ITSS-B

IT-Sicherheitsstandard des FMG-Konzerns

Einführung & Betrieb von IT-Systemen

V 2.1

	Datum	Organisations-einheit	Name
erstellt	18.09.2017	IT	A. Cmarits
geprüft	25.10.2017	PEGO	C. Reiser
freigegeben	07.11.2017	GFB	Dr. M. Kerkloh, A. Gebbeken, T. Weyer

Gliederung

1 Einleitung

Der IT-Sicherheitsstandard des FMG-Konzerns (ITSS) definiert verbindliche Sicherheits-Mindestvorgaben für die Entwicklung, die Einführung, den Betrieb, die Außerbetriebnahme und die Entsorgung von informationsverarbeitenden Systemen im FMG-Konzern. Bei kritischen Geschäftsprozessen sind gegebenenfalls zusätzliche Maßnahmen zu ergreifen.

Der ITSS ist Bestandteil des FMG Informationssicherheits-Rahmenwerk (IS-Framework), aus dessen Vorgaben Sicherheitskonzepte und -maßnahmen so abgeleitet werden, dass stets ein angemessener Schutz gewährleistet ist.

Der ITSS beschreibt nicht die Umsetzung der Sicherheits-Mindestvorgaben – diese muss jeweils projekt- bzw. bereichsspezifisch erarbeitet werden.

Neben dem vorliegenden „ITSS-B: Einführung & Betrieb von IT-Systemen" existiert ein ergänzender Teil „ITSS-E: Entwicklung von IT-Systemen" als Sicherheitsstandard für Software-Entwicklung.

1.1 Rollen & Verantwortlichkeiten

FMG-Informationssicherheits-Management

Der ITSS wird vom FMG-Informationssicherheits-Management (IS-Management) erarbeitet und in Kraft gesetzt. Er wird im Intranet der FMG veröffentlicht. Der ITSS wird jährlich oder bei Bedarf überprüft und den aktuellen organisatorischen Bedingungen, neuen IT-Entwicklungen und Bedrohungen der Informationssicherheit angepasst.

Die Rollen des IS-Managements der FMG sind in der Informationssicherheitsleitlinie beschrieben.

Auftraggeber und Betreiber

Zusätzliche Rollen innerhalb des ITSS sind die des Auftraggebers und des Betreibers. Mit dem Begriff „Betreiber" sind alle Betreiber (operativer Betrieb) von Informationssystemen gemeint. Mit dem Begriff „Auftraggeber" ist der für ein System Verantwortliche gemeint. Im Sinne des ITSS ist dies der Unternehmensteil, der das System in Auftrag gegeben hat, selbst betreibt oder durch einen „Betreiber" betreiben lässt.

Der Auftraggeber hat dafür zu sorgen, dass die Einhaltung des ITSS durch ihn oder die von ihm beauftragten Betreiber sichergestellt ist. Das beinhaltet, dass die vom Betreiber zu gewährleisteten ITSS-Regelungen vertraglich klar fixiert sind.

Innerhalb des betreffenden Unternehmensteils (Auftraggeber) tragen die personalverantwortlichen Führungskräfte die Verantwortung für die Einhaltung des ITSS.

Informationsverantwortlicher

Der Informationsverantwortliche ist verantwortlich für die Klassifizierung von Informationen in seinem Verantwortungsbereich. Typischerweise gehört er der ersten oder zweiten Führungsebene an oder hat bereichsübergreifende Aufgaben (z. B. Revision, Beihilfe, IS, Arbeitsschutz, Datenschutz). Bei Aufgaben- und Funktionsänderungen passt er die Berechtigungen entsprechend an. Die Verantwortlichkeit zur Klassifizierung von Informationen kann durch ihn auch an andere Mitarbeiter delegiert werden.

1.2 Geltungsbereich

Der ITSS gilt ortsunabhängig für alle Bereiche und Beteiligungsgesellschaften des FMG-Konzerns und ist für alle Auftraggeber sowie deren interne und externe Mitarbeiter, die direkt oder indirekt bei der Entwicklung, der Einführung, dem Betrieb sowie der Außerbetriebnahme und Entsorgung von Anwendungen und informationsverarbeitenden Systemen im FMG-Konzern beteiligt sind, verbindlich.

