



netzkontor nord
Weil das Ergebnis zählt

**„Breitbandnetz-Ausbau ohne § 109 TKG
ist wie fahren ohne Führerschein!“**

Sicherheitskonzept

Sicherheitskonzepte nach § 109 TKG

Breitbandnetze bieten dem Betreiber zahlreiche Möglichkeiten neue Geschäftsfelder für sich zu erschließen. Zugleich unterliegt deren Betrieb jedoch auch der Einhaltung diverser Regularien. Der § 109 TKG nimmt „Diensteanbieter, Betreiber von öffentlichen Telekommunikationsnetzen und Erbringer von öffentlich zugänglichen Telekommunikationsdiensten“ in die Pflicht. Dabei geht es um die wichtigen Themen Datenschutz, Wahrung des Fernmeldegeheimnisses sowie Gewährleistung der Verfügbarkeit der Dienste. Konkret muss der Netzbetreiber entsprechend dem „Katalog von Sicherheitsanforderungen für das Betrei-

ben von Telekommunikations- und Datenverarbeitungssystemen ...“ ein Sicherheitskonzept erstellen, einführen und der BNetzA zur Genehmigung vorlegen. **netzkontor nord** hat in zahlreichen Projekten erfolgreich Sicherheitskonzepte entwickelt, die in allen Fällen von der BNetzA ohne Probleme genehmigt werden konnten.

Wenn Sie bei der Erstellung, der Aktualisierung oder der Pflege Ihres Konzeptes Unterstützung benötigen, helfen wir Ihnen gerne.

Weil das Ergebnis zählt!



Geringer interner Aufwand!

Garantierte Genehmigung durch BNetzA!

Echte Verbesserung der Sicherheit!

Sicherheit mit  **netzkontor nord**
Weil das Ergebnis zählt

Sicherheitskonzept

Informationssicherheits-Managementsysteme (ISM-Systeme)

In unserer Informationsgesellschaft mit ihrer digitalisierten Arbeitswelt ist die IT längst zum strategisch und wirtschaftlich extrem wichtigen Faktor geworden. Ein längerer Ausfall der IT oder der Verlust von Daten kann für Unternehmen existenzbedrohend sein. Diese Tatsache sowie zahlreiche weitgehende Vorfälle haben die Bundesregierung alarmiert und zum IT-Sicherheitsgesetz veranlasst.

Betroffen von diesem Gesetz sind alle als maßgeblich erkannten Träger der sogenannten **kritischen Infrastrukturen**. Als solche gelten Unternehmen aus den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen. **Ziel ist es, die Unternehmen zu einem systematischen Ansatz zur Gewährleistung ihrer IT-Verfügbarkeit sowie dem Schutz ihrer Daten zu bewegen.**



Damit verbunden ist die Einführung eines Informations-sicherheitsmanagement-Systems (ISM-System). Jedoch sollte auch jeder andere Unternehmer einmal darüber nachdenken, wie wichtig ihm die Sicherheit seiner Daten und die Verfügbarkeit seiner IT-Systeme ist und ob er zu deren Schutz nicht systematisch vorgehen sollte.

Eine ausgezeichnete Basis für den Aufbau eines ISM-Systems bietet der IT-Grundschutz des BSI (Bundesamt für Sicherheit in der Informationstechnik). Dabei handelt es sich um einen anerkannten Standard, um bei Bedarf eine Zertifizierung des ISM-Systems nach DIN 27001 zu erlangen.

Wenn Sie beim Aufbau Ihres ISM-Systems Hilfe benötigen, stehen wir Ihnen gerne zur Verfügung. Wir begleiten Sie auf Wunsch auf Ihrem gesamten Weg vom Sicherheitsaudit (auch Ihrer Lieferanten oder Partnerunternehmen) über den Aufbau Ihres ISM-Systems bis zur Zertifizierung.

Weil das Ergebnis zählt!



**Sicherheitskonzept
gemäß § 109 TKG
- Einleitung -**

- 1. Inhaltverzeichnis
- 2. Einleitung
- 3. Zielsetzung
- 4. Begriffsdefinitionen
- 5. Organisation
- 6. ISM-System
- 7. ISM-System
- 8. ISM-System
- 9. ISM-System
- 10. ISM-System
- 11. ISM-System
- 12. ISM-System
- 13. ISM-System
- 14. ISM-System
- 15. ISM-System
- 16. ISM-System
- 17. ISM-System
- 18. ISM-System
- 19. ISM-System
- 20. ISM-System

SFG	ISG	BSI	Nat.	EG	Mögliche Gefährdungen / Auswirkungen	Erläuterung Gefährdung / Auswirkungen	Schutzmaßnahmen	IS	Maßnahmen	ISG
				EG	Elementare Gefährdung	Keine Relevanz. Eine Gefährdung durch Blitz hat zwar zunächst eine geringe Relevanz, da über das Stromnetz des Kunden durch Blitzschlag relevante Induktionsspannungen entstehen können. Die Relevanz wird aber insgesamt mit 0 bewertet, weil hier maximal nur Einzelstörungen produziert werden können.	Keine Maßnahme erforderlich			
				TS	Technische Störungen, Ausfälle etc.	Keine Relevanz. Hier können maximal Einzelstörungen produziert werden.	Keine Maßnahme erforderlich			
				OG	Organisatorische Gefährdungen und menschliche Fehlerhandlungen, Mängel durch Fehler in der Planung/Realisierung (intern / extern), Anschläge, Vandalismus, weitere strafbare Handlungen	Keine Relevanz. Die Mitarbeiterkonten sind in geschützten Bereichen (Netz) des Endkunden und ist sicherheitstechnisch in dessen Verantwortungsbereich. Damit ist eine detaillierte Sicherheitsanalyse durch den Telekommunikationsanbieter nicht erforderlich.	Keine Maßnahme erforderlich			

Abb.: Sicherheitskonzept



Sie haben Fragen oder Anregungen?

netzkontor nord gmbh
Otto-Hahn-Straße 2
D-24941 Flensburg



Ihr Ansprechpartner:

Herr Jan Ipsen
fon: +49 (0) 461 / 481 600-54
jan.ipsen@netzkontor-nord.de