertrauliche Behandlung aller Firmendaten,
- den Schutz der Interessen der Anwender unserer Softwarelösungen durch die Einhaltung der Vorgaben zu Datenschutz und Informationssicherheit in unseren Softwarelösungen, die konsequente Anwendung von „Best Practices“ und Grundsätzen der sicheren Softwareentwicklung sowie die Absicherung unserer Entwicklungsumgebungen,
- den Schutz unseres Unternehmens, unserer Kunden, Partner und Mitarbeiter durch Einhaltung der geltenden gesetzlichen Bestimmungen sowie sonstiger rechtsverbindlicher Regelungen.

Damit ergeben sich als abgeleitete Ziele die Sicherstellung

- der Vertraulichkeit dieser Informationen, insbesondere von personenbezogenen Daten,
- der Verfügbarkeit unserer Infrastruktur und unserer gesamten Geschäftsinformationen,
- der Integrität sämtlicher IT-Systeme und Informationen,
- die Authentizität aller an der Informationsverarbeitung beteiligten Akteure und Interessengruppen,
- der Informationssicherheit unserer Softwarelösungen,
- des Schutzes unseres Unternehmens vor Datenverlusten und Informationsabfluss.

2.2 Datenschutz

Der Schutz natürlicher Personen in Bezug auf die Verarbeitung personenbezogener Daten ist ein Grundrecht. Das Ziel des Datenschutzes und des Schutzes der Privatsphäre innerhalb von KISTERS besteht darin, Folgendes zu gewährleisten:

- den Schutz aller personenbezogenen Daten von Kunden, Partnern, Zulieferern und Mitarbeitern in unseren IT-Systemen und –Prozessen zur Gewährleistung der informationellen Selbstbestimmung und dem Schutz der Privatsphäre aller betroffenen Personen,
- die Wahrung der Interessen der Nutzer unserer Softwarelösungen und KISTERScloud-Dienste durch Einhaltung der Datenschutzbestimmungen in unseren Softwarelösungen.

2.3 Business Continuity – Geschäftsfortführung

Im Falle eines Notfalls oder einer Krise sind unsere Geschäftsprozesse oder die Erfüllung unserer Aufträge aufgrund fehlender oder nicht verfügbarer Ressourcen wie Personal, Informationen, Infrastruktur und Dienstleister gefährdet.
Unsere Kunden, Partner, Mitarbeiter und andere Interessengruppen erwarten jedoch, dass KISTERS geeignete Vorkehrungen trifft um entstandene Schäden schnell, systematisch und angemessen zu begrenzen und zu beheben. Die Nichtverfügbarkeit wesentlicher Ressourcen muss kurzfristig so kompensiert werden, dass der Geschäftsbetrieb aufrechterhalten oder schnellstmöglich wiederhergestellt werden kann.
Ziel des Business Continuity Managements bei KISTERS ist die Aufrechterhaltung der Geschäftsaktivitäten und die Erfüllung der vertraglichen Verpflichtungen in Notfällen, um

- unsere Mitarbeiter in Notfällen jederzeit zu schützen,
- die kontinuierliche Ausführung aller unserer kritischen Geschäftsprozesse zu ermöglichen,

- die kontinuierliche Erfüllung unserer Aufgaben und die Erbringung unserer Dienstleistungen wie Support und KISTERScloud-Betrieb für unsere Kunden und Partner zu ermöglichen,
- unsere Interessen und unsere Vertrauenswürdigkeit in den Augen unserer Kunden und Partner durch eine angemessene und systematische Notfallplanung zu wahren,
- etwaige negative Folgen von Notfällen für Kunden, Partner und Lieferanten abzumildern,
- Notfälle bei unseren Kunden, Partnern und Lieferanten, die unsere Geschäftsaktivitäten oder Dienstleistungen beeinträchtigen, abzumildern oder zu kompensieren,
- personenbezogene Daten vor Verlust, Missbrauch und Manipulation zu schützen.

Dies soll sowohl durch proaktive/präventive Maßnahmen und Kontrollen (Notfallplanung) als auch durch reaktive Maßnahmen (Notfallreaktion) erreicht werden, um

- die Widerstandsfähigkeit unserer Geschäftsprozesse und der Bereitstellung von Diensten gegen störende Einflüsse zu verbessern,
- während eines Notfalls kritische Geschäftsprozesse und Dienste - möglicherweise in reduzierter oder eingeschränkter Form - weiterzuführen.