1.3 Ausnahmeregelung

Abweichungen vom ITSS sind durch den Auftraggeber bzw. durch den Betreiber, soweit vertraglich in seiner Verantwortung, beim FMG IS-Beauftragten mit Angabe von Gründen schriftlich mit dem bereitgestellten Standard-Formular zu melden.

Können einzelne Regeln des ITSS nachweislich technisch nicht realisiert werden (z. B. Virenschutz auf Switches), so haben hierfür keine Meldungen zu erfolgen.

1.4 Überwachung

Die Umsetzung des ITSS wird stichprobenartig durch den FMG IS-Beauftragten überprüft.

2 Vorgaben im Bereich Technologien

2.1 Passwörter

Sicherheitsziel: Kontrolle des Zugriffs auf Systeme und Informationen.

- Es muss erzwungen werden, dass nur sichere Passwörter gewählt werden können und diese zyklisch (Mindestvorgabe 90 Tage) geändert werden müssen.
- Sichere Passwörter bestehen aus mindestens acht Zeichen, die drei der vier folgenden Zeichensätze enthalten:
    1. Kleinbuchstaben
    2. Großbuchstaben
    3. Sonderzeichen
    4. Ziffern
- Passwörter von privilegierten Kennungen (z.B. Administratoren) müssen für Notfälle einem definierten Vertreterkreis zugänglich sein und an einem besonders geschützten Ort aufbewahrt werden.
- Voreingestellte (Default-)Passwörter müssen bei Systemeinführung geändert werden.
- Es muss sichergestellt werden, dass Benutzer bei der ersten Anmeldung das Erstpasswort ändern müssen.
- Ein Passwort- bzw. PIN-Schutz muss auch auf mobilen Geräten etabliert werden.

2.2 Antivirus (AV) und Schutz vor bösartigem Code

Sicherheitsziel: Schutz der Integrität von Software und Informationen vor Schaden durch bösartige Software.

- Auf allen Systemen im IT-Verbund muss ein geeigneter Schutz vor Viren und bösartigem Code implementiert und laufend aktualisiert werden.
- An Übergängen zu anderen IT-Verbünden muss ein dedizierter Virenschutz eingesetzt werden.
- Ausnahmen von obigen Regelungen sind genehmigungsfähig wenn:
    - der Hersteller des IT-Systems oder -Verbunds explizit den Einsatz einer AV-Lösung verbietet oder
    - der Einsatz der AV-Lösung drastische Performance-Einbußen bzw. Instabilitäten erzeugt oder
    - durch sonstige Maßnahmen sichergestellt ist, dass keinerlei Viren auf die Systeme ohne AV-Lösung gelangen können.
- Mindestens einmal pro Monat muss ein Komplett-Scan durchgeführt werden.
- Es muss sichergestellt werden, dass durch infizierte Dateien kein weiterer Schaden verursacht werden kann (Löschen der Dateien; Verschieben in Quarantäne).

2.3 Remote-Zugriffe

Sicherheitsziel: Informationssicherheit beim Einsatz von Mobile Computing und externen Zugriffen auf FMG-IT-Infrastruktur.

- Systeme oder Netze, die für Remote-Zugriffe genutzt werden, müssen gegen unbefugten Zugriff geschützt werden. Sie müssen mit einer sicheren Konfiguration inkl. Virenschutz und sicherer Authentifizierung ausgerüstet werden.
- Remote-Zugriffsverbindungen müssen von Produktionsnetzwerken durch Firewall-Mechanismen getrennt werden.
- Remote-Zugriffe über öffentliche Netze (z.B. Internet) müssen durch den Einsatz eines verschlüsselten VPNs abgesichert werden. Bei einer ISDN-Verbindung mit vordefiniertem Rückruf (predefinied callback) oder einer Verbindung über eine private Standleitung (ISDN, ATM) ist keine VPN-Verschlüsselung notwendig.
- Remote-Zugriffe über Transfernetze müssen generell verschlüsselt werden, es sei denn der Betreiber des Fremd-Netzwerkes betreibt dieses ITSS-konform.
- Die Verbindungsdaten von Remote-Zugriffssitzungen müssen protokolliert werden.
- Die Remote-Zugriffsysteme und das Netz in dem sie sich befinden müssen ITSS konform betrieben werden. Dies beinhaltet insbesondere die Kommunikation mit nicht ITSS-konformen Systemen und Netzen.
- Eine 2-Faktor-Authentifizierung ist zu gewährleisten (z. B durch SecureID-Token oder SmartCards).

