

Statement of Applicability

des Informationssicherheitsmanagementsystems

finstreet GmbH

Friedrich-Ebert-Straße 113 - 48153 Münster

Datum:

24. Juni 2022

Erstellt durch:

Lutz Bigalke

Klassifikation:

öffentlich

Version:

v3

isms@finstreet.de

Dokumenten Kontrolle

Handhabungshinweise

Klassifikation	öffentlich	Datum
Erstellt durch	Lutz Bigalke	24. Juni 2022
Freigegeben durch	Geschäftsführung	24. Juni 2022
Empfänger	Alle Mitarbeiter und Kunden der finstreet GmbH	

Änderungshistorie

Version	Datum	Geändert durch	Beschreibung der Änderung
v1	28. Januar 2022	Lutz Bigalke	Bewertung 2021
v2	13. Mai 2022	Lutz Bigalke	Review 2022/05
V3	24. Juni 2022	Lutz Bigalke	Review 2022/06, Auswahlgrund adaptiert.

A.5 Informationssicherheitsrichtlinien		
A.5.1	Vorgaben der Leitung für Informationssicherheit	Keine Ausschlüsse enthalten
A.6 Organisation der Informationssicherheit		
A.6.1	Interne Organisation	Keine Ausschlüsse enthalten
A.6.2	Mobilgeräte und Telearbeit	Keine Ausschlüsse enthalten
A.7 Personalsicherheit		
A.7.1	Vor der Beschäftigung	Keine Ausschlüsse enthalten
A.7.2	Während der Beschäftigung	Keine Ausschlüsse enthalten
A.7.3	Beendigung und Änderung der Beschäftigung	Keine Ausschlüsse enthalten
A.8 Verwaltung der Werte		
A.8.1	Verantwortlichkeit der Werte	Keine Ausschlüsse enthalten
A.8.2	Informationsklassifizierung	Keine Ausschlüsse enthalten
A.8.3	Handhabung von Datenträgern	Keine Ausschlüsse enthalten
A.9 Zugangssteuerung		
A.9.1	Geschäftsanforderungen an die Zugangsdaten	Keine Ausschlüsse enthalten
A.9.2	Benutzerzugangsverwaltung	Keine Ausschlüsse enthalten
A.9.3	Benutzerverantwortlichkeiten	Keine Ausschlüsse enthalten
A.9.4	Zugangssteuerung für Systeme und Anwendungen	Keine Ausschlüsse enthalten
A.10 Kryptographie		
A.10.1	Kryptographische Maßnahmen	Keine Ausschlüsse enthalten
A.11 Physische- und umgebungsbezogene Sicherheit		
A.11.1	Sicherheitsbereiche	Keine Ausschlüsse enthalten
A.11.2	Geräte und Betriebsmittel	Keine Ausschlüsse enthalten
A.12 Betriebssicherheit		
A.12.1	Betriebsabläufe und -verantwortlichkeiten	Keine Ausschlüsse enthalten

A.12.2	Schutz vor Schadsoftware	Keine Ausschlüsse enthalten
A.12.3	Datensicherung	Keine Ausschlüsse enthalten
A.12.4	Protokollierung und Überwachung	Keine Ausschlüsse enthalten
A.12.5	Steuerung von Software im Betrieb	Keine Ausschlüsse enthalten
A.12.6	Handhabung technischer Schwachstellen	Keine Ausschlüsse enthalten
A.12.7	Audit von Informationssystemen	Keine Ausschlüsse enthalten

A.13 Kommunikationssicherheit

A.13.1	Netzwerksicherheitsmanagement	Keine Ausschlüsse enthalten
A.13.2	Informationsübertragung	Keine Ausschlüsse enthalten

A.14 Anschaffung, Entwicklung und Instandhaltung von Systemen

A.14.1	Sicherheitsanforderungen an Informationssysteme	Keine Ausschlüsse enthalten
A.14.2	Sicherheit in Entwicklungs- und Unterstützungsprozessen	Keine Ausschlüsse enthalten
A.14.3	Testdaten	Keine Ausschlüsse enthalten

A.15 Lieferantenbeziehungen

A.15.1	Informationssicherheit in Lieferantenbeziehungen	Keine Ausschlüsse enthalten
A.15.2	Steuerung der Dienstleistungserbringung von Lieferanten	Keine Ausschlüsse enthalten

A.16 Handhabung von Informationssicherheitsvorfällen

A.16.1	Handhabung von Informationssicherheitsvorfällen und Verbesserungen	Keine Ausschlüsse enthalten
--------	--	-----------------------------

A.17 Sammeln von Beweismaterial

A.17.1	Aufrechterhaltung der Informationssicherheit	Keine Ausschlüsse enthalten
A.17.2	Redundanzen	Keine Ausschlüsse enthalten

A.18 Compliance

A.18.1	Einhaltung gesetzlicher und vertraglicher Anforderungen	Keine Ausschlüsse enthalten
A.18.2	Überprüfung der Informationssicherheit	Keine Ausschlüsse enthalten