3 Geltungsbereich

Diese Leitlinie beschreibt den allgemeinen strategischen Ansatz von KISTERS für das Management der Informationssicherheit, des Datenschutzes und der Geschäftskontinuität. Sie gilt für alle Geschäftsbereiche, Standorte und Mitarbeiter der KISTERS Gruppe einschließlich der gesamten IT-Infrastruktur und der darin betriebenen IT-Systeme.

4 Rollen, Verantwortlichkeiten und Abhängigkeiten

Die Gesamtverantwortung für Informationssicherheit, Datenschutz und Business Continuity trägt der Vorstand der KISTERS AG. Der Vorstand der KISTERS AG unterstützt die systematische Verfolgung der Sicherheitsziele, indem er eine Organisation für den Aufbau und den Betrieb eines Managementsystems für Informationssicherheitsmanagement (ISMS), Datenschutzmanagement (DPMS) und Business Continuity Management (BCMS) etabliert.

Der Vorstand delegiert die Umsetzung des Managementsystems an offiziell eingesetzte Beauftragte, die direkt an den Vorstand der KISTERS AG berichten:

- Der KISTERS Chief Information Security Officer (CISO) ist für die Entwicklung und Ausführung der Informationssicherheitskonzepte und die Überwachung ihrer Einhaltung verantwortlich.
- Der KISTERS Datenschutzbeauftragte (DSB) ist für die Entwicklung, Umsetzung und Überwachung von Datenschutzkonzepten zuständig, um die Einhaltung der geltenden Datenschutzbestimmungen bei allen Geschäftsaktivitäten zu gewährleisten.
- Der KISTERS Business Continuity Management Officer (BCMO) steuert die Aktivitäten zur Notfallvorbereitung für die KISTERS und trägt dazu bei. Er ist verantwortlich für die Entwicklung, Implementierung, Pflege und kontinuierliche Verbesserung des Business Continuity Managements und der damit verbundenen Prozesse und Dokumente.

Die eingesetzten Beauftragten werden als gegenseitige Stellvertreter benannt. Sie werden von Informationssicherheitsteams und Business Continuation Teams (IS-Teams, BCM-Teams) unterstützt, die für die Umsetzung dieser Leitlinie in bestimmten Geschäfts- oder Anwendungsbereichen verantwortlich sind. Die

IS-Teams und BCM-Teams werden entsprechend den Rollen und Verantwortlichkeiten für die einzelnen Geschäfts- oder Anwendungsbereiche zusammengestellt.
Der Vorstand stellt den Beauftragten und den IS- und BCM-Teams ausreichende finanzielle und zeitliche Ressourcen zur Verfügung, damit sie sich regelmäßig weiterbilden, auf dem Laufenden halten und die vom Vorstand festgelegten Ziele in Bezug auf die Informationssicherheit, den Datenschutz und die Geschäftskontinuität erreichen können.
Die Beauftragten sind frühzeitig in alle Projekte einzubeziehen, um Aspekte der Informationssicherheit, des Datenschutzes und der Geschäftskontinuität bereits in der Planungsphase zu berücksichtigen.
Die IS-Teams, BCM-Teams und die Beauftragten sind von allen Mitarbeitern bei ihrer Arbeit zu unterstützen. Die Mitarbeiter müssen sich in allen Fragen der Informationssicherheit, des Datenschutzes und der Business Continuity an die Weisungen der Beauftragten halten.

5 Anwendbare gesetzliche und sonstige Anforderungen

Die Anforderungen an die Informationssicherheit, den Datenschutz und die Geschäftskontinuität werden durch die Anforderungen von Interessengruppen, gesetzlichen Vorschriften, unseren Geschäftszielen und den Best Practices der Branche definiert. Die wichtigsten Interessengruppen sind Kunden, Partner, Lieferanten und Mitarbeiter.
Aufgrund der Vielfalt der von KISTERS angebotenen Dienstleistungen und seiner weltweiten Geschäftstätigkeit können die Anforderungen von Interessengruppen und Behörden je nach den spezifischen Umständen variieren. Die Anforderungen der Interessengruppen sind in individuellen Verträgen manifestiert, die bei der Umsetzung dieser Leitlinie berücksichtigt werden müssen. Nationale und internationale Gesetze und Vorschriften, die auf die Geschäftstätigkeit oder das Dienstleistungsangebot von KISTERS anwendbar sind, werden von den Beauftragten oder delegierten Spezialisten regelmäßig überprüft. Im Rahmen des ISMS wird ein Kataster der geltenden Gesetze und Vorschriften geführt.
Zur Einhaltung von Best Practices der Branche richten wir unsere Systeme und Geschäftspraktiken an nationalen und internationalen Standards wie ISO/IEC 27001, ISO/IEC 22301, BSI Grundschutz, BSI Standard 200-4, BSI C5, AICPA SOC 2 und anderen anwendbaren Rahmenwerken aus. Wann immer dies erforderlich und möglich ist, bemühen wir uns um unabhängige Prüfungen und Zertifizierungen nach diesen Standards.