2.4 Kryptographische Maßnahmen

Sicherheitsziel: Schutz der Vertraulichkeit, Authentizität und Integrität von Informationen.

- Festplatten von mobilen Geräten wie Notebooks bzw. Datenspeicher von PDAs oder Blackberry auf denen vertrauliche Informationen gespeichert sind, müssen verschlüsselt werden. Dies gilt auch für Datenträger wie z.B. CDs, DVDs, USB-Sticks oder externe Festplatten.

- Vertrauliche oder streng vertrauliche Informationen müssen bei Übertragung in oder durch öffentliche Netze verschlüsselt werden. Hierzu müssen Lösungen verwendet werden, die auf bewährten Normen, Verfahren und Methoden beruhen.
- Kryptographische Maßnahmen dürfen andere IT-Sicherheitsvorkehrungen (z. B. VirenScanner, Content-Filter etc.) nicht unterlaufen.

2.5 Netzwerk

Sicherheitsziel: Sicherheit von Informationen und Diensten in Netzen sowie Schutz der unterstützenden Netzwerk-Infrastruktur. Erhaltung der Sicherheit organisationseigener Geräte zur Informationsverarbeitung und der Informationswerte.

2.5.1 Netzzugriffskontrolle und Schnittstellen

- Es müssen geeignete organisatorische und technische Maßnahmen getroffen werden, die einen unberechtigten Zugriff auf Netzwerke und Schnittstellen verhindern.
- Öffentlich zugängliche Systeme müssen mit Sicherheitsmechanismen ausgestattet werden, die eine Verbindung nur zu erlaubten Systemen zulassen.

2.5.2 Fremdsysteme im internen Netz

- Fremdsysteme dürfen nur über entsprechende Schutzmechanismen (Firewall, Proxy, etc.) an die IT-Systeme der FMG angeschlossen werden.
- Ausnahmen können vom Betreiber des internen Netzes nur genehmigt werden, wenn sichergestellt ist, dass diese Systeme vor Verbindungsaufbau umfassend und aktuell auf Viren und bösartige oder nicht erwünschte Anwendungen überprüft werden und somit keine Gefährdungen für die IT-Systeme der FMG darstellen.
  Eine Prüfung kann erfolgen durch
    - den Betreiber des internen Netzes
    - den Bediener des Fremdsystems, sofern vom Eigentümer vertraglich zugesichert ist, dass das System ITSS-konform betrieben wird

  Die Ausnahmen sind an den Bereichs-IS-Beauftragten zu melden.

2.6 Sicherheit von Server & Arbeitsstationen

Sicherheitsziel: Einschränkung des Risikos von Systemausfällen.

- Informationen über mögliche sicherheits-/verfügbarkeitsrelevante Schwachstellen von IT-Systemen müssen regelmäßig und aktuell beschafft werden und bezüglich des Risikos bewertet werden.
- Wenn im Rahmen der Risikoabschätzung Handlungsbedarf ermittelt wird, müssen entsprechende Maßnahmen zeitnah getestet und implementiert werden. Die Resultate müssen dokumentiert werden.
- Updates und wesentliche Konfigurationsänderungen müssen bei Systemen mit hoher oder sehr hoher Verfügbarkeit vorher in einer geeigneten Testumgebung überprüft werden.
- Der Einsatz von Härtungs-Maßnahmen (z.B. Deaktivierung nicht benötigter Dienste bzw. Entfernung von Berechtigungen) muss pro IT-System bewertet, dokumentiert und die Maßnahmen bei Handlungsbedarf umgesetzt werden. Für Systeme in der DMZ und öffentliche zugängliche Systeme müssen Härtungs-Maßnahmen auf jeden Fall implementiert werden.
- Die Nutzung eines passwortgeschützten Bildschirmschoners muss – soweit technisch möglich – erzwungen werden.
- Es dürfen nur die notwendigen Zugriffsrechte für Benutzer und Endgeräte gewährt werden.
- Protokolle, welche Authentifizierungsinformationen unverschlüsselt übertragen (z. B. r-Dienste, telnet, ftp,) dürfen nicht eingesetzt werden.

