Leitlinie zur Gewährleistung der IT-Sicherheit in der F1 GmbH
(IT- Sicherheitsleitlinie)

0. Präambel
Für die F1 GmbH sind die Unversehrtheit, die Verfügbarkeit und die Vertraulichkeit von Informationen von größter Bedeutung. Maßgaben zur Informationssicherheit sind nicht nur gesetzlich vorgeschrieben, sondern werden auch durch die Anforderungen beim Zusammenwirken mit den Geschäftspartnern bestimmt. Jeder Mitarbeiter der F1 GmbH muss daher sein Handeln nach diesen Maßgaben und den daraus abgeleiteten Anforderungen und Richtlinien ausrichten.
Die Geschäftsführung der F1 GmbH ist sich der Bedeutung der IT-Sicherheit für die Aufrechterhaltung, Effektivität und Rechtmäßigkeit der Geschäftsprozesse bewusst.
Sie nimmt deshalb zielgerichtet Einfluss auf Umsetzung und Durchsetzung von IT-Sicherheit im Unternehmen. Zu diesem Zwecke stellt sie diese *LEITLINIE ZUR GEWÄHRLEISTUNG DER IT-SICHERHEIT IN DER F1 GMBH* als Handlungsanweisung auf.
Jeder Mitarbeiter ist verantwortlich für die IT-Sicherheit in seinem Bereich. Er hat geeignete Maßnahmen im Sinne der IT-Sicherheitsleitlinie zu treffen, um die Verfügbarkeit der eingesetzten Systeme und die Integrität der Informationen zu sichern. Bei übergreifenden vernetzten Systemen hat er zudem die Unterstützung des zentralen IT-Sicherheitsmanagements zu gewährleisten.
Die Geschäftsführung steuert die Risiken, die sich beim Einsatz von Informationstechnik ergeben, bewusst. Optionen zur Behandlung der Risiken sind die Ergreifung geeigneter Maßnahmen zur Verminderung der Risiken, die bewusste und objektive Akzeptanz der Risiken und ggf. die Übertragung der Risiken auf Dienstleister. Bei der Erarbeitung von Richtlinien zum Risikomanagement bzw. zum Qualitätsmanagement sind die Regelungen der IT-Sicherheitsleitlinie zu berücksichtigen.

1. Gegenstand und Geltungsbereich
Die IT-Sicherheitsleitlinie dient der Gewährleistung der IT-Sicherheit in der F1 GmbH.
Die IT-Sicherheitsleitlinie beschreibt den Aufbau und den Betrieb eines zentral koordinierten, übergreifenden Informationssicherheitsmanagementsystems (ISMS) mit dessen Hilfe die Erfüllung der IT-Sicherheitsziele zu gewährleisten sind.
Durch die IT-Sicherheitsleitlinie soll sichergestellt werden, dass der Bedeutung der jeweiligen Schutzziele angemessene Sicherheitsmaßnahmen ergriffen werden, um Informationswerte und personenbezogene Daten angemessen zu schützen und um die Verfügbarkeit von informationstechnischen bzw. kommunikationstechnischen Verfahren zu gewährleisten.
Die Geschäftsleitung setzt einen IT-Sicherheitsmanager im Unternehmen ein. In Zusammenarbeit mit diesem wird ein PDCA-Prozess etabliert, der die Durchsetzung und Aufrechterhaltung der IT-Sicherheit auf Basis dieser Leitlinie in einem kontinuierlichen Verbesserungsprozeß gewährleistet.
Durch Anwendung geeigneter Awareness-Maßnahmen sichert die Unternehmensleitung in diesem Prozess die kontinuierliche Fortbildung der Mitarbeiter und die Ausrichtung von deren Handlungsweise auf die Aufrechterhaltung der IT-Sicherheit innerhalb des Geschäftsfeldes.
Die IT-Sicherheitsleitlinie ist Bestandteil eines hierarchisch abgestuften Regelwerks. Die IT-Sicherheitsleitlinie beinhaltet die strategischen Vorgaben der Geschäftsleitung und ist das übergeordnete Regelwerk für IT-Sicherheitskonzepte in den einzelnen Geschäftsfeldern.