6 Maßnahmen und Verfahren

Die KISTERS Leitlinie zur Informationssicherheit folgt dem Grundsatz, dass der Aufwand für Maßnahmen und Verfahren immer in Relation zum erzielten Sicherheitsgewinn, zum Nutzen der betroffenen Interessengruppen und zum Wert der zu schützenden Werte gesetzt werden muss. Alle Sicherheitsmaßnahmen sind so zu wählen, dass sie geeignet und angemessen sind. Sie müssen die Risiken so weit wie möglich minimieren und in einem angemessenen Verhältnis zu den Kosten oder Verlusten stehen, die im Schadensfall entstehen könnten.
Die in dieser Leitlinie dargelegten Maßnahmen und Verfahren sind durch zusätzliche spezifische Richtlinien, Arbeitsanweisungen und andere geeignete Regelungen zu ergänzen.

6.1 Informationssicherheit

Für alle betrieblichen Werte - Informationen, Prozesse, IT-Anwendungen, IT-Systeme usw. - sind System- oder Service-Owner zu benennen, die den jeweiligen Schutzbedarf festlegen, Informationen klassifizieren und Zugriffsberechtigungen vergeben. Für alle verantwortlichen Funktionen sind Stellvertreter zu benennen. Durch Unterweisungen und angemessene Dokumentation muss sichergestellt werden, dass die System- und Diensteigentümer und ihre Stellvertreter in der Lage sind, ihre Aufgaben zu erfüllen.
Auf der Grundlage der Analyse des Schutzbedarfs sowie der identifizierten und bewerteten Risiken sind geeignete personelle, organisatorische und technische Maßnahmen zu definieren.
Gebäude und Räume sind durch geeignete Zutrittskontrollen zu schützen. Der Zugang zu IT-Systemen ist durch geeignete Zugangskontrollen und der Zugriff auf Informationen durch ein restriktives Berechtigungskonzept zu schützen, insbesondere wenn es sich um personenbezogene Daten handelt.
Auf allen IT-Systemen sind Programme zum Schutz vor Computerviren zu installieren. Alle Internet-Gateways sind mit einer geeigneten Firewall zu schützen. Alle Schutzprogramme sind so zu konfigurieren und zu administrieren, dass sie einen wirksamen Schutz bieten und unbefugte Zugriffe und Manipulationen verhindert werden. Alle IT-Systeme sind zu überwachen, um mögliche Sicherheitsereignisse schnellstmöglich erkennen zu können. Darüber hinaus haben die IT-Anwender diese Sicherheitsmaßnahmen durch sicherheitsbewusstes Arbeiten zu unterstützen und bei Auffälligkeiten die entsprechenden Ansprechpartner zu informieren.
Datenverluste lassen sich nie ganz ausschließen. Eine umfassende Datensicherheit soll gewährleisten, dass der IT-Betrieb schnell wiederhergestellt werden kann, wenn Teile des betrieblichen Datenbestandes verloren gehen oder offensichtlich defekt sind. Um Schäden oder Verluste für KISTERS oder KISTERS-Kunden als Folge von Sicherheitsereignissen zu begrenzen oder zu verhindern, muss die Reaktion auf Sicherheitsereignisse schnell und entschlossen nach einem etablierten Incident-Management-Prozess erfolgen.
Die Notfallkontrollen sind in einem Notfallvorsorgekonzept zusammenzufassen. Unser Ziel ist es, kritische Geschäftsprozesse sowie die unserer Kunden, insbesondere der KISTERScloud-Kunden, aufrechtzuerhalten bzw. selbst zu betreiben und die Verfügbarkeit ausgefallener Systeme innerhalb eines vertretbaren Zeitraums wiederherzustellen. Dies soll durch die Sicherung von Informationen und IT-Systemen und erprobte Wiederherstellungsverfahren für kritische Systeme unterstützt werden.
Soweit Dienstleistungen an externe Dritte ausgelagert werden, sind in den vertraglichen Vereinbarungen spezifische Anforderungen an die Informationssicherheit vorzugeben. Das Recht zur Kontrolle wird festgelegt.
Die Softwareentwicklung berücksichtigt die Aspekte der Informationssicherheit und des Datenschutzes im gesamten Entwicklungsprozess, von der Anforderungserfassung bis zur Auslieferung und dem Betrieb der Softwarelösungen. Regulatorische Anforderungen sowie die Anforderungen unserer Kunden und aktuelle "Best Practices" werden bei der Konzeption und Programmierung berücksichtigt und durch entsprechendes Qualitätsmanagement verifiziert. Die Entwicklungsumgebungen werden vor unberechtigtem Zugriff geschützt und die Integrität der zu liefernden Softwarelösungen wird gewährleistet.
Die KISTERS-Mitarbeiter nehmen regelmäßig an Schulungen zur Informationssicherheit und zum Informationsschutz sowie zur korrekten Nutzung von IT-Diensten und den damit verbundenen Sicherheitsmaßnahmen teil.