2.7 Trennung von Schulungs-, Entwicklungs-, Test- und Produktivsystemen

Sicherheitsziel: Schutz der Produktivsysteme / Verhinderung gegenseitiger Störung.

- Kritische Produktivsysteme müssen gegen Schulungs-, Entwicklungs-, Test- und Demonstrationssysteme durch geeignete Maßnahmen abgesichert werden.

2.8 Freigabe neuer Technologien bezüglich Informationssicherheit

Sicherheitsziel: Schutz vor Sicherheitsrisiken beim Einsatz neuer Technologien.

- Neue IT-Technologien müssen vor Einführung auf sicherheitsrelevante Schwachstellen bezüglich der Regeln des ITSS geprüft und bewertet werden.
- Ihre erstmalige Nutzung muss beim FMG-IS-Beauftragten unter Angabe der Prüfergebnisse beantragt werden. Die Freigabe - bezüglich Informationssicherheit - erfolgt durch den FMG-IS-Beauftragten.

2.9 Physische Sicherheit

Sicherheitsziel: Verhinderung von unberechtigtem Zugang zu Geräten und Informationen bzw. deren Beschädigung, Veränderung oder Verlust.

- Es muss sichergestellt werden, dass der Zutritt zu IT-Systemen und -Räumen nur durch autorisierte Personen erfolgen kann.
- Es muss sichergestellt werden, dass die IT-Systeme unter den geforderten Bedingungen (z.B. Klima, USV, Brandschutz, Staubfreiheit) betrieben werden.
- Es müssen organisatorische und technische Maßnahmen ergriffen werden, um den Diebstahl von Geräten und Informationen zu verhindern.
- Die Aufbewahrung und der Transport von Geräten sowie von Datenträgern und Informationen müssen so organisiert werden, dass diese vor unberechtigtem Zugriff, Missbrauch oder Verfälschung geschützt sind.
- Zentrale Serverkomponenten müssen in den Rechenzentren des Servicebereiches IT betrieben werden.

3 Vorgaben im Bereich Prozesse

3.1 Betriebsverfahren

Sicherheitsziel: Gewährleistung des korrekten und sicheren Betriebs von IT-Systemen.

3.1.1 Systemmanagement

- Der ordnungsgemäße Betrieb der IT-Systeme muss gemäß den Anforderungen an Verfügbarkeit, Vertraulichkeit, Integrität und Authentizität durch geeignete organisatorische und technische Maßnahmen proaktiv sichergestellt werden.
- Mögliche Maßnahmen sind:
    - die zyklische Kontrolle von Logfiles oder der regelmäßige Failover-Test von hochverfügbaren Systemen,
    - Kontrolle von Kapazitätsanforderungen in Bezug auf Verarbeitungsleistung, Durchsatz und Speicherkapazität von IT-Systemen,
    - Überwachung und Bewertung von Systemzuständen (z. B Prozessorlast) und ggf. Einleitung von Maßnahmen.

3.1.2 Management von Änderungen

- Änderungen an IT-Systemen müssen anhand eines definierten Prozesses (z.B. Genehmigung, Test, Freigabe, Überprüfung, Rückfall, etc.) eingebracht und dokumentiert werden.

3.1.3 Management von Vorfällen

- Jeder sicherheitsrelevante Vorfall muss dokumentiert und dem zuständigen Bereichs-IS-Beauftragten gemeldet werden.
- Der Bereichs-IS-Beauftragte muss kritische Informationssicherheitsvorfälle umgehend dem FMG-IS-Beauftragten melden oder dafür sorgen, dass diese gemeldet werden. Informationssicherheitsvorfälle, die mehrere FMG-Bereiche betreffen, müssen immer dem FMG-IS-Beauftragten gemeldet werden.
- Der Bereichs-IS-Beauftragte meldet dem FMG-IS-Beauftragten jährlich im Rahmen des ITSS-Statusberichtes die kritischen und überblicksartig die sonstigen in seinem Bereich aufgetretenen Sicherheitsvorfälle.
- Sicherheitsrelevante Vorfälle müssen analysiert und bewertet werden. Wenn im Rahmen der Bewertung Handlungsbedarf ermittelt wird, müssen entsprechende Maßnahmen ergriffen werden.
- Kritische Sicherheitsvorfälle entsprechen dem Business Impact „hoch“ bzw. „sehr hoch“ (siehe Kapitel 3.7)

