Leitlinie zur Informationssicherheit

3st kommunikation GmbH
Version 1.1 / 01.11.2021

Leitlinie zur Informationssicherheit

Version:	1.1
Datum der Version:	01.11.2021
Erstellt durch:	3st
Genehmigt durch:	Alex Knaub, Florian Heine, Marcel Teine, Thilo Breider
Vertraulichkeitsstufe:	intern

Änderungs-Historie

Datum	Version	Erstellt durch	Beschreibung der Änderung
31.03.2021	0.1	DataGuard	Grundstruktur des Dokuments
13.07.2021	1.0	Florian Heine	Ergänzung Verantwortlichkeiten, textliche Anpassungen
7.10.2021	1.1	FH	Finalisierung
01.11.2021	1.1	FH	Überführung in Indesign / PDF (zur internen / externen Kommunikation)

Vorwort

Informationssicherheit wird angesichts zunehmender Anforderungen und Risiken zum immer wichtigeren Faktor für unseren Agenturerfolg. Daher haben wir in unserer Agentur ein Informationssicherheits-Managementsystem (ISMS) 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.

Hierfür haben wir 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, Fachbereich und ISB ermöglicht eine praxisnahe und gelebte Informationssicherheit.

Informationssicherheit ist ein wichtiger Bestandteil zur Sicherung des Fortbestands 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 integrierte Marken- und Unternehmenskommunikation mit Sitz in Mainz. Zu unseren Leistungen gehört die konzeptionelle Entwicklung und kreative Umsetzung von Websites, Corporate Brands, CSR- und Geschäftsberichten sowie Unternehmensmagazinen für nationale und internationale Kunden vom Mittelständler bis zum DAX-Konzern aus verschiedensten Branchen. Unsere Agentur ist gegliedert in die Bereiche Entwicklung, Kreation, Redaktion/Film, Mediengestaltung und Verwaltung. Die Entwicklung ist für den Betrieb unserer IT verantwortlich.

2. Geltungs- und Anwendungsbereich

Unsere Kunden erwarten neben der Entwicklung kreativer und qualitativ hochwertiger Kommunikationsdienstleistungen auch den Nachweis der Qualität und Sicherheit unserer internen Systeme und Prozesse. Die vorliegende Informationssicherheitsleitlinie adressiert dieses Erfordernis 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. Verwaltung der Informationssicherheit

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

- Erfüllung unserer vertraglichen und gesetzlichen Verpflichtungen (Compliance),
- Verringerung wirtschaftlicher Risiken und Schäden durch (potenzielle) Vorfälle,
- Sicherstellung der Aufrechterhaltung des Betriebes im Falle von eingetretenen Vorfällen,
- Erhöhung unserer Qualität durch standardisierte Prozesse im Umgang mit Informationen,
- Wettbewerbsvorteile durch geprüfte und ausgewiesene Informationssicherheit,
- Verbesserung unseres Images und des Vertrauens 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 sind u.a. folgende KPIs definiert:

1) Awareness / ISMS-Schulung unserer MitarbeiterInnen (Ziel: 90 % bis 31.12.2021)
2) Anzahl der Informationssicherheitsvorfälle mit ungeklärter Ursache (Ziel: <5 bis 09/2022)
3) Risikominimierung (Ziel: Verringerung von 4 Risiken mit Potenzial > 2 bis 09/2022)
4) Reduktion Zugangsrechte-Korrekturen (Ziel: Anzahl nachträglicher Korrekturen im Falle von Änderung oder Beendigung eines Vertrags-/Beschäftigungsverhältnisses < 5 bis 09/2022)
5) Dienstleisterverträge (Anteil Verträge mit ISO-Klauseln an allen Dienstleistern > 20% bis 09/2022)

Der Geschäftsführer HR ist dafür verantwortlich, dass mindestens einmal jährlich die Erfüllung der Zielvorgaben gemessen und 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 der Informationen sicherzustellen, die im Rahmen der Projekte der Agentur behandelt werden (Geschäftsberichte, strategische Branding-Projekte, sensible Web-Projekte etc.).

Dazu etabliert die Agentur ein umfassendes ISMS, kommuniziert dies an alle mit Informationen umgehenden Personen intern (Mitarbeiter*innen) und extern (Kunden, Dienstleister, Partner) und strebt eine Zertifizierung nach ISO/IEC 27001 an.

Nach der Implementierung und Zertifizierung des ISMS ist es das langfristige Ziel, dies im Hinblick auf Awareness aller Beteiligten sowie hinsichtlich der Wirksamkeit, Eignung und Angemessenheit im Bezug auf die definierten Ziele und Kennzahlen (KPIs) kontinuierlich verbessern.

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.

Eine detaillierte Auflistung aller vertraglichen und rechtlichen Anforderungen wird mit der → *Liste der rechtlichen und vertraglichen Verpflichtungen* bereitgestellt, die von Admin & Services verwaltet wird.

4.3 Maßnahmen zur Informationssicherheit
Unsere Kunden stellen an uns als Agentur für Unternehmenskommunikation besondere Anforderungen an die Integrität, Kontinuität und Verfügbarkeit von Informationen. Der Geschäftserfolg unseres Unternehmens ist davon abhängig, dass wir bestehende 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
Betriebliches Kontinuitätsmanagement wird in der → *Richtlinie für betriebliches Kontinuitätsmanagement* festgelegt.

4.5 Verantwortlichkeiten
Folgendes sind die grundsätzlichen Verantwortlichkeiten für das ISMS:

Der Geschäftsführer HR ist für den Betrieb und die Koordination des ISMS verantwortlich, sowie für die Berichterstattung über dessen Leistungsfähigkeit.

Der Geschäftsführer IT stellt die IT-Prozesse zur technischen und organisatorischen Umsetzung des ISMS bereit und ist für die Behandlung von Sicherheitsvorfällen verantwortlich.

Die Geschäftsführung stellt sicher, dass das ISMS entsprechend dieser Richtlinie umgesetzt wird und alle

notwendigen Ressourcen verfügbar sind. Sie definiert, welche ISMS-Informationen mit welchen (internen und externen) interessierten Parteien kommuniziert werden. 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.

Admin & Services ist für die Verwaltung der Verträge mit Kunden und Dienstleistern / Lieferanten und deren Bewertung hinsichtlich Risikomanagement und Informationssicherheit verantwortlich

HR ist für die Umsetzung der Informationssicherheit in der gesamten Personalarbeit, für die Planung und Durchführung von ISMS-Trainings und die Awareness aller Mitarbeiter*innen zuständig.

IT-Administration ist für die rasche Behandlung von Sicherheitsvorfällen (per Ticketsystem Gitlab), die umgehende Meldung an den ISB 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, Verfügbarkeit und Vertraulichkeit derjenigen Informationswerte verantwortlich, deren Eigentümer sie sind. Vorfälle melden sie unverzüglich an die IT-Administration.

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 ISMS-Implementierung und deren kontinuierliche Weiterverbesserung mit geeigneten Ressourcen (Personal und Budget) unterstützt werden, um alle in dieser Leitlinie genannten Zielvorgaben zu erfüllen.

Dieses Dokument ist gültig ab 01.11.2021. Der Eigentümer dieses Dokuments ist der Geschäftsführer HR, der das Dokument mindestens einmal jährlich prüfen und gegebenenfalls aktualisieren muss.

Mainz, 01.11.2021

Alex Knaub Marcel Teine Thilo Breider Florian Heine

Geschäftsführung
3st kommunikation