Innerhalb der F1 GmbH erstreckt sich der Geltungsbereich über
- den Sitz in Neuenhagen und
- die Niederlassung in Berlin

und über die Geschäftsfelder
- IT-Sicherheitstechnologien
- Programmierung
- Technologieberatung

2. Mitgeltende Unterlagen

- BGB,HGB
- Bundesdatenschutzgesetz
- Telekommunikationsgesetz, Telemediengesetz, Fernmeldegeheimnis
- GDPU

3. Definitionen

Für die IT-Sicherheitsleitlinie gelten die folgenden Definitionen.

3.1 IT-Sicherheit

IT-Sicherheit im Sinne von Informationssicherheit ist die Sicherung und Aufrechterhaltung der:

- Vertraulichkeit: Gewährleistung des Zugangs und Zugriffs zu IT-Systemen und Informationen ausschließlich durch die dazu Berechtigten,
- Integrität: Sicherstellung der Richtigkeit und Vollständigkeit von Informationen und Verarbeitungsmethoden,
- Verfügbarkeit: Gewährleistung des bedarfsorientierten Zugangs zu Informationen, zugehörigen Werten und Ressourcen für berechtigte Benutzer.

3.2 Informationssicherheitsmanagementsystem (ISMS)

Unter einem ISMS wird der Teil des gesamten Managementsystems verstanden, der auf Basis eines Geschäftsrisikoansatzes die Entwicklung, Implementierung, Durchführung, Überwachung, Überprüfung, Aufrechterhaltung und Verbesserung der IT-Sicherheit abdeckt. Das Managementsystem umfasst dabei Strukturen, Richtlinien, Planungsaktivitäten, Verantwortlichkeiten, Praktiken, Verfahren, Prozesse und Ressourcen der F1 GmbH.
Für die wesentlichen Geschäftsprozesse ist ein Risikomanagement umzusetzen:

- Risikoidentifikation
- Risikoanalyse
- Risikobewertung
- Risikobehandlung

3.3 Informationstechnik (IT)

Informationstechnik (IT) im Sinne der IT-Sicherheitsleitlinie umfasst alle Formen der elektronischen Informationsverarbeitung und Telekommunikation.

3.4 Informationseigentümer

Zu jedem IT-unterstützten Geschäftsprozess und jeder Fachanwendung muss ein Ansprechpartner benannt werden, der als so genannter Informationseigentümer für alle Fragen der Informationsverarbeitung und der Informationssicherheit im Rahmen dieses Geschäftsprozesses verantwortlich ist.
Der Verantwortliche für einen Geschäftsprozess muss als Informationseigentümer sicherstellen, dass die für seinen Geschäftsprozess relevanten IT-Sicherheitsmaßnahmen dem Sicherheits- und Kontrollumfang dem jeweiligen Gefährdungspotential entsprechen.

3.5 Sicherheitsdomänen

IT-Sicherheitsrichtlinien bzw. Sicherheitskonzepte beziehen sich immer auf eine bestimmte Sicherheitsdomäne. Als Sicherheitsdomäne wird dabei ein logisch, organisatorisch zusammengehöriger Bereich mit einheitlichen Sicherheitsanforderungen und/oder einheitlicher Sicherheitsadministration bezeichnet:
In der F1 GmbH werden folgende Sicherheitsdomänen definiert:

- Geschäftsführung (Personal, Vertragswesen, Controlling)
- Einkauf, allg. Querschnittsfunktionen
- Programmierung (Eigenleistungen, Fremdaufträge)
- IKT-Support (In-House, als externer Dienstleister)
- Projektentwicklung, -management,
- Gutachtertätigkeit

4. Ziele der IT-Sicherheit

Allgemeingültige Sicherheitsziele innerhalb der F1 - GmbH sind:

- Zuverlässige Unterstützung der Geschäftsprozesse durch die IT und Sicherstellung der Kontinuität der Arbeitsabläufe innerhalb des Unternehmens,
- Realisierung sicherer und vertrauenswürdiger IT-Verfahren,
- Erhaltung der in Technik, Informationen, Arbeitsprozesse und Wissen investierten Werte,
- Sicherung der hohen, möglicherweise unwiederbringlichen Werte der verarbeiteten Informationen,
- Erhalt bzw. Gewährleistung der aus gesetzlichen Vorgaben resultierenden Anforderungen,
- Gewährleistung des informationellen Selbstbestimmungsrechts des Betroffenen bei der Verarbeitung personenbezogener Daten,
- Reduzierung der im Schadensfall entstehenden Kosten sowie
- Wahrung besonderer Dienstgeheimnisse.

Für jedes Geschäftsfeld können weitere angepasste IT-Sicherheitsziele aufgestellt werden.

5. Grundsätze der Sicherheitspolitik

Bei der Erstellung von IT-Sicherheitsrichtlinien bzw. Sicherheitskonzepten sind folgende Grundsätze zu berücksichtigen.

5.1 Angemessenheit von Sicherheitsmaßnahmen

Ziele und Aufwand von Sicherheitsmaßnahmen werden bestimmt durch die Bedeutung der IT-Prozesse für die jeweiligen Geschäftsvorfälle.
Neben der Beachtung gesetzlich vorgeschriebener Sicherheitsanforderungen müssen sich daraus ergebende Sicherheitsmaßnahmen zugleich auch immer auf Verhältnismäßigkeit der Maßnahmen und Verfahren überprüft werden.
Bei der Auswahl und Umsetzung von Sicherheitsmaßnahmen ist davon auszugehen, dass die Umsetzung der Geschäftsprozesse vorrangig zu behandeln ist und möglichst wenig durch die gewählten Sicherheitsmaßnahmen beeinträchtigt wird.

5.2 Bereitstellung von ausreichenden Ressourcen für die IT-Sicherheit

Zur Erreichung und Aufrechterhaltung eines angemessenen Maßes an IT-Sicherheit sind ausreichende finanzielle, personelle und zeitliche Ressourcen bereitzustellen.
Beim Festlegen des IT-Sicherheitsniveaus und bei der Formulierung konkreter IT-Sicherheitsanforderungen ist darauf zu achten, dass das angestrebte IT-Sicherheitsniveau auch wirtschaftlich sinnvoll ist.
Sollten die gestellten Sicherheitsanforderungen nicht finanzierbar sein, müssen die Sicherheitsanforderungen, aber auch die Geschäftsprozesse und die Art und Weise des IT-Betriebes grundsätzlich überdacht werden.

5.3 Einbindung aller Mitarbeiter in den IT-Sicherheitsprozess

IT-Sicherheit betrifft ohne Ausnahme alle Mitarbeiter. Jeder Einzelne kann durch verantwortungs- und sicherheitsbewusstes Handeln dabei helfen, Schäden zu vermeiden und zum Erfolg beitragen. Sensibilisierung für IT-Sicherheit und fachliche Schulungen der Mitarbeiter sind daher eine Grundvoraussetzung für IT-Sicherheit.
Mitarbeiter müssen über den Sinn von Sicherheitsmaßnahmen aufgeklärt werden.
Dies ist besonders wichtig, wenn sie Komfort- oder Funktionseinbußen zur Folge haben. Die Sicherheitsmaßnahmen sollten für den Anwender transparent und verständlich sein, sofern dadurch kein Sicherheitsrisiko entsteht.

5.4 Informationsklassifizierung und Informationsschutz

Alle Informationen, welche im Rahmen von IT-unterstützten Geschäftsprozessen verarbeitet werden, müssen anhand ihrer Bedeutung für die Geschäftsprozesse klassifiziert werden.

5.5 Sicherheit der Informationssysteme während des Lebenszyklus'
Vor dem erstmaligen Einsatz von informationstechnischen bzw. kommunikationstechnischen Verfahren ist zu prüfen, welche Gefährdungen und Risiken für Geschäftsprozesse sich durch den Einsatz ergeben können. Einschlägige rechtliche Regelungen sind zu berücksichtigen.
Während des Lebenszyklus von Informationssystemen sind Maßnahmen zu treffen, um zu prüfen, ob die ausgewählten Sicherheitsmaßnahmen noch ausreichend sind.