3.1.4 Backup, Restore und Archivierung

- Es muss ein Datensicherungskonzept erarbeitet und umgesetzt werden, dass die Anforderungen der Geschäftsprozesse berücksichtigt.
- Die Betriebsfähigkeit des Backup / Restore - inkl. Prüfung der Backup-Logs, regelmäßiger Restore-Tests - muss sichergestellt werden.
- Vor Inbetriebnahme eines Systems muss der Restore getestet werden.

- Backup-Medien müssen in einem gesonderten Brandabschnitt - sicher verwahrt - ausgelagert werden.
- Eine Archivierung muss entsprechend der aktuell gültigen gesetzlichen Regelungen, bzw. entsprechend den Anforderungen der Geschäftsprozesse durchgeführt werden.

3.1.5 Disaster Recovery / Notfallvorsorge

- Für Unglücksfälle in der Informationstechnologie (z. B. Ausfall von Serverräumen durch Brand) müssen für kritische Geschäftsprozesse Pläne zur Aufrechterhaltung oder der angemessenen Wiederherstellung (Notfallpläne) vorhanden sein.
- Die Notfallpläne müssen in regelmäßigen Abständen getestet und an die aktuellen Anforderungen angepasst werden. Die beteiligten Personen müssen regelmäßig geschult werden.
- Ein Notfallplan kann auch eine „manuelle" Rückfallstufe (d. h. ohne Einsatz von IT-Systemen) definieren, z. B. die Verwendung von Betriebsfunk bei Ausfall des Wireless-LAN Netzwerks.

3.1.6 Softwarelizenzen

- Es muss sichergestellt werden, dass für sämtliche eingesetzten Systeme und Anwendungen gültige Softwarelizenzen vorhanden sind.

3.1.7 Dokumentation

- Es muss eine Übersichtsdokumentation für jeden IT-Verbund erstellt und aktuell gehalten werden. Eine Übersichtsdokumentation enthält mindestens:
    - Inventarliste sämtlicher eingesetzter Hard- & Software (inkl. Lizenzmanagement)
    - Netzwerkplan (inkl. Schnittstellen und Datenfluss zu anderen Netzen)
- Für IT-Systeme, die kritische Geschäftsprozesse unterstützen (z.B. produktive Datenbankserver, Firewall, etc.), muss eine zusätzliche Dokumentation vorhanden sein. Diese enthält:
    - Basis-Implementierung inkl. Systembeschreibung
    - Betriebsprozesse inkl. Administrationsbeschreibung
- Die Dokumentation muss die Anforderungen an die Verfügbarkeit, Wiederherstellungszeit und die Qualifikation der zur Verfügung stehenden Mitarbeiter berücksichtigen.

3.2 Zugriffskontrolle und Berechtigungsvergabe

Sicherheitsziel: Verhinderung eines unberechtigten Benutzerzugriffs bzw. unerlaubter Zugriff auf IT-Systeme und Informationen.

- Die Zuteilung und der Widerruf von Zugriffsberechtigungen müssen durch einen formalen Verwaltungsprozess überwacht und dokumentiert werden.
- Nach dem Prinzip der Funktionstrennung müssen Beantragung, Genehmigung und Aktivierung von Zugriffsberechtigungen personell getrennt werden.

- Die Zugriffsberechtigungen müssen in regelmäßigen Abständen, mindestens jährlich oder bei Aufgaben- bzw. Funktionsänderungen (u. a. bei Versetzungen) auf Aktualität und Angemessenheit überprüft werden.
- Bei Kündigung müssen alle Berechtigungen deaktiviert werden.
- Soweit technisch möglich und sofern die Geschäftsprozesse dies zulassen, muss allen Benutzern eine eindeutige Kennung (Benutzer-ID) für ihren persönlichen und alleinigen Gebrauch zugewiesen werden. Bei Gruppenkennungen muss durch organisatorische oder technische Maßnahmen eine Identifikation sichergestellt werden.
- Kennungen dürfen nur mit den Rechten ausgestattet werden, die zur Ausführung der Tätigkeiten notwendig sind (Prinzip der minimal notwendigen Rechte).
- Administrative und Benutzerkonten müssen getrennt werden. Standard-Benutzeraufgaben dürfen nicht unter administrativen Kennungen durchgeführt werden.
- Das Surfen im Internet mit administrativen Rechten ist untersagt.

