ISO/IEC 9001 : 2015 14001 : 2015 27001 : 2013	**Informationssicherheitspolitik**	fischer elektronik kühlen schützen verbinden

Die Informationssicherheit ist für uns von elementarer Bedeutung. Sie leistet einen wesentlichen Beitrag zur vertrauensvollen Zusammenarbeit mit unseren Geschäftspartnern sowie allen interessierten Parteien und hilft, den fortwährenden Unternehmenserfolg zu sichern.

Allen Mitarbeiterinnen und Mitarbeitern ist unabdingbar die Notwendigkeit bewusst, die täglichen Aufgaben im Sinne der Informationssicherheit durchzuführen. Um dies sicherzustellen, findet die kontinuierliche Sensibilisierung und Qualifikation aller Mitarbeiterinnen und Mitarbeiter statt.

Hierzu wurden von der Geschäftsleitung folgende Compliance-Leitsätze erstellt, die sich an den Vorgaben für ein Informationssicherheitsmanagementsystem (ISMS) nach DIN EN ISO 27001:2013 ausrichten:

Leitsatz 1: Verantwortung

Die Geschäftsleitung unterstützt die Aufrechterhaltung des ISMS. Mitarbeiter wurden sensibilisiert, mögliche Verbesserungen oder Schwachstellen unverzüglich zu melden.

Leitsatz 2: Vertraulichkeit

Sämtliche Informationen, die nicht öffentlich sind, werden vor unbefugtem Zugriff durch Autorisierung geschützt.

Leitsatz 3: Integrität

Informationen werden so behandelt, dass sie stets vollständig und unverändert zur Verfügung stehen.

Das Senden und Empfangen von Informationen kann von niemand geleugnet oder bestritten werden. (Verbindlichkeit)

Zugang zu Informationen und dem nichtöffentlichen Bereich der Organisation erhalten nur diejenigen Personen oder Entitäten, deren Identität oder andere Eigenschaften sowie deren berechtigtes Interesse zweifelsfrei nachgewiesen wurden. (Authentizität)

Leitsatz 4: Verfügbarkeit

Die Informations- und IT-Systeme werden so betrieben, dass den anfordernden interessierten Parteien Informationen und Funktionen immer zum geforderten Zeitpunkt zur Verfügung stehen.

Leitsatz 5: Fortlaufende Verbesserung

Das ISMS wird mindestens einmal jährlich auf seine Aktualität und Wirksamkeit geprüft. Maßnahmen werden daraufhin untersucht, ob sie den betroffenen Mitarbeitern bekannt, umsetzbar und in den Betriebsablauf integrierbar sind.

Leitsatz 6: Umgang mit Abweichungen

Abweichungen werden mit dem Ziel analysiert, das ISMS zu verbessern und ständig auf dem aktuellen Stand der IT-Sicherheitstechnik zu halten.