Leitlinie zur Informationssicherheit

3st kommunikation GmbH
Version 2.1 / 30.09.2024

Leitlinie zur Informationssicherheit (V. 2.1 / 2024)

Version:	2.1
Datum der Version:	30.09.2024
Erstellt durch:	3st kommunikation GmbH
Genehmigt durch:	Geschäftsführung
Vertraulichkeitsstufe:	öffentlich

Änderungs-Historie

Datum	Version	Erstellt durch	Beschreibung der Änderung
31.03.2021	0.1	DataGuard	Grundstruktur des Dokuments
13.07.2021	1.0	3st	Ergänzung Verantwortlichkeiten, textliche Anpassungen
01.11.2021	1.1	3st	Überführung PDF (zur internen und externen Kommunikation)
26.10.2023	1.2	3st	Überprüfung, Anpassungen (u.a. neuer ISB, TISAX)
24.09.2024	2.0	3st	Geringfügige Anpassungen (Organisationsstruktur, Verantwortlichkeiten)
30.09.2024	2.1	3st	Ergänzung 4.1 Zielvorgaben: Klimawandel

Vorwort

Die Sicherheit von Informationen wird angesichts zunehmender Anforderungen und Risiken zu einem kritischen Faktor für den Erfolg unserer Kunden und unserer Agentur. Daher haben wir für 3st ein Informationssicherheits-Managementsystem (ISMS) entwickelt und implementiert, das die Aufgabe hat, in einem ständigen Verbesserungsprozess einen auf allen Ebenen sicheren Umgang mit Informationen zu schaffen, aufrecht zu erhalten und kontinuierlich zu verbessern. Seit 2023 sind wir zudem nach den Vorgaben des Bundesverbandes der Automobilindustrie (VDA ISA) mit einem TISAX-Label für die Informationssicherheit auditiert.

Hierfür sind klare Verantwortlichkeiten für die Informationssicherheit definiert und notwendige Ressourcen (Personal und Budget) bereitgestellt. In unserer Agentur sind die Geschäftsführer IT und HR gemeinsam mit unserem externen Informationssicherheitsbeauftragten (ISB) zentrale Ansprechpartner für alle Fragen zum Thema Informationssicherheit und initiieren, planen, überwachen und steuern alle Tätigkeiten in diesem Bereich. Sie unterstützen die Fachbereiche, ihre Prozesse konform zu den Vorgaben zur Informationssicherheit zu gestalten.

Diese Leitlinie zur Informationssicherheit ist dabei zentral für den gesamten Informationssicherheitsprozess und wird auf das gesamte ISMS angewendet. 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 in der Agentur ausgerollt werden. Die Zusammenarbeit zwischen Geschäftsleitung, Fachbereichen und ISB ermöglicht eine praxisnahe, wirksame und gelebte Informationssicherheit.

Informationssicherheit ist ein wichtiger Bestandteil zur Sicherung des Erfolgs unserer Agentur und hat einen entsprechend hohen Stellenwert. Alle unsere Mitarbeiter*innen sind angehalten, die Vorgaben und Leitlinien zur Informationssicherheit zu beachten und einzuhalten.

1. Unternehmen und Geschäftszweck

3st kommunikation ist eine Agentur für Digital, Branding und Content mit Sitz in Mainz. Zu unseren Leistungen gehört die konzeptionelle Entwicklung und kreative Umsetzung von Websites, Corporate Brands, CSR- und Geschäftsberichten sowie Content-Produkten für nationale und internationale Kunden vom Mittelständler bis zum DAX-Konzern aus verschiedensten Branchen. Unsere Agentur ist gegliedert in die Fachbereiche Digital (UX-Design, Development), Kreation (Design), Content (Redaktion, Film), Media Design, Projektmanagement und Verwaltung (People & Culture, Office Management, Buchhaltung).

2. Geltungs- und Anwendungsbereich

Unsere Kunden erwarten von uns neben der Entwicklung kreativer und hochwertiger Kommunikationslösungen auch den Nachweis der Qualität und Sicherheit unserer internen Systeme und Prozesse. Die vorliegende Informationssicherheitsleitlinie adressiert dieses Anforderung im Hinblick auf die Sicherheit der Informationsverarbeitung innerhalb unserer Agentur. Sie gilt somit für das gesamte Unternehmen – Anwender dieser Leitlinie sind alle Mitarbeiter*innen, sowie relevante externe Parteien (Dienstleister, Partner).