3.3 Umgang mit klassifizierten Informationen

Sicherheitsziel: Verhinderung eines unberechtigten Zugriffs auf bzw. Missbrauch von vertraulichen Informationen.

- Vertrauliche Informationen, die elektronisch verarbeitet und gespeichert werden, sind durch geeignete organisatorische und technische Maßnahmen vor unberechtigtem Zugriff zu schützen.
- Die entsprechenden Regeln sind zu dokumentieren, die Mitarbeiter zu schulen.
- Für die FMG GmbH sind detaillierte Regelungen in der „Richtlinie zum Umgang mit Informationen unterschiedlicher Vertraulichkeitsklassen“ definiert.

3.4 Öffentlich zugängliche Systeme und Informationen

Sicherheitsziel: Verhinderung von Verlust, Änderung oder Missbrauch von Informationen.

- Bevor Informationen öffentlich bereitgestellt werden, muss deren Veröffentlichung durch den Informationsverantwortlichen genehmigt werden.
- Die Integrität öffentlich zugänglicher Informationen muss durch geeignete Maßnahmen (z. B. Absicherung von Webservern und Applikationen) gegen unberechtigte Veränderungen geschützt werden.

3.5 Protokollierung und Auditing

Sicherheitsziel: Überprüfung, ob die Vorgaben des IS Frameworks, insbesondere des ITSS-B eingehalten werden.

- Die Gesetze und Bestimmungen zum Datenschutz müssen eingehalten werden, insbesondere hinsichtlich der Privatsphäre eines jeden Mitarbeiters (Überwachung, Protokollierung).
- Die gezielte Überprüfung bzw. Überwachung einzelner Mitarbeiter ist verboten. Ausnahmen sind nur in Abstimmung mit Betriebsrat, Datenschutz und dem FMG IS-Beauftragten möglich.
- Überwachungs- und Sicherheitsprotokolle von sicherheitsrelevanten Ereignissen in IT-Systemen müssen ausreichend Informationen zur Verfügung stellen, um eine umfassende Überprüfung der Wirksamkeit und Übereinstimmung mit dem ITSS-B sowie forensische Analysen zu unterstützen.
- Überwachungs- und Sicherheitsprotokolle von IT-Systemen müssen regelmäßig auf auffällige Aktivitäten geprüft werden.
- Es müssen regelmäßige Sicherheitsüberprüfungen durchgeführt und dokumentiert werden, um Sicherheitslücken im System ausfindig zu machen. Wenn im Rahmen der Bewertung der Sicherheitslücken Handlungsbedarf ermittelt wird, müssen entsprechende Maßnahmen ergriffen werden.

ITSS-Statusbericht

- Es muss jährlich pro IT-System ab Schutzbedarf „hoch“ ein Sicherheitsstatusbericht erstellt werden, welcher folgende Punkte beinhaltet:
    - Aktueller Schutzbedarf, ggf. Änderungen
    - Umsetzungsstatus der noch offenen Sicherheitsmaßnahmen aus dem letzten Audit (sofern verfügbar)
    - Maßnahmenplan für zukünftige Sicherheitsmaßnahmen

3.6 Vernichtung von Informationen

Sicherheitsziel: Sichere Vernichtung von Informationen

- Bei Außerbetriebnahme, Entsorgung oder anderer Verwendung von IT-Komponenten muss sichergestellt werden, dass Unbefugte keinen Zugriff auf Informationen erhalten, die auf den IT-Komponenten gespeichert sind.
- Bezüglich der Aussonderung / Vernichtung von unternehmenskritischen Informationen muss bei der FMG GmbH die „Richtlinie zum Umgang mit Informationen unterschiedlicher Vertraulichkeitsklassen“ beachtet werden.