5.6 Bildung von IT-Sicherheitsdomänen
Sicherheitsdomänen sind durch entsprechende technische und organisatorische Maßnahmen abzugrenzen.

6. Rollen und Verantwortlichkeiten

6.1 Informationseigentümer
Der Informationseigentümer ist zuständig für:
- die Festlegung der geschäftlichen Relevanz seiner Informationen und die Schutzbedarfsfeststellung,
- die Sicherstellung, dass Verantwortlichkeiten explizit definiert und Sicherheits- und Kontrollmaßnahmen zur Verwaltung und zum Schutz seiner Informationen implementiert werden.

Der Informationseigentümer muss die Zugänglichkeit auf Informationen sowie den Umfang und die Art der Autorisierung definieren, die im jeweiligen Zugriffsverfahren erforderlich sind. Bei diesen Entscheidungen ist Folgendes zu berücksichtigen:
- die Notwendigkeit, die Informationen entsprechend ihrer geschäftlichen Relevanz zu schützen,
- die Aufbewahrungsvorschriften und mit den Informationen verbundenen rechtlichen Anforderungen und
- inwieweit die für die jeweiligen Geschäftsanforderungen erforderlichen Informationen zugänglich sein müssen.

6.2 Informationsnutzer
Mitarbeiter sind bei der Erstellung, Nutzung und Verwaltung von Informationen verpflichtet, die IT-Sicherheitsleitlinie und die IT-Sicherheitsstandards sowie die weiteren Maßgaben, denen die IT-Sicherheitsleitlinie zu Grunde liegt, einzuhalten.

6.3 Informationstreuhänder
Ein Informationstreuhänder wird durch Servicevertrag (Service Level Agreement, Vollmacht, ...) begründet. Der Informationstreuhänder ist zuständig für die Gewährleistung der Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität der Informationen im vereinbarten Umfang. Der Informationstreuhänder ist verantwortlich, den Informationseigentümer über Risiken zu informieren, die sich aus Kontroll- bzw. Sicherheitsentscheidungen ergeben können.

6.4 IT-Sicherheitsmanager
Der IT-Sicherheitsmanager ist zuständig für die Wahrnehmung aller Belange der IT-Sicherheit. In diesem Sinne erfüllt er auch die Aufgabe als IT-Sicherheitsbeauftragter der F1 GmbH. Die Hauptaufgabe des IT-Sicherheitsmanagers besteht darin, die Geschäftsführung bei der Wahrnehmung ihrer Aufgaben im Hinblick auf die IT-Sicherheit zu beraten, bei deren Umsetzung zu unterstützen und zu kontrollieren. Die Aufgaben des IT-Sicherheitsmanagers umfassen unter anderem:
- Mitwirkung im gesamten IT-Sicherheitsprozess,
- den ressortübergreifenden IT-Sicherheitsprozess zu initiieren und zu begleiten,
- die Umsetzung der IT-Sicherheitsleitlinie zu kontrollieren,
- ressortübergreifende IT-Systemrichtlinien und IT-Sicherheitsstandards zu entwickeln bzw. weiterzuentwickeln,
- einen jährlichen Umsetzungsplan zur IT-Sicherheit zu erarbeiten und die Umsetzung zu überprüfen,