6.2 Datenschutz

Der Umgang mit personenbezogenen Daten erfolgt nach den Grundsätzen der Transparenz, der Erforderlichkeit der verarbeiteten Daten, der Datenvermeidung und der Datenminimierung. Die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten erfolgt grundsätzlich nur, soweit dies für die Aufnahme, Durchführung oder Beendigung der Geschäftstätigkeit von KISTERS erforderlich ist. Personenbezogene Daten werden nur im Rahmen der Zweckbestimmung verarbeitet oder genutzt, die den Betroffenen bekannt ist. Eine Änderung oder Erweiterung der Zweckbestimmung erfolgt nur, wenn sie gesetzlich zulässig ist, die Betroffenen darüber informiert wurden und die Betroffenen eingewilligt haben.

6.3 Business Continuity – Geschäftsfortführung

Um die Ziele des Business Continuity Management zu erreichen, werden die Geschäftsprozesse, Dienstleistungen und Vermögenswerte analysiert, ihre Kritikalität für die Organisation eingestuft und die kritischen Ressourcen, die sie unterstützen, identifiziert. Ziel ist es, Maßnahmen zur Notfallprävention und -reaktion festzulegen und entsprechende Ressourcen bereitzustellen, die angemessen und wirtschaftlich machbar sind. Bei der Bewertung sind die einschlägigen Anforderungen und Auflagen, wie gesetzliche, vertragliche oder behördliche Anforderungen, zu berücksichtigen.
Als allgemeine Strategie ist die Durchführung proaktiver Maßnahmen zu bevorzugen, soweit dies möglich und wirtschaftlich vertretbar ist, um die Wahrscheinlichkeit und/oder die Auswirkungen von Notfällen so weit wie möglich zu verringern. Da sich das Eintreten eines Notfalls jedoch nicht völlig ausschließen lässt, müssen angemessene Pläne für Notfallmaßnahmen vorhanden sein.
Eine Analyse der Auswirkungen auf den Betrieb (Business Impact Analysis, BIA) muss Informationen über kritische Geschäftsprozesse und Ressourcen liefern. Für diese kritischen Prozesse und Ressourcen sind die Auswirkungen eines teilweisen oder vollständigen Verlusts oder Ausfalls in Abhängigkeit von der Zeit zu bewerten. Die BIA wird für jeden Bereich, der von Interesse ist, einzeln durchgeführt. Bei der Bewertung sind auch die Abhängigkeiten zwischen den ermittelten Bereichen sowie die Abhängigkeiten von externen Lieferanten und Dienstleistern zu berücksichtigen.
Anhand der Analyse sind Notfallwiederherstellungsziele festzulegen, zu denen das Ziel für die Wiederherstellungszeit (RTO), das Ziel für den Wiederherstellungspunkt (RPO) und die Mindestmenge an Ersatzressourcen (Personal, Informationen, Infrastruktur und Dienstleister) gehören, die während eines Notfalls verfügbar sein müssen, um das erforderliche Wiederherstellungsniveau zu erreichen.
Es wird eine BCM-Risikoanalyse (BCM-RA) für alle identifizierten Ressourcen kritischer Prozesse durchgeführt, um die Möglichkeit der Umsetzung von Präventivmaßnahmen zu bestimmen und eine Anleitung für deren Priorität zu geben.
Auf der Grundlage der Ergebnisse von BIA und BCM-RA werden mögliche Strategien und Lösungen zur Unterstützung der Geschäftsfortführung entwickelt. Daraus werden Strategien und Lösungen ausgewählt, deren Umsetzung in Business Continuity Plans (BCP) und Emergency Procedures (EP) entwickelt und beschrieben wird.