3.7 Schutzbedarfsfeststellung und Risiko-Analyse

Sicherheitsziel: Feststellung des Schutzbedarfes

- Der Schutzbedarf muss durch den Auftraggeber festgestellt werden, die Risikoanalyse wird durch Auftraggeber und Betreiber gemeinsam erarbeitet.
- Schutzbedarf und Risikoanalyse müssen regelmäßig überprüft werden.

3.8 Vorgaben für Outsourcing

Sicherheitsziel: Sicherstellung, dass Dienstleister den Mindestanforderungen der FMG Sicherheitsrichtlinien gerecht werden damit die Sicherheit der IT-Systeme und Informationen aufrecht erhalten wird.

- Fremdfirmen, die IT-Systeme für den FMG-Konzern betreiben, müssen mit dem „Vertrag über Vereinbarungen zum FMG-IT-Sicherheitsstandard und über Vertraulichkeitspflichten" auf die Einhaltung des ITSS verpflichtet werden.
- Der Auftraggeber muss regelmäßig den Dienstleister analog Kapitel 3.5 auf Einhaltung des ITSS-B überprüfen. Dies kann z. B. durch direkte Audits des Auftraggebers oder durch Prüfung von Dokumenten des Dienstleisters erfolgen.

4 Vorgaben für Personal von Betreibern

Sicherheitsziel: Sicherstellen, dass Mitarbeiter von Betreibern über die notwendige Kompetenz verfügen

- Mitarbeiter von Betreibern müssen die nötige Fachkunde zur Ausführung ihrer Tätigkeiten besitzen und müssen gemäß aktuellen technischen Standards im Bereich Informationssicherheit geschult werden.
- Mitarbeiter von Betreibern müssen zum ITSS-B, ITSS-E und anderen relevanten Sicherheitsrichtlinien geschult werden.
- Mitarbeiter von Betreibern müssen vom Betreiber auf das Datengeheimnis nach §5 BDSG verpflichtet sein.

5 Glossar

2-Faktor-Authentifizierung	Sichere Anmeldung durch Besitz und Wissen (ähnlich EC-Karte und PIN)
Angriff	Bewusster oder absichtlicher Versuch, eine Verwundbarkeit in einem System auszunutzen oder zu suchen
Authentifizierung	Überprüfen einer Identität
Authentizität	Überprüfte und bestätigte zweifelsfreie Herkunft bzw. Identität
Autorisierung	Erteilte Berechtigung
Bedrohung	Umstand, der direkt oder indirekt zu einem Schaden oder Sicherheitsverlust führen kann
Besitzer	Ist derjenige, der Zugriff auf Informationen erteilen und widerrufen kann
Betreiber	FMG-interne und externe Anbieter von IT-Dienstleistungen, IT-Diensten, IT-Systemen oder IT-Bestandteilen technischer Systeme, die im Auftrag des FMG-Konzerns Leistungen erbringen
Daten	Gebilde aus Zeichen zur Abbildung von Informationen und Medien (Sprache, Bilder), die gespeichert oder verarbeitet werden
DMZ	Demilitarized Zone (auch ent- oder demilitarisierte Zone) bezeichnet ein Computernetz mit sicherheits-technisch kontrollierten Zugriffmöglichkeiten auf die daran angeschlossenen Server

FMG-IT	Servicebereich für informationstechnische Systeme innerhalb des FMG-Konzerns
FMG-Konzern	FMG, Töchter sowie Beteiligungsgesellschaften
Fremdsysteme	Systeme, die nicht unter der Verwaltung des Betreibers stehen, z. B private PCs, Rechner von Wartungstechnikern oder Beratern etc.
Härtung	Ein gehärtetes System ist so konfiguriert, dass nicht benötigte Dienste bzw. Benutzerkonten deaktiviert oder gelöscht, sonstige Rechte restriktiv gesetzt und straffe Systemrichtlinien aktiviert sind.
Informationen	Im Rahmen von Geschäftsabläufen interpretierte Daten
Integrität	Eigenschaft, dass IT-Systeme und Daten, die genutzt bzw. gespeichert, verarbeitet oder übertragen werden, ausschließlich zulässigen Veränderungen unterlagen
IT	Abkürzung für Informationstechnologie
Informationssicherheit	Fachgebiet, das sich mit der Sicherheit von IT-Prozessen befasst. Informationssicherheit entsteht aus einem sinnvollen Zusammenspiel von technischen und organisatorischen Maßnahmen
IS-Management	Managementaufgabe, die sich mit der Erstellung von Richtlinien, deren Einhaltung und der Erfassung und Minimierung von Risiken befasst
IT-Systeme	Informationstechnische Systeme:

	Mit Informatikmitteln (Computer, Datenbanken, Programmen etc.) realisiertes Informationssystem zur Unterstützung eines Geschäftssystems. Dazu zählen auch proprietäre, IT-basierte Steuerungen für Anlagen (z. B Gepäckförderanlage, Gebäudeleitsystem etc.).
IT-Verbund	Nach BSI-Grundschutz: Als Gesamtheit von infrastrukturellen, organisatorischen, personellen und technischen Komponenten zu verstehen, die der Aufgabenerfüllung in einem bestimmten Anwendungsbereich der Informationsverarbeitung dienen. Ein IT-Verbund kann dabei als Ausprägung die gesamte IT einer Institution oder auch einzelne Bereiche umfassen, die durch organisatorische Strukturen (z. B. Abteilungsnetz) oder gemeinsame IT-Anwendungen (z. B. Personalinformationssystem) gegliedert sind (FMG-spezifisch, z. B Gepäckförderanlage, E-Mail-System).
Kritische Geschäftprozesse	Geschäftprozesse, deren Schutzbedarf „hoch" bzw. „sehr hoch" ist.
Kritische Produktivsysteme	Systeme, die für das Funktionieren kritischer Geschäftsprozesse notwendig sind.
Mobile Geräte	z. B Notebooks, PDAs, Blackberries, SmartPhones etc.
Nachweisbarkeit	Verbindlicher Nachweis, so dass an Veränderungen Beteiligte über keinerlei Mittel verfügen, ihre Beteiligung zu bestreiten
Öffentlich zugängliche Systeme	System, welches öffentlich zugänglich ist, z. B Public WLAN, Internetterminals
Passwort	Zeichenkette, die als Authentifizierungsinformation dient

Projektleiter	Verantwortlicher Mitarbeiter für die Einführung von neuen Systemen bzw. nachträgliche Änderungen. Projektleiter können Anträge auf Abweichung vom ITSS bzw. auf IT-Sicherheitsfreigabe neuer Technologien stellen.
Restrisiko	Risiko, das zwar erkannt, aus technischen, organisatorischen oder finanziellen Gründen nicht, oder nur mit unverhältnismäßigem Aufwand, beseitigt werden kann
Risiko	Möglichkeit, einen Schaden zu erleiden. Im IT-Verbund ergeben sich Risiken aufgrund der Tatsache, dass real existierende Bedrohungen auf Verwundbarkeiten treffen können.
[IT-]Service	Dienstleistung, die mit Hilfe von Informationstechnologie erbracht wird. Im Idealfall sind für IT-Services Qualitätsmerkmale über Service Level Agreements festgelegt.
Sicherheit	Zustand, in dem Schutz vor Gefahr oder Schaden gewährleistet ist
Transfernetz	Externe Verbindungen zu ausgewählten Partnern, die dedizierte private Netzwerke nutzen.
Verfügbarkeit	Gewährleistung der Durchführung genehmigter Zugriffe und Veränderungen auf Daten und Systeme innerhalb einer definierten Zeit
Vertraulichkeit	Gewährleistung, dass nur berechtigten Nutzern der Zugang zu einem definierten Zweck möglich ist
VPN	Virtual Private Network. Ein VPN ist ein Netz, das zum Transport privater Daten ein öffentliches Netzwerk (z.B. das Internet) nutzt. Die Verbindung über das öffentliche Netzwerk muss verschlüsselt werden (z.B. IPSEC, SSL).

Änderungshistorie

Org.-einheit	Bearbeiter	Datum	Änderung	Alte Versionsnr.
ITS	A. Cmarits		Aufteilung des Dokumentes in 3 Varianten: • ISM • Delfin intern • Externe Version	2.02
ITS	A. Cmarits	07.07.2010	• Anlage ITSS-Statusbericht entfernt	2.03
IT	A. Cmarits	18.09.2017	• Anpassung an FMG Layout, • Entfernung Anhang • Erweiterung Abschnitt physischer Schutz	2.04