A1 Security Governance

Standard
für den sicheren Servicebetrieb

Standard für das
A1 Informationssicherheitsmanagement

Für A1 Mitarbeitende:

Der Schutzbedarf wird aus der Serviceklasse und der Vertraulichkeitsklasse errechnet und ist in der SIAM ersichtlich.

Der Schutzbedarf wird automatisch auf mindestens **Erweitert** erhöht, sobald die Verarbeitung **personenbezogener Daten** von EU-Bürgern auf Systemen außerhalb des Geltungsbereichs der EU-Verordnung 2016/679 (DSGVO / GDPR) erfolgt. Das gilt **nicht** für die Verarbeitung von Anmeldedaten.
Als Anmeldedaten gelten folgende Informationen, jeweils auch einzeln:

- eMail-Adresse
- Vorname und/oder Nachname
- IP-Adresse

Für A1 Lieferanten:

Es liegt in der Verantwortung des Lieferanten eine schriftliche Information zu dem von A1 festgelegten Schutzbedarf zu erhalten.
Der Lieferant erklärt sich bereit, alle 36 Monate für ein Sicherheits - Review-Gespräch mit einem A1 Mitarbeitenden zur Verfügung zu stehen.

Die zu erfüllenden Sicherheitsanforderungen für den festgelegten Schutzbedarf sind der folgenden Tabelle zu entnehmen:

Schutzbedarfs-Anforderung	Kapitel 2.1	Kapitel 2.2	Kapitel 2.3
Standard	x	-	-
Erweitert	x	x	-
Hoch	x	x	x

Inhaltsverzeichnis

1 Geltungsbereich & generelle Zielsetzung

Der vorliegende Standard für den sicheren Betrieb von Services und Servicekomponenten richtet sich an Lieferanten und Partner von A1 (nachstehend auch: Auftragnehmer, Supplier, Provider, Dienstleister, Auftragsverarbeiter) sowie alle Mitarbeitenden von A1, die mit dem Betrieb, Wartung und Außerbetriebnahme von IKT-Services betraut sind.

Diese Vorgaben gelten sowohl für innerhalb der A1 IKT-Infrastruktur (On-Premises) betriebene Services, Anwendungen und Plattformen, wie auch für außerhalb der A1 IKT-Infrastruktur betriebene Dienste, Services, (Cloud-) Anwendungen und Plattformen.

Für Fragen und Beratung stehen die in Kapitel 3 aufgelisteten Kontakte zur Verfügung.

2 Sicherheitsanforderungen

In den nachfolgenden Kapiteln sind die Anforderungen gemäß der Schutzbedarfsklassen an Anwendungen und Services, welche A1 Informationen / Daten verarbeiten, beschrieben.

Es gelten die auf den folgenden Seiten definierten Anforderungen gemäß des von A1 festgestellten und dokumentierten Schutzbedarfs.

2.1 Sicherheitsanforderungen an die Schutzbedarfsklasse „Standard“

Alle durch oder im Auftrag von A1 betriebenen Services müssen die Anforderungen an diese Schutzbedarfsklasse „**Standard**“ erfüllen. Services mit dem Schutzbedarf „**Erweitert**“ und „**Hoch**“ unterliegen zusätzlichen Bestimmungen (siehe Kap. Sicherheitsanforderungen an die Schutzbedarfsklasse „Erweitert“ 2.2 ab Seite 8 und für „Hoch“ 2.3 ab Seite 13.).

2.1.1 Vulnerability & Incident Management

- Die eingesetzte Software muss unter Support stehen.
- Schwachstellen müssen gemäß folgender Tabelle behoben werden.
  Alternativ muss ein Risiko im A1 Risk Management angelegt werden.

VULNERABILITIES

Kritikalität	Patching Zeitvorgaben
LOW	6 Monate
MEDIUM	3 Monate
HIGH	1 Monat
CRITICAL	2 Kalenderwochen

- Für die Behebung von Sicherheitsschwachstellen dürfen keine Kosten verrechnet werden.
- Incidents und Data Breaches müssen unverzüglich an das zuständige A1 Service Center gemeldet werden, siehe Kapitel 3.

