Inhaltsverzeichnis

1 Einleitung

Diese Sicherheitsleitlinie soll allen Mitarbeitern, Vertragspartnern und Lieferanten dabei helfen, die drei wichtigen Ziele unseres Informationsmanagementsystems einzuhalten:

Sicherstellung der Vertraulichkeit, Verfügbarkeit und Integrität aller wichtigen Informationen

Die Einhaltung dieser Sicherheitsleitlinie ist von elementarer Wichtigkeit für alle Geschäftsprozesse bei der IAT mbH. Die Geschäftsleitung erwartet deshalb, dass diese Grundsätze zum Informationsschutz und die daraus abgeleiteten Standards und Richtlinien beachtet werden. Die Geschäftsleitung überprüft regelmäßig die Einhaltung dieser Sicherheitsleitlinie.

2 Geltungsbereich

Diese Sicherheitsleitlinie gilt für den Bereich Technische Berechnung, Softwareentwicklung, Konstruktion und Produktion innerhalb der IAT mbH mit dem Standort Berlin und Stuttgart.

3 Stellenwert der IT-Sicherheit und Bedeutung der IT für die Aufgabenerfüllung

Im Rahmen von Entwicklungsprojekten werden vertrauliche Daten im Unternehmen verteilt und mit unseren Vertragspartnern ausgetauscht. Um die Vertraulichkeit, Verfügbarkeit und Integrität der Daten zu gewährleisten, stellt die Geschäftsleitung dem IT-Managementteam finanzielle Mittel zur Verfügung.

4 Sicherheitsziele und Sicherheitsstrategie

Der gesamte IT-Verbund wird so geschützt, dass:

- die Vertraulichkeit in angemessener Weise gewahrt ist,
- die Integrität des gesamten IT-Verbunds sichergestellt ist, was bei Bedarf verfügbar ist
- die Beteiligung an einem sicherheitsrelevanten IT-Vorgang nicht geleugnet werden kann (Verbindlichkeit),
- das Risikoprioritätszahl (RPZ) von 200 nicht überschritten wird,
- es gesetzliche, vertragliche und aufsichtsrechtliche Verpflichtungen erfüllen kann.

Es ist erforderlich, dass:

- der jeweils für den IT-Verbund geltende Sicherheits- und Kontrollumfang am jeweiligen Betriebsrisiko ausgerichtet ist,
- für alle Teile des gesamten IT-Verbunds (Rechner, Daten und Verfahren) namentlich Systemverantwortliche ernannt werden,
- die einzelnen Nutzer für die sachgerechte Nutzung des IT-Verbunds verantwortlich sind,
- durch Erzeugung zusätzlicher Informationen und durch zusätzliche Verfahren die Nachvollziehbarkeit sämtlicher sicherheitsrelevanter IT-Vorgänge gewährleistet ist.

Die Sicherheitsstrategie basiert auf folgenden Prinzipien:

- Risikoeinschätzung,
- jährliches Managementreview,
- interne Audits,
- Schulung der Mitarbeiter,
- Betrieb von Server-Systemen nur in eingeschränkt zugänglichen Räumen,
- Einsatz verschlüsselter Übertragungs- und Speicherverfahren, soweit technisch realisierbar und soweit eine Vertraulichkeit der Inhalte gegeben ist,
- Tägliche Sicherung der Daten,
- Räumliche Trennung von Daten-Servern und Backup-Systemen.
- Beschränkung von Zugriffsrechten auf die für die Aufgabenerfüllung notwendigen Rechte,
- sichere Konfiguration der IT-Systeme durch Beschränkung der installierten Software und aktivierten Dienste auf die für die Funktion der Systeme benötigten Komponenten,
- sichere Konfiguration der IT-Systeme durch zeitnahe Implementierung sicherheitsrelevanter Software-Korrekturen,
- Strukturierung des Netzes entsprechend der benötigen Sicherheitsniveaus und Unterbindung aller nicht notwendigen Zugriffsmöglichkeiten auf IT-Systeme.

5 Verantwortlichkeiten und Organisationsstruktur

Die Gesamtverantwortung für die Sicherheit des gesamten IT-Verbunds hat die Geschäftsleitung.

Das IT-Sicherheitsmanagement-Team ist verantwortlich für:

- die Erstellung, Überprüfung, Entwicklung, Fortschreibung und Veröffentlichung der IT-Sicherheitsleitlinie,
- Veranlassung und/oder Durchführung von Einweisungen und Schulungen in die IT-Sicherheit,
- die Veröffentlichung, Information und Sensibilisierung der Mitarbeiter

6 Umsetzung

Die IT-Sicherheitsleitlinie sowie deren Umsetzung wird in regelmäßigen Abständen durch das IT-Sicherheitsmanagement-Team der IAT in Zusammenarbeit mit den zuständigen Abteilungen unter Berücksichtigung aktueller Gegebenheiten überprüft und aktualisiert.

Sämtliche Mitarbeiter werden regelmäßig über die Sicherheitsleitlinie, deren Umsetzung und eventuelle Aktualisierungen informiert und ggf. eingewiesen.

Die Kenntnisnahme der IT-Sicherheitsleitlinie wird von allen Beschäftigten durch eine Erklärung für die Personalakte bestätigt.

Die Umsetzung der IT-Sicherheitsleitlinie wird konkretisiert durch die Sicherheitsrichtlinien. Diese regeln die interne Benutzung der IT-Strukturen durch die Mitarbeiter, deren Beachtung Voraussetzung für einen störungsfreien und sicheren Betrieb der IT-Anlage ist, einschließlich der Vorgehensweise bei Verstößen und damit verbundener disziplinarischer Konsequenzen.

Ergänzende Sicherheitsleit- und Richtlinien werden durch das IT-Sicherheitsmanagement-Team erstellt und laufend aktualisiert.

Der Erfolg des ISMS wird laufend durch das IT-Sicherheitsteam kontrolliert, das Ergebnis dieser laufenden Kontrollen wird an die Geschäftsleitung berichtet. Sollte sich abzeichnen, dass das ISMS nicht erfolgreich funktioniert, wird die Geschäftsleitung unmittelbar Maßnahmen einleiten, die den Erfolg des ISMS sicherstellt.