



UNTERNEHMENSGRUNDSÄTZE

Leitlinie zur Informationssicherheit

Öffentliche Grundsätze zum Schutz von Informationen

Verlässliche IT-Dienstleistungen setzen einen verantwortungsvollen Umgang mit Informationen voraus. Die EMOS Software GmbH beschreibt mit dieser Leitlinie ihre Sicherheitsziele und die Anforderungen, an denen Schutzmaßnahmen und die Zusammenarbeit mit Kunden und Geschäftspartnern auszurichten sind.

In diesem Dokument

Ziele Verantwortung und Zugriffsschutz	2
Sicherheit im Projekt und Weiterentwicklung	3

Herausgeber

EMOS Software GmbH
Lateinschulgasse 15 · 94469 Deggendorf
emos@emos.de · +49 89 54558 119

Geschäftsführer Benjamin Artinger
Amtsgericht Deggendorf · HRB 2776

1 Ziel und Geltungsbereich

Unser Ziel ist es, die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen angemessen zu schützen. Dazu gehören Kundendaten, personenbezogene Daten, Quellcode, Zugangsdaten und interne Geschäftsunterlagen. Die Anforderungen gelten für unsere Tätigkeiten in Beratung, Entwicklung, Testing und IT-Unterstützung sowie für den Umgang mit Informationen bei Kunden und im mobilen Arbeiten.

Der erforderliche Schutz richtet sich nach der Sensibilität der Informationen, möglichen Auswirkungen eines Vorfalls und den geltenden gesetzlichen und vertraglichen Anforderungen. Besondere Sicherheitsanforderungen sind vor Beginn einer Leistung mit dem Kunden abzustimmen.

2 Verantwortung und Risikobewertung

Die Geschäftsführung trägt die Verantwortung für die Sicherheitsziele, die Festlegung von Zuständigkeiten und die Bereitstellung angemessener Ressourcen. Führungskräfte und Projektverantwortliche müssen Sicherheitsanforderungen in Planung und Durchführung berücksichtigen. Alle Mitarbeitenden sind verpflichtet, die für ihre Aufgaben geltenden Schutzregeln einzuhalten.

Risiken sollen bei Einführung und wesentlicher Änderung von Systemen, Verfahren und Dienstleistungen bewertet werden. Schutzmaßnahmen sind am Risiko auszurichten, nachvollziehbar festzulegen und bei neuen Erkenntnissen anzupassen. Verbleibende wesentliche Risiken sind der zuständigen Entscheidungsebene vorzulegen.

3 Vertraulicher und berechtigter Zugriff

Informationen dürfen nur für zulässige und vereinbarte Zwecke genutzt werden. Zugriffe sind auf Personen und Systeme mit entsprechendem Aufgabenbezug zu begrenzen. Berechtigungen müssen bei Aufgabenwechsel und Beendigung einer Tätigkeit angepasst oder entzogen werden.

Authentifizierung, Schutz von Endgeräten, sichere Übertragung und geeignete Verschlüsselung sind entsprechend dem Schutzbedarf vorzusehen. Zugangsdaten und vertrauliche Inhalte dürfen nicht unkontrolliert weitergegeben oder in nicht freigegebene Werkzeuge übernommen werden.

4 Sicherheit im Projekt und im Betrieb

Sicherheitsanforderungen sind möglichst früh in die Entwicklung und Auswahl von IT-Lösungen einzubeziehen. Dazu gehören ein geregelter Umgang mit Softwarekomponenten und Schwachstellen sowie angemessene Prüfungen vor der Bereitstellung. Testdaten und Testumgebungen benötigen einen ihrem Inhalt entsprechenden Schutz.

Für den jeweiligen Leistungsumfang sind geeignete Verfahren zur Aktualisierung, Datensicherung und Wiederherstellung vorzusehen. Zuständigkeiten zwischen EMOS, Kunden und weiteren Dienstleistern sind eindeutig zu vereinbaren. Diese Leitlinie enthält keine pauschale Zusage bestimmter Verfügbarkeiten oder Wiederherstellungszeiten; solche Anforderungen werden leistungsbezogen geregelt.

5 Geschäftspartner und externe Dienste

Bei der Einbindung weiterer Dienstleister sind Schutzbedarf, Zugriffsrechte, Verarbeitungsorte und vertragliche Anforderungen zu berücksichtigen. Externe Cloud- oder KI-Dienste dürfen für vertrauliche Informationen nur nach entsprechender Prüfung und Freigabe eingesetzt werden.

Nachweise und Detailinformationen zu Schutzmaßnahmen werden im Rahmen berechtigter Kundenanfragen und geeigneter Vertraulichkeitsvereinbarungen bereitgestellt. Die öffentliche Leitlinie dient der Darstellung unserer Grundsätze und ersetzt keine projektspezifische Sicherheitsvereinbarung.

6 Sicherheitsvorfälle und Hinweise

Verdachtsfälle und Sicherheitsvorfälle sind unverzüglich an die zuständigen Personen weiterzugeben. Ziel ist es, Auswirkungen zu begrenzen, Ursachen zu klären und geeignete Verbesserungen einzuleiten. Kunden und weitere Stellen sind entsprechend den geltenden gesetzlichen und vertraglichen Anforderungen zu informieren.

Externe Hinweise können zunächst an emos@emos.de oder telefonisch unter +49 89 54558 119 gerichtet werden. Bitte übermitteln Sie dabei keine Passwörter, vollständigen Kundendatensätze oder ausnutzbaren technischen Einzelheiten. Für sensible Informationen ist ein geeigneter Übermittlungsweg abzustimmen. Sicherheitsprüfungen fremder Systeme bedürfen einer gesonderten ausdrücklichen Autorisierung.

7 Sensibilisierung und Weiterentwicklung

Mitarbeitende sollen vor Übernahme entsprechender Aufgaben und danach risikogerecht zu Sicherheitsanforderungen informiert werden. Die Geschäftsführung überprüft diese Leitlinie mindestens jährlich und bei wesentlichen Änderungen. Die Leitlinie beschreibt unsere Anforderungen und begründet keine Aussage über eine vorhandene Zertifizierung.