- die Realisierung von IT-Sicherheitsmaßnahmen zu initiieren und zu überprüfen,
- zu überprüfen, ob die in den IT-Systemrichtlinien geplanten Sicherheitsmaßnahmen wie beabsichtigt funktionieren und geeignet und wirksam sind,
- die Umsetzung von IT-Sicherheitsrichtlinien und IT-Sicherheitskonzepten in den Sicherheitsdomänen zu unterstützen,
- der Leitungsebene zu berichten,
- federführend bei der Erstellung von jährlichen IT-Sicherheitsberichten und Umsetzungsplänen zur Information der Geschäftsleitung mitzuwirken,
- sicherheitsrelevante Projekte zu begleiten,
- Sensibilisierungs- und Schulungsmaßnahmen anzuregen. Der IT- Sicherheitsbeauftragte kann ressortweit die Durchführung von Sensibilisierungs- und Schulungsmaßnahmen koordinieren.
- evtl. auftretende sicherheitsrelevante Zwischenfälle festzustellen und zu untersuchen sowie
- interne Auditierung der IT-Sicherheit in der F1 GmbH zur Erkennung von Schwachstellen durchzuführen
- spezifische Methoden und Prozesse für die IT-Sicherheit zu vereinbaren,
- an der Erarbeitung von Vorgaben für Hard- und Software mitzuwirken, die der Gewährleistung oder Verbesserung der IT-Sicherheit von zentral betriebenen Querschnittsverfahren dienen, wie z.B. Firewall-Lösungen, Virenschutzsoftware, Verschlüsselungssoftware oder VPN-Lösungen,
- die Erstellung von Schulungs- und Sensibilisierungsprogrammen für IT-Sicherheit zu unterstützen und Awarenessmaßnahmen zu planen sowie auf ihre Wirksamkeit hin zu überwachen.

Für den nachgeordneten Bereich können auch für einzelne Geschäftsfelder IT-Sicherheitsbeauftragte benannt werden.
Der IT-Sicherheitsmanager ist bei allen neuen Projekten mit IT-Bezug in den jeweiligen Geschäftsfeldern sowie bei der Einführung neuer IT-Anwendungen und IT-Systeme zu beteiligen, um die Beachtung von IT-Sicherheitsaspekten in den verschiedenen Projektphasen zu gewährleisten.
Die fachliche Qualifikation und die Arbeitsfähigkeit des IT- Sicherheitsmanagers in den Geschäftsfeldern wird gewährleistet durch Freistellung im erforderlichen Umfang sowie regelmäßige Fortbildung.

7. Der IT-Sicherheitsprozess in der F1 GmbH

Zur Sicherstellung der Qualität des ISMS ist die Beschreibung des IT-Sicherheitsprozesses durch ein PDCA-Modell mit den Phasen Planen, Durchführen, Überwachen und Optimieren geeignet.

7.1 Planen des ISMS, Umsetzung und Durchführung

Für jede Sicherheitsdomäne wird auf der Grundlage der IT-Sicherheitsleitlinie eine IT-Sicherheitsrichtlinie verabschiedet, die die spezifischen Anforderungen widerspiegelt.
Insbesondere sind für jede Sicherheitsdomäne ein Virenschutzkonzept, ein Datensicherungs- und Archivierungskonzept, ein Notfallvorsorgekonzept, ein Berechtigungskonzept und IT-Sicherheitsregeln für die IT-Nutzung zu erarbeiten.

7.2 Überwachung und Prüfung des ISMS

Die Mitarbeiter sind verpflichtet, alle aufgetretenen Sicherheitsvorfälle, welche die IT-Sicherheit beeinträchtigen könnten, dem IT-Sicherheitsmanager bzw. durch das ISMS zur Meldung zu bringen. Dies umfasst u.a. Virenmeldungen, festgestellte Einbruchsversuche in IT-Systeme, festgestellte IT-Sicherheitslücken, Verlust von Backupmedien mit Systemkonteninformationen und auffällige Aktivitäten auf Firewallsystemen bzw. auf Intrusion Detection Systemen.
Die Geschäftsführung kann sich auf Grundlage der nachgewiesenen Sicherheitsvorfälle jederzeit einen Überblick über die Gefährdungslage verschaffen.
Der IT-Sicherheitsmanager überprüft regelmäßig die Wirksamkeit des ISMS und berichtet planmäßig an die Geschäftsführung (2-mal jährlich). In wichtigen Fällen wird die Geschäftsleitung unverzüglich informiert.

