Ingenieurgesellschaft für Automobiltechnik mbH

SICHERHEITSLEITLINIE

Einleitung

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

Sicherstellung der Vertraulichkeit, Verfügbarkeit und Integrität aller wichtigen Informationen.

Die Einhaltung dieser Sicherheitsleitlinie ist von elementarer Wichtigkeit für alle Geschäftsprozesse bei IAT. 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.

Geltungsbereich

Diese Sicherheitsleitlinie gilt für den Bereich Technische Berechnung und Softwareentwicklung innerhalb der IAT.

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 QIS-Team alle erforderlichen Ressourcen zur Verfügung.

Sicherheitsziele und Sicherheitsstrategie

Das gesamte IT-System bei IAT wird so geschützt, dass:

- die Vertraulichkeit in angemessener Weise gewahrt ist,
- die Integrität der IT-Systeme sichergestellt ist,
- die IT-Systeme bei Bedarf verfügbar sind,
- die Beteiligung an einem sicherheitsrelevanten IT-Vorgang nicht geleugnet werden kann (Verbindlichkeit),
- das Risiko regelmäßig analysiert und verringert wird,
- es gesetzliche, vertragliche und aufsichtsrechtliche Verpflichtungen erfüllen kann.

Es ist erforderlich, dass:

- der jeweils für das IT-System geltende Sicherheits- und Kontrollumfang am jeweiligen Betriebsrisiko ausgerichtet ist,
- für alle Teile des gesamten IT-Systems (Rechner, Daten und Verfahren) namentlich Systemverantwortliche ernannt werden,
- die einzelnen Nutzer für die sachgerechte Nutzung des IT-Systems 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.

Verantwortlichkeiten und Organisationsstruktur

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

Das QIS-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

Umsetzung

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

Sämtliche Mitarbeiter werden regelmäßig über die Sicherheitsleitlinie, deren Umsetzung und eventuelle Aktualisierungen informiert und ggf. eingewiesen. Die Einhaltung der Sicherheitsleitlinie ist für alle Mitarbeiter verpflichtend. Die Nichtbeachtung hat disziplinarische und rechtliche Konsequenzen.

Die Umsetzung der Sicherheitsleitlinie wird konkretisiert durch die Richtlinien. Diese regeln die interne Benutzung der IT-Strukturen durch die Mitarbeiter, einschließlich der Vorgehensweise bei Verstößen und damit verbundener disziplinarischer Konsequenzen.

Ergänzende Richtlinien werden durch das QIS-Team erstellt und laufend aktualisiert.

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