2.1.2 Netzwerksicherheit

- Network Devices: Endgeräte dürfen sich erst nach erfolgreicher Authentifizierung mit dem A1 Netzwerk („Client Zone") verbinden. Maßgebend für die Authentifizierung der Geräte ist der aktuelle Stand der Technik für den LAN-Zugang. Neue Geräte im internen A1 Netz müssen jedoch IEEE 802.1X unterstützen. Jedes Gerät in den Netzen von A1 muss einzeln identifizierbar sein.

- IoT-Devices dürfen nicht direkt aus dem Internet erreichbar sein. Security-Updates müssen über den ganzen Lebenszyklus automatisiert und ohne manuellen Eingriff eingespielt werden. Es dürfen keine Passwörter in den Devices fest (hardcoded) hinterlegt sein, herstellerseitige Standard-Passwörter müssen bei Erst-Inbetriebnahme geändert werden.

2.1.3 Software-Architektur

- Falls mehrere Mandanten auf demselben Service eingerichtet sind, muss eine saubere Mandantentrennung zu anderen Kundendaten gewährleistet sein.

2.1.4 Verschlüsselung

- Die Daten-Kommunikation zwischen IKT-Systemen von Dritten und den IKT-Systemen von A1 Österreich muss verschlüsselt erfolgen.

2.1.5 Authentifizierungsmethoden

- Benutzende (A1 Team Member) müssen sich mittels SSO (Single Sign-On) gegenüber einem IKT-Service authentifizieren (AD / Kerberos). Falls weniger als 50 Benutzende das Service nutzen oder falls SSO nicht möglich ist, liegt die Benutzerverwaltung in der Verantwortung des zuständigen A1-Team Members.

- Die Benutzerverwaltung (anlegen, löschen, sperren, ändern) durch A1 muss möglich sein.

- Jeder angelegte Benutzende muss in einem zentralen Benutzerverzeichnis geführt werden und der gewählte Ablauf der Authentifizierung durch den A1-Verantwortlichen dokumentiert werden.

- **Passwortschutz:** Die Passwörter dürfen nicht identisch zum A1-Passwort sein, wenn keine Anbindung an das Authentifizierungssystem von A1 (ADFS) vorliegt und müssen die A1-Vorgaben für sichere Passwörter erfüllen:

    - Mindestens 8 Zeichen lang (max. 256)
    - 3 dieser 4 Kriterien erfüllen: Großbuchstaben, Kleinbuchstaben, Zahlen, Sonderzeichen
    - Regelmäßige Passwortwechsel müssen technisch unterstützt werden.
    - Eine Passwortspeicherung und -übertragung im Klartext ist nicht zulässig.

- **Biometrische Authentifizierung:**
  - Bei biometrischer Authentifizierung dürfen die Authentifizierungsdaten ausschließlich lokal und sicher am jeweiligen Gerät gespeichert werden und dürfen nicht mit Standard-Rechten (beispielsweise von der Festplatte) auslesbar sein.
  - Bei Verfahren zur Gesichtserkennung müssen Kriterien wie Dreidimensionalität oder Temperatur mitgeprüft werden.
  - Bei Verfahren zum Fingerabdruck-Scanning müssen Kriterien wie Fingerpuls oder Temperatur mitgeprüft werden.
  - Die Falschakzeptanzrate (unberechtigte User werden autorisiert) muss bei maximal 1 zu 50.000 liegen.
  - Die Falschrückweisungsrate (berechtigter User wird nicht autorisiert) muss in einem akzeptablen Rahmen sein.
  - Um sich bei einer Falschrückweisung trotzdem authentifizieren zu können, muss alternativ ein Passwortschutz gemäß den oberen Angaben möglich sein.
- **Alternative Authentifizierungsmethoden:**
  - Alternative Authentifizierungsmethoden sind zulässig, sofern sie ein gleich- oder höherwertiges Schutzniveau verglichen zu den oben angegebenen Verfahren aufweisen.

2.1.6 Reporting

Mindestens quartalsweise muss ein Reporting vom Provider über die erbrachten Leistungen erfolgen und an den A1 Leistungsempfänger übermittelt werden. Dieser Report muss zumindest folgende Punkte (Keymetrics) beinhalten:

- Verfügbarkeit des Systems kalendermonatlich
- Incident Reaction Time
- Resolution Time kalendermonatlich
- durchgeführte technische Security Maßnahmen
- gefundene Schwachstellen nach CVSS-Klasse
- behobene Schwachstellen
- Behebungszeiten für Schwachstellen

2.1.7 Malwareschutz

Es muss zumindest eine Antivirussoftware im Einsatz sein, welche laufend die Systeme und Dateien auf Schadsoftware überprüft. Die Software muss laufend aktualisiert werden. Schadsoftware muss unverzüglich entfernt werden.