7 Kontinuierliche Verbesserung

Zur kontinuierlichen Verbesserung der Informationssicherheit, des Datenschutzes und der Geschäftsfortführung wird das gesamte ISMS regelmäßig auf Aktualität und Wirksamkeit überprüft. Hierbei sind interne

und externe Änderungen und Weiterentwicklungen zu berücksichtigen, unter anderem bei Kundenanforderungen, bei regulatorischen Anforderungen, bei Bedrohungslagen, durch die geopolitischen Situation oder den Klimawandel, beim Stand der Technik oder bei der internen Organisation der KISTERS Gruppe. Außerdem sind die getroffenen Maßnahmen regelmäßig daraufhin zu überprüfen, ob sie den betroffenen Mitarbeitern bekannt sind, ob sie praktikabel sind und ob in den Betriebsablauf integriert werden können. Durch eine kontinuierliche Überprüfung der Regelungen und deren Einhaltung soll das gewünschte Niveau der Informationssicherheit, des Datenschutzes und der Geschäftsfortführung hergestellt werden. Zu diesem Zweck werden interne und externe Audits, einschließlich Sicherheitstests und Übungen zum Notfallmanagement und zu Wiederherstellungsverfahren, durchgeführt. Die Ergebnisse der Überprüfungen und Audits werden genutzt, um Möglichkeiten für weitere Verbesserungen der Informationssicherheit, des Datenschutzes und der Fortführung des Geschäftsbetriebs zu ermitteln.

8 Verpflichtung und Inkrafttreten

Alle Mitarbeiter der KISTERS-Gruppe sind verpflichtet, aktiv zur Informationssicherheit, zum Datenschutz und zum Betriebskontinuitätsmanagement beizutragen und die entsprechenden Richtlinien einzuhalten. Grob fahrlässige und vorsätzliche Verstöße gegen die Richtlinien durch Mitarbeiter oder Dritte werden im Rahmen der gesetzlichen Möglichkeiten verfolgt und geahndet.

Diese Revision der Leitlinie wurde vom Vorstand der KISTERS AG verabschiedet und tritt am Tag nach ihrer Veröffentlichung in Kraft.

Aachen, den 01. Okt. 2024

Klaus Kisters, Vorstand, KISTERS AG

9 Dokumenthistorie

Dieses Dokument wird mindestens einmal jährlich auf Aktualität geprüft und ggfs. angepasst. Die offizielle Version dieses Dokuments wird online verwaltet. Vor der Verwendung von elektronischen Kopien oder gedruckten Versionen sind diese auf Aktualität zu überprüfen.

Version	Datum	Editor*in	Aktion
4.1	2024-10-01	Klaus Kisters	Prüfung und Freigabe
4.1	2024-10-01	H.-J. Schlebusch	Kleine redaktionelle Änderungen
4.0	2023-08-29	Klaus Kisters	Review and Release
4.0	2023-08-29	H.-J. Schlebusch	Weitgehende Überarbeitung zur Zusammenführung von IS- and BCM-Leitlinie
3.6	2022-07-18	Klaus Kisters	Prüfung und Freigabe
3.6	2022-07-18	H.-J. Schlebusch	Expliziter Verweis auf KRITIS, Fehlerkorrekturen
3.5	2021-07-30	Klaus Kisters	Prüfung und Freigabe
3.5	2021-07-30	H.-J. Schlebusch	Redaktionelle Änderungen und Fehlerkorrekturen
3.4	2020-08-25	Klaus Kisters, H.-J. Schlebusch	Prüfung und Freigabe ohne Änderungen
3.3	2019-07-29	Klaus Kisters	Prüfung und Freigabe
3.3	2019-07-29	H.-J. Schlebusch	Geschäftsbereich „Umweltinformatik“ entfernt
3.2	2019-02-19	Klaus Kisters	Prüfung und Freigabe
3.2	2019-02-14	H.-J. Schlebusch	Ergänzungen zur Softwareentwicklung
3.1	2018-05-20	Klaus Kisters	Prüfung und Freigabe
3.1	2018-05-10	H.-J. Schlebusch	Fehlerkorrekturen
3.0	2018-03-20	Klaus Kisters	Prüfung und Freigabe
3.0	2018-01-31	H.-J. Schlebusch	Weitgehende Überarbeitung unter besonderer Berücksichtigung des Schutzes personenbezogener Daten
2.0	2016-11-04	Klaus Kisters	Prüfung und Freigabe
2.0	2016-09-15	H.-J. Schlebusch	Erweiterungen und Anpassungen: KISTERS AG -> KISTERS Group; IT-Sicherheit -> Informationssicherheit
1.0	2015-09-01	Klaus Kisters	Prüfung und Freigabe
1.0	2015-08-21	Klaus Kisters H.-J. Schlebusch	Erstellung