Er kann dazu in allen Geschäftsfeldern Penetrationstests oder angemessene Sicherheits-Audits vorgeben und deren planmäßige Durchführung organisieren.
Der IT-Sicherheitsmanager wertet mit dem betroffenen IT-Sicherheitsbeauftragten die vorgenommenen internen Audits aus und entwickelt mit den IT-Sicherheitsbeauftragten gemeinsam einen Behandlungsplan für die durch das Audit festgestellten Risiken und Gefährdungen.
Die Prozesse, Ergebnisse und Maßnahmen sind unter Anleitung des IT-Sicherheitsmanagers zu dokumentieren.

7.3 Aufrechterhaltung und Verbesserung des ISMS

Zur Aufrechterhaltung und Verbesserung des ISMS werden Hinweise/Vorschläge und Kritiken (H/V/K´s) durch die Mitarbeiterinnen und Mitarbeiter des Unternehmens an den Sicherheitsmanager des Unternehmens herangetragen. Dieser erfasst die H/V/K´s, kategorisiert diese und legt sie der Geschäftsleitung zur Entscheidung vor. Nach der Entscheidung durch die Geschäftsleitung werden die entsprechenden H/V/K´s Bestandteil des ISMS.

8. IT-Sicherheitsstandards

Wesentliche gesetzliche Vorgaben und Standards in Bezug auf IT-Sicherheit sind in der Anlage 1 (IT-Standards) genannt.

9. Durchsetzung

Für die Sicherheitsdomänen wird die Umsetzung der Vorgaben der IT-Sicherheitsleitlinie in ihrer jeweiligen IT-Sicherheitsrichtlinie geregelt. Die in den Sicherheitsdomänen tätigen Mitarbeiter haben diese Anweisungen umzusetzen bzw. die Umsetzung herbei zu führen.
Die IT-Sicherheitsleitlinie wird als ergänzende Arbeitsanweisung zum Arbeitsvertrag gültig, inklusive der arbeitsrechtlichen Folgen von Verstößen.

10. Schlussbestimmungen

Die IT-Sicherheitsleitlinie tritt am 01.02.2010 in Kraft.
Die Aktualität der IT-Sicherheitsrichtlinie wird im Abstand von 2 Jahren hinsichtlich ihrer Aktualität überprüft, wenn nicht zwischenzeitliche Änderungen infolge von neuen Erfordernissen notwendig werden.

Berlin, den 01.02.2010

gez. Silke Schirmer *gez. Bernd Schulz*

Anlage1: IT-Standards (Standards bzw. Standard-Familien)
Familie DIN ISO 2700x
DIN ISO 20000

Glossar

Authentizität	Grundsatz, dass der Empfänger zweifelsfrei sicher sein kann, dass eine Nachricht tatsächlich von dem angeblichen Verfasser geschaffen und nicht gefälscht wurde oder anderweitig durch Dritte verändert worden ist.
Informationen	Daten, die gespeichert oder verwaltet werden auf Systemen oder Medien, in der Infrastruktur oder im Rahmen von Geschäftsabläufen.
Integrität	Vermeidung unberechtigter Änderungen, Erstellung oder Duplizierung von Informationen.
ISMS	Informationssicherheitsmanagementsystem
IT	Informationstechnik
PDCA	Plan – Do – Check - Act (Planen – Durchführen – Kontrollieren - Handeln)
Sicherheit	Schutz von Informationsquellen vor unberechtigten Änderungen, Zerstörungen oder Preisgabe - unabhängig davon, ob sie absichtlich oder unabsichtlich erfolgten.
SPAM	Synonym für unerwünschte, unangeforderte (Massen-)Werbung per E-Mail
Verbindlichkeit	Dieser Grundsatz besagt, dass später nachgewiesen werden kann, dass die an einer Transaktion Beteiligten die Transaktionen tatsächlich autorisiert haben und sie über keinerlei Mittel verfügen, ihre Beteiligung zu bestreiten.
Verfügbarkeit	Vermeidung einer nicht annehmbaren Verzögerung bei der Durchführung eines genehmigten Zugriffs auf Informationen.
Vertraulichkeit	Vermeidung der Offenlegung von Informationen ohne Erlaubnis des Eigentümers.
VPN	Virtual Private Network
WLAN	Wireless Local Area Network