2.2 Sicherheitsanforderungen an die Schutzbedarfsklasse „Erweitert"

Zusätzlich gelten für die Schutzbedarfsklasse „**Erweitert**" neben den Anforderungen an die Schutzbedarfsklasse „**Standard**" (Siehe Kap. 2.1 Seite 5), auch die nachfolgenden Bestimmungen in diesem Kapitel.

IKT-Dienstleister, welche vertrauliche A1 Daten (Schutzbedarf ab „Erweitert") auf eigener Infrastruktur außerhalb des A1 Netzes speichern (Cloud-Anbieter, externes Hosting, XaaS), **müssen** eine gültige ISO 27001 Zertifizierung vorweisen können und für den gesamten Zeitraum der Zusammenarbeit mit A1 für die von A1 bezogenen Leistungen aufrechterhalten.

2.2.1 Formale Kriterien

- Die Rechnerstandorte, an denen A1-Daten gespeichert und verarbeitet werden, müssen gegenüber A1 offengelegt werden.
- Die Daten dürfen nur dann externen A1 Partnern (Auftragsverarbeitern) zugängig gemacht werden, wenn eine Vertraulichkeitsvereinbarung (NDA) und eine Datenschutzvereinbarung (DPA, sofern personenbezogene Daten verarbeitet werden) mit A1 vereinbart und unterzeichnet wurden. Auch für Prototyping, Laboraufbauten und POCs (Proof of Concept) müssen derartige Vereinbarungen unterzeichnet werden, wenn der Zugriff oder Zugang zu / auf A1 Echtdaten erfolgt.
- Alle Änderungen und Implementierungen von A1-Assets oder an von A1 genutzten Applikationen müssen gemäß eines dokumentierten IT-Change-Enabling Prozesses durchgeführt werden.
- Auditrecht: Der A1 Lieferant muss sich im Bedarfsfall nach entsprechender Vorankündigungszeit von A1 auditieren lassen.

2.2.2 Vulnerability & Incident Management

- Für wesentliche Einrichtungen lt. NISG[1] und TKG[2] müssen die Hardening-Vorgaben der CIS-Benchmarks eingehalten werden.
- Vulnerability Scans müssen in regelmäßigen Abständen auf die durch das A1 Service genutzte Infrastruktur durchgeführt werden.
- Relevante Logdateien für forensische Analysen müssen 18 Monate zurückreichend bereitgestellt werden.
- Alle A1 On-Premises Services sowie durch A1 betriebene PaaS & IaaS Cloud-Services müssen an ein SIEM-System von A1 angebunden werden
- Administratoren- und Benutzerverhalten (Log-on, Log-off, Passwortwechsel, relevante Kopiervorgänge, etc.) müssen protokolliert werden. Die Logdateien müssen bei Bedarf für forensische Analysen zur Verfügung gestellt werden.
- Regelmäßige Datensicherungen müssen durchgeführt und deren Wiederherstellbarkeit getestet werden. Zudem müssen die Anforderungen an die Verfügbarkeit in einem Service Level Agreement (SLA) mit A1 vereinbart und eingehalten werden.

2.2.3 Netzwerksicherheit

- Es müssen Sicherheitsmaßnahmen gegen netzbasierte Angriffe (IPS, Firewall) im Einsatz sein.
- Die Netzwerke müssen innerhalb der Netz- und Informationssysteme abhängig vom Schutzbedarf segmentiert werden.
- Die Ownership für Netzwerksegmente muss eindeutig definiert sein.
- Die Sicherheit innerhalb der Netzwerksegmente und der Schnittstellen zwischen den Netzwerksegmenten muss sichergestellt sein.
- Jeder Netzwerkverkehr, der nicht für das Funktionieren der Systeme erforderlich ist, muss verboten sein.

