


Dokumentenbezeichnung Informationssicherheitspolitik			
Dokumententyp Politik	Geltungsbereich PNE	Ablageort ISMS Share Point	Systembereich ISMS
Dokumentnummer PNEID-1373422699-310 V4.0	Klassifizierung Öffentlich	Dokumenteigner ISB	Seite 1/2

Informationssicherheitspolitik

Bedeutung


Die PNE-Gruppe ist international tätig und trägt eine wesentliche Verantwortung für die sichere Energieversorgung der Bevölkerung. Eine zuverlässige Stromerzeugung, -verteilung sowie die Erbringung unterstützender Dienstleistungen sind entscheidend für die Erfüllung unserer Kundenaufträge und für den nachhaltigen Unternehmenserfolg.

Wir erkennen die besondere Verantwortung an, die mit dem Umgang mit Informationssystemen und sensiblen Daten verbunden ist. Ein sicherer, rechtskonformer und verantwortungsbewusster Umgang mit Informationen ist für uns von zentraler Bedeutung.

Diese Informationssicherheitspolitik bildet den übergeordneten Rahmen für alle spezifischen Regelungen und Maßnahmen im Bereich der Informationssicherheit. Sie stellt sicher, dass alle Mitarbeitenden ihre Verantwortung kennen und angemessen handeln. Vorstand, Geschäftsführung, Führungskräfte und Mitarbeitende verpflichten sich gleichermaßen, die daraus abgeleiteten Anforderungen umzusetzen und das Informationssicherheitsmanagementsystem (ISMS) fortlaufend zu verbessern.

Grundsätze

1. **Gemeinsames Verständnis der Informationssicherheit**
Informationssicherheit ist integraler Bestandteil aller Geschäftsprozesse und wird in allen Unternehmensbereichen gelebt.
2. **Strategische Bedeutung**
Risiken im Zusammenhang mit Informationsverarbeitung und IT-Systemen sind bekannt. Informationssicherheit wird als strategischer Erfolgsfaktor aktiv gesteuert.
3. **Ganzheitlicher Ansatz**
Informationssicherheit umfasst technische, organisatorische, infrastrukturelle und personelle Maßnahmen. Sicheres Handeln ist Aufgabe aller Mitarbeitenden.
4. **Schutzziele**
Wir verpflichten uns zur Sicherstellung von:
 - **Verfügbarkeit** von Informationen und Systemen,
 - **Integrität** von Daten und Prozessen,
 - **Vertraulichkeit** sensibler Informationen.
5. **Kontinuierliche Verbesserung**
Das ISMS wird regelmäßig überprüft, bewertet und nach dem Plan-Do-Check-Act-Prinzip weiterentwickelt.

Dokumentenbezeichnung Informationssicherheitspolitik			
Dokumententyp Politik	Geltungsbereich PNE	Ablageort ISMS Share Point	Systembereich ISMS
Dokumentnummer PNEID-1373422699-310 V4.0	Klassifizierung Öffentlich	Dokumenteigner ISB	Seite 2/2

Fördernde Maßnahmen

Verantwortung auf Vorstandsebene

Die strategische Steuerung und Überwachung der Informationssicherheit erfolgt durch den Vorstand bzw. die Geschäftsführung. Informationssicherheit ist regelmäßiger Bestandteil der Managementagenda.

Operative Verantwortung

Der Informationssicherheitsbeauftragte (ISB) trägt gemeinsam mit der Unternehmensleitung die operative Verantwortung. Er koordiniert alle sicherheitsrelevanten Aktivitäten und berichtet regelmäßig an die Leitung.

Risikobasierter Ansatz

Risiken werden systematisch identifiziert, bewertet und behandelt. Angesichts unserer Verantwortung für die Versorgungssicherheit können bestimmte Risiken nicht dauerhaft akzeptiert oder ausschließlich versichert werden.

Dienstliche vs. private IT-Nutzung

Die Trennung privater und dienstlicher Hard- und Software ist verpflichtend. Ausnahmen sind nur in definierten Sonderfällen zulässig.

Sensibilisierung und Schulungen

Alle Mitarbeitenden erhalten regelmäßige verpflichtende Schulungen sowie vertiefende Trainings bei sicherheitsrelevanten Aufgaben. Ziel ist eine gelebte Sicherheitskultur.

Informationssicherheitsmanagementsystem (ISMS)

Das ISMS bildet die Grundlage zur Umsetzung aller technischen, organisatorischen und strukturellen Sicherheitsmaßnahmen.

Sicherheitsorganisation

Rollen, Verantwortlichkeiten und Entscheidungswege sind klar definiert und im Unternehmen kommuniziert.

Melde- und Eskalationswege

Sicherheitsvorfälle, Schwachstellen und verdächtige Aktivitäten sind unverzüglich über die vorgesehenen Kanäle zu melden. Das Verfahren gewährleistet eine zeitnahe Analyse und Bearbeitung.

Interne Audits und Schwachstellenanalysen

Regelmäßige Audits und Analysen dienen der Überprüfung der Wirksamkeit der Sicherheitsmaßnahmen und der kontinuierlichen Verbesserung des ISMS.