3. Informationssicherheit: Grundbegriffe

4. Organisation der Informationssicherheit

4.1 Zielvorgaben und Messung/Überprüfung
Die übergeordneten Zielvorgaben unseres Informationssicherheits-Managementsystems sind:

- Erfüllung aller vertraglichen und gesetzlichen Verpflichtungen (→ Compliance),
- Verringerung wirtschaftlicher Risiken und Schäden (→ Risikomanagement),
- Sicherstellung der Aufrechterhaltung des Betriebes im Falle von eingetretenen Vorfällen (→ BCM),
- Erhöhung unserer Qualität durch standardisierte Prozesse im Umgang mit Informationen,
- Verringerung unseres Impacts auf den Klimawandel durch geeignete Nachhaltigkeitsmaßnahmen,
- Wettbewerbsvorteile durch ausgewiesene und zertifizierte Informationssicherheit,
- Verbesserung unserer Reputation und des Vertrauens aller Stakeholder in unsere Agentur.

Diese Ziele stimmen mit unseren Geschäftszielen und unserer Strategie überein. Die Geschäftsführung ist für die Überprüfung der übergeordneten Zielvorgaben und die Definition neuer Zielvorgaben verantwortlich.

Ziele für Sicherheitsmaßnahmen werden vom Informationssicherheitsbeauftragen (ISB) vorgeschlagen und von der Geschäftsführung im Rahmen der → *Erklärung zur Anwendbarkeit / EzASoA* genehmigt.

Alle Zielvorgaben müssen mindestens einmal jährlich im Rahmen der Managementprüfung (Management Review) überprüft werden. Die effektive Einhaltung der Zielvorgaben durch das ISMS bzw. deren Anpassung für die Folgeperiode ist durch die Geschäftsführung zu dokumentieren. Zur Auswertung des ISMS hinsichtlich Wirksamkeit und Angemessenheit werden im Rahmen des jährlichen Management Reviews geeignete KPIs definiert, gemessen und ausgewertet.

Der Geschäftsführer HR ist dafür verantwortlich, dass mindestens einmal jährlich die Erfüllung der letzten Zielvorgaben bewertet und anschließend an die Geschäftsführung in Form einer Vorlage für die Managementprüfung berichtet wird.

4.2 Anforderungen und Ziele der Informationssicherheit

Ziel ist es, den Zweck der Agentur mit der Informationssicherheit in Einklang zu bringen – d.h. einerseits die strategischen und wirtschaftlichen Ziele und andererseits den besonderen Schutz von Informationen sicherzustellen, die im Rahmen der Projekte der Agentur behandelt werden (Geschäftsberichte, Branding-Projekte, Web-Projekte etc.).

Dazu hat die Agentur ein umfassendes ISMS etabliert und 2021 erfolgreich nach ISO/IEC 27001 auditiert und zertifiziert, sowie 2023 nach den Vorgaben des Bundesverbandes der Automobilindustrie (VDA ISA) das TISAX-Label für die Informationssicherheit auditiert. Das langfristige Ziel unseres ISMS ist die kontinuierliche Verbesserung im Hinblick auf die Awareness aller Beteiligten sowie auf die Wirksamkeit, Eignung und Angemessenheit im Bezug auf die definierten Ziele und Kennzahlen (KPIs).

Diese Richtlinie 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 maßgeblich sind. Ein Verzeichnis aller vertraglichen und rechtlichen Anforderungen (→ Compliance) wird zu diesem Zweck regelmäßig geprüft und aktualisiert.

4.3 Maßnahmen zur Informationssicherheit / Risikomanagement

Unsere Kunden stellen an uns als Agentur für Unternehmenskommunikation besondere Anforderungen an die Integrität, Kontinuität und Verfügbarkeit von Informationen. Der Geschäftserfolg unseres Unternehmens ist in hohem Maße davon abhängig, dass wir bestehende oder neue Risiken für unsere Informationssicherheit erkennen und bewerten, durch geeignete Sicherheitsmaßnahmen vermeiden bzw. mindern und verbleibende Risiken geeignet behandeln.

Dazu haben wir eine → *Methodik zur Risikoeinschätzung und Risikobehandlung* erstellt, die den Prozess bei der Auswahl von Maßnahmen definiert, sowie eine umfassende Risikoanalyse erstellt. Der Geschäftsführer IT ist dafür verantwortlich, mindestens einmal jährlich die → *Risikoanalyse* zu überprüfen und ggf. anzupassen, die Umsetzung der Maßnahmen zu messen und zu bewerten, und die Ergebnisse anschließend an die Geschäftsführung in Form einer Vorlage für die Managementprüfung zu berichten.

Die gewählten Maßnahmen und deren Umsetzungsstatus sind in der Richtlinie → *Erklärung zur Anwendbarkeit (EzA / SoA)* in der jeweils aktuellen Fassung aufgeführt.

4.4 Betriebliches Kontinuitätsmanagement

Das betriebliche Kontinuitätsmanagement (BCM) dient der Aufrechterhaltung bzw. Wiederherstellung des regulären Geschäftsbetriebs. Die dafür erforderlichen Prozesse und Maßnahmen sind in der → *Richtlinie für betriebliches Kontinuitätsmanagement* festgelegt.