[1] https://www.nis.gv.at/

[2] https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20011678

2.2.4 Secure Coding & Software-Architektur

- Applikationen müssen in mehreren Tiers (Ebenen) aufgebaut sein, die sicher voneinander getrennt sein müssen.
- Beim Zugriff darf kein Tier übersprungen werden.
- Der Zugriff von einem Tier zum Nächsten, darf nur über definierte Protokolle (Ports) erfolgen.
- Es muss eine Trennung in Prä-Produktiv- und Produktivsysteme erfolgen.
- Die Daten auf Prä-Produktiv-Systemen müssen anonymisiert sein.
- Zugriffe auf Produktivsysteme die Echtdaten enthalten, müssen auf einen reduzierten Personenkreis mit dokumentierten Businessneed eingeschränkt werden und das Need-to-know Prinzip sowie Seperation-of-Duties für kritische Aktionen muss gewährleistet sein.

2.2.5 Verschlüsselung

- Vertrauliche und geheime Daten müssen verschlüsselt übertragen werden.
- Wenn die zugrundeliegende IKT-Infrastruktur nicht durch A1 verwaltet wird (Bsp. externes Hosting, Cloud) müssen vertrauliche und geheime Daten verschlüsselt gespeichert werden. Hierzu kann Verschlüsselung auf Dateisystem-, Betriebssystem-, Datenbank- oder Applikationsebene eingesetzt werden.
- Kryptographische Schlüssel müssen in sicherer Umgebung erzeugt, aufbewahrt und archiviert werden.
- State-of-the-Art Verschlüsselung muss eingesetzt werden: AES (Schlüssellänge 128-256 Bit), Camellia (128-256 Bit), ECIES (>250 Bit), DLIES (>3000 Bit), RSA (>3000 Bit)
- Veraltete Verfahren dürfen nicht eingesetzt werden: Triple-DES, Serpent, Twofish, DES, RC4, Blowfish
- Die Netzwerkkommunikation zu Subdienstleistern und zwischen den Rechnerstandorten muss verschlüsselt erfolgen.

2.2.6 Authentifizierungsmethoden

- Der Zugriff auf vertrauliche oder geheime A1 Daten über ungeschützte Netze (Bsp. Internet, Cloud-Services) oder ausgehend von IKT-Infrastruktur von Dritten, welche nicht in der Verwaltung von A1 steht (BYOD, IKT-Ausrüstung des Partners), muss per MFA-Authentifizierung erfolgen.

Passwortschutz:

- Initialpasswörter müssen zufallsbedingt erzeugt werden, verschlüsselt übertragen werden, dürfen nur ein einziges Mal eingesetzt werden und dürfen nur maximal 2 Wochen gültig sein.
- Nach dem Ersteinstieg mittels Initialpassword muss sofort ein Passwortwechsel erzwungen werden. Im Bedarfsfall, beispielsweise nach einem Angriff, muss es möglich sein, die Anmeldeinformation zu ändern.
- Nach 15 fehlgeschlagenen Anmeldeversuchen muss der Zugriff für min. 15 Minuten gesperrt werden oder gleichwertige Methoden zur Verhinderung unberechtigter Zugriffe auslösen.

2.2.7 Physische Sicherheit

- Der physische Zutritt zu Bürogebäuden und Rechnerräumen muss überwacht werden.
- Der Betrieb datenverarbeitender Komponenten muss in zutrittsgeschützten Räumen erfolgen.

2.2.8 Berechtigungsmanagement

- Die regelmäßige Überprüfung von Rollen und Rechten durch den verantwortlichen A1-Mitarbeitenden muss möglich sein und in Intervallen von maximal 12 Monaten erfolgen.
- Für die Autorisierung ist der Standard-Genehmigungsprozess der A1-Benutzerverwaltung anzuwenden.
- Der Dienstleister muss es A1 ermöglichen, Berechtigungen nach A1-internen Anforderungen flexibel vergeben bzw. entziehen zu können. Eine zentrale Auflistung bzw. die Einsicht und eine automatische Auswertung aller Berechtigungen müssen ermöglicht werden.

2.2.9 Deprovisionierung & Datenlöschung

- Zu Vertragsende müssen sämtliche bestehenden Daten an A1 übergeben werden.
- Jeder Lieferant hat die Daten sicher zu löschen, wenn sie nicht mehr zur Erfüllung der vertraglichen Pflichten benötigt werden. Dies kann durch mehrmaliges Überschreiben der Daten, durch die Vernichtung kryptographischen Schlüssel oder zertifizierte Zerstörung der Datenträger erreicht werden.

