operational services GmbH & Co. KG

MANAGEMENT-HANDBUCH

IMPRESSUM

Titel	Version	Vertraulichkeit
Management-Handbuch	3.2	öffentlich
Thema	Aufzeichnungsdatum	Status
Integriertes Managementsystem	18.06.2018	freigegeben
Autor	Inhaltlich geprüft von	Freigegeben von
L. Wilhalm, D. Wedekind	S. Tomas	Geschäftsführung
Firma		
operational services GmbH & Co. KG		
Archivierungspflicht	Aufbewahrungsfrist	Archivierungsort
☒	6 Jahre	OS-Portal

ÄNDERUNGSHISTORIE

Datum	Version	Beschreibung	Autor
12.08.2010	0.8	Initiale Erstellung des Management-Handbuchs	Ralf Bremert
06.12.2010	0.9	Review	Dr. Jörg Cordsen
10.12.2010	1.0	Freigabe	Geschäftsführung
12.08.2011	2.0	Überarbeitung	Ralf Bremert
05.11.2012	2.1	Freigabe	Lutz Wilhalm
12.12.2012	2.2	Integration Verpflichtungserklärung	Lutz Wilhalm
14.01.2013	2.3	Kapitel 7.9: Managementreview kann aufgeteilt werden	Lutz Wilhalm
08.02.2013	2.4	Einarbeitung Leitsätze und Ziele	Lutz Wilhalm, Sebastian Ruppert