4.5 Verantwortlichkeiten

Folgendes sind die grundsätzlichen Verantwortlichkeiten für das ISMS:

Der externe Informationssicherheitsbeauftragte (ISB) ist für die Koordination des ISMS verantwortlich, sowie für die Überprüfung und Berichterstattung über dessen Leistungsfähigkeit und Wirksamkeit.

Die internen Informationssicherheitskoordinatoren (ISK, Alex Knaub und Florian Heine) sind der interne Brückenkopf zum externen ISB hinsichtlich der Meldung, Einstufung und Bearbeitung von Informationssicherheitsereignissen und/oder -vorfällen. Stellen sicher, dass der externen ISB in alle Themen eingebunden wird, welche einen Bezug zur Informationssicherheit aufzeigen.

Der Geschäftsführer HR ist für den Betrieb des ISMS in Abstimmung mit dem ISB verantwortlich, sowie für die Bereiche physische Sicherheit, Personalsicherheit, Compliance, Lieferantenbeziehungen, Datenschutz und BCM/Notfallmanagement.

Der Geschäftsführer IT stellt gemeinsam mit den IT-Administratoren die IT-Prozesse zur technischen und organisatorischen Umsetzung des ISMS bereit und ist für die Behandlung von Sicherheitsvorfällen sowie

für die Ausgabe und/oder Freigabe von Zugängen, Kommunikationswegen, Passwörtern und jeglicher Hardware verantwortlich.

Die Gesamtgeschäftsführung stellt sicher, dass das ISMS entsprechend dieser Richtlinie umgesetzt wird und alle notwendigen Ressourcen verfügbar sind. Sie überprüft das ISMS mindestens einmal jährlich im Management Review bzw. immer im Falle von erheblichen Änderungen und erstellt ein Protokoll dazu. Zweck des Management Reviews ist der Nachweis der Angemessenheit, Eignung und Wirksamkeit des ISMS.

Die Führungsebene (Creative Direction, Teamleads) unterstützt bei der Awareness ihrer Teammitglieder hinsichtlich der geeigneten Klassifizierung und Behandlung von Informationen in unseren Projekten sowie bei Sicherheitsvorfällen und in Krisen- oder Notfallsituationen.

Administration & PM / New Business ist für die Verwaltung der Verträge mit Kunden und Dienstleistern / Lieferanten und deren Bewertung hinsichtlich Risikomanagement und Informationssicherheit verantwortlich

People & Culture ist für die Umsetzung der Informationssicherheit, des Datenschutzes sowie der Compliance-Richtlinien in der gesamten Personalarbeit verantwortlich. P&C ist zudem für die Planung und Durchführung von ISMS-, DSGVO und Compliance-Trainings und Awareness aller Mitarbeitenden hinsichtlich dieser Themenbereiche zuständig.

IT-Administration ist für die rasche Behandlung von Sicherheitsvorfällen (per Ticketsystem Gitlab), die umgehende Meldung an die GF und im Falle datenschutzrechtlicher Relevanz an den DSB verantwortlich. Dabei sind zudem etwaige vertragliche Pflichten gegenüber Kunden sowie gesetzliche Pflichten gegenüber Behörden (Datenschutz) zu berücksichtigen

Die Mitarbeiter*innen sind für den Schutz der Integrität, Vertraulichkeit und Verfügbarkeit derjenigen Informationswerte verantwortlich, deren Eigentümer sie sind. Vorfälle melden sie unverzüglich an die IT-Admin.

4.6 Leitlinien-Kommunikation
Der Geschäftsführer HR stellt sicher, dass alle Mitarbeiter*innen von 3st, sowie relevante externe Parteien (Dienstleister, Partner) mit dieser Leitlinie vertraut sind.

5. Unterstützung der ISMS Umsetzung

Die Geschäftsführung erklärt, dass die Aufrechterhaltung des ISMS und dessen kontinuierliche Weiterverbesserung mit geeigneten Ressourcen (Personal und Budget) unterstützt werden, um alle in dieser Leitlinie genannten Zielvorgaben zu erfüllen.

Dieses Dokument ist gültig ab 24.09.2024. Der Eigentümer dieses Dokuments ist der Geschäftsführer HR, der das Dokument mindestens einmal jährlich prüfen und gegebenenfalls aktualisieren muss.

Informationssicherheitsbeauftragter (ISB): sapite GmbH, Mainz, Marc Schubert, isms@3st.de
Datenschutzbeauftragter (DSB): RMPrivacy GmbH, Mainz, Matthias Rosa, datenschutz@3st.de

Mainz, 24.09.2024
Geschäftsführung
3st kommunikation

Alex Knaub Marcel Teine Thilo Breider Florian Heine