2.3 Sicherheitsanforderungen an die Schutzbedarfsklasse „Hoch"

Zusätzlich zu den Anforderungen aus den Schutzbedarfsklassen „**Standard**" (Seite 5) und „**Erweitert**" (Seite 8) gelten für Services mit dem Schutzbedarf „**Hoch**" die nachfolgenden Bestimmungen in diesem Kapitel.

2.3.1 Externes Hosting

- Als geheim klassifizierte Daten / Informationen dürfen nur mit einer expliziten Ausnahmegenehmigung durch den A1 local CISO außerhalb der A1 On-Premise IKT-Infrastruktur (Cloud, externes Hosting etc.) gespeichert werden.

2.3.2 Formale Kriterien

- Ein definiertes Vorgehensmodell für das Service Management muss eingehalten werden (beispielsweise COBIT, ITIL, ISO 20.000).
- Backgroundchecks beim eingesetzten Personal (beispielsweise Strafregisterbescheinigung) müssen durchgeführt werden.

2.3.3 Vulnerability & Incident Management

- Alle Services und Dienste müssen an ein SIEM-System von A1 angebunden werden.
- Das Notfallmanagement muss geplant, dokumentiert und aufgesetzt sein.
- Zumindest alle 18 Monate muss der Lieferant Penetration-Tests durchführen, welche die Angreifbarkeit prüfen. Aus den gefundenen Schwachstellen müssen Maßnahmen abgeleitet und umgesetzt werden.

2.3.4 Netzwerksicherheit

- Ein Tool zur automatisierten Denial-of-Service (DoS) - Mitigation wird eingesetzt.
- Alle wichtigen Versorgungskomponenten müssen redundant ausgelegt sein.
- Eine Standortredundanz über mindestens 2 Rechnerstandorte muss gegeben sein.
- Alle Komponenten müssen in ein zentrales Management eingebunden sein.

2.3.5 Secure Coding & Software-Architektur

- Es müssen statische Sourcecode-Analysen zur Vermeidung von Sicherheitsschwachstellen durchgeführt werden.

2.3.6 Verschlüsselung

- Die verwendeten kryptographischen Schlüssel für die Verschlüsselung von gespeicherten Daten („Data-at-rest") müssen unter A1 Kontrolle sein.
- Regelmäßige Schlüsselwechsel müssen technisch unterstützt durchgeführt werden können. Prozesse zum Schlüsselwechsel müssen vorliegen. Schlüsselwechsel müssen beauftragt werden können.
  ODER: Der Schlüssel ist in A1 Hoheit und wird bei A1 generiert.

2.3.7 Continuity Management

- Notfallpläne müssen erstellt, angewendet, regelmäßig bewertet und erprobt werden.

3 Security Service-Center Kontakte

In alphabetischer Reihenfolge:

A1 Austria und A1 Group	**A1 Service Operation Center** T 0800 501 511 T +43 50 664 8 501 511 @ Attacke@A1.at
A1 Belarus	@ cybersecurity@A1.by
A1 Bulgarien	@ security@A1.bg
A1 Digital	**A1 Digital – Information Security** @ security@A1.digital
A1 Kroatien	@ informationsystemssecurity@A1.hr
A1 Mazedonien	@ InfoSec@A1.mk
A1 Serbien	@ security.alerts@A1.rs
A1 Slowenien	@ security.slo@A1.si

4 Publikation & inhaltliche Verantwortung

	Der Inhalt wurde erstellt von: A1 OneSEC (Austria) Security@A1.at

5 Versionshistoire

Version 2.4		
	Erstellung	Freigabe
Name:	Friedrich HEIGL	Alexandra FEHRINGER
Datum:	27.10.2023	28.11.2023
Gültig ab: 01.12.2023		

Changelog:

- allgemein: „IT" durch „IKT" ersetzt
- allgemein: MUSS-Anforderungen klarer formuliert
- allgemein: Checklisten-Tabellen entfernt (zuvor: 2.1.6, 2.2.10, 2.3.8)
- Kapitel 2.1.1 Vulnerability & Incident Management: Schwachstellenmanagement neu formuliert
- Kapitel 2.1.4 Verschlüsselung: neu formuliert, Forderung nach Ansprechpartner gestrichen
- Kapitel 2.1.5 Authentifizierungsmethoden: Passwort-Anforderungen neu formuliert
- Kapitel 2.1.6 Reporting: Kapitel neu eingefügt
- Kapitel 2.1.7 Malwareschutz: Kapitel neu eingefügt
- Kapitel 2.2.1 Formale Kriterien": Text bzgl. Änderungen / Changes gekürzt
- Kapitel 2.2.2 Vulnerability & Incident Management: CIS-Benchmarks als MUSS für wesentliche Einrichtungen gemäß NISG und TKG eingefügt; Aufbewahrungsfrist für Log-Dateien mit 18 Monaten spezifiziert; Backup-Wiederherstellbarkeit muss getestet werden.
- Kapitel 2.2.3 Netzwerksicherheit: Kapitel neu formuliert
- Kapitel 2.2.4 Secure Coding & Software-Architektur: neu formuliert bzgl. Produktiv- vs. Prä-Produktiv-Systemen
- Kapitel 2.2.6 Authentifizierungsmethoden: 2FA durch MFA ersetzt; Passwortschutz: Forderung bzgl. unzulässiger Passwörter gestrichen
- Kapitel 2.2.9 Deprovisionierung & Datenlöschung: Text neu formuliert
- Kapitel 2.3.2 Formale Kriterien: Forderung nach Reporting gelöscht, weil nun bereits in Kapitel 2.1.6 gefordert
- Kapitel 2.3.3 Vulnerability & Incident Management: Forderung nach Backup-Wiederherstellbarkeit gestrichen, weil nun bereits in Kapitel 2.2.2 gefordert
- (ehemaliges) Kapitel 2.3.4 Authentifizierung: Kapitel gestrichen
- Kapitel 2.3.5 Secure Coding & Software-Architektur: Satz bzgl. Sicherheit als Teil des Entwicklungsprozesses gestrichen
- Kapitel 2.3.7 Continuity Management: Kapitel neu eingefügt

Versionshistoire

Version 2.3		
betrifft:	Erstellung	Freigabe
Name:	Friedrich HEIGL	Alexandra FEHRINGER
Datum:	25.11.2022	02.05.2023
Gültig ab: Freigabedatum		
Changelog: - TLP-Bezeichnung von „WHITE" auf „CLEAR" aktualisiert - Text-Teile durch allgemeinere Formulierungen ersetzt (ADSV und Splunk) - „Büros" auf „Bürogebäude" geändert - Anforderung „Ansprechpartner für Sicherheit und Kryptographie" von Schutzbedarf HOCH zu STANDARD verschoben - Kapitel 2.2.8 Berechtigungsmanagement: Information zum Prüf-Intervall hinzugefügt. - Kapitel 2.3.1 Externes Hosting: „A1 CISO" geändert auf „A1 local CISO" - allgemeine Tippfehler Korrekturen - Kapitel 3 3 Security Service-Center Kontakte: Liste der Security Service Center der A1 Gruppe neu eingefügt. - Verweise auf lokale Richtlinien von A1-Österreich entfernt bzw. allgemeingültig formuliert. - Schutzbedarf-Feststellung auf Seite 2 gekürzt. - Hol-Schuld für Lieferanten bzgl. A1-Schutzbedarfsklassifizierung eingetragen. - Schutzbedarfs-Ankreuzfelder entfernt - Hinweis auf die Ablage im Intranet entfernt, da für Lieferanten nicht erreichbar. - Rückfragen-Kontakt von Security@A1.at auf die Kontakt-Liste in Kapitel 3 geändert. - Kapitel 2.2.1 Formale Kriterien: Verweis auf Greenlight entfernt. - Kapitel 2.2.4 Secure Coding & Software-Architektur: statt Verweis auf OWASP Top10 nun allgemeinere Formulierung		

Version 2.2		
betrifft:	Erstellung	Freigabe
Name:	Friedrich HEIGL Information Security	Alexandra FEHRINGER Leitung Information Security
Datum	25.01.2022	25.01.2022
Gültig ab: Freigabedatum		
Changelog: Dokumenthistorie eingefügt Hinweise bzgl. Schutzbedarfserhöhung eingefügt Telefon-Nummer des SOC korrigiert eMail-Adressen korrigiert Kapitel 2 gestrichen Kapitel 2.1.6 eingefügt Kapitel 2.2.10 eingefügt Kapitel 2.3.8 eingefügt Inhaltsverzeichnis aktualisiert Anmerkung: zu früheren Versionen dieses Dokumentes liegt keine Versionshistorie vor.		

--- Ende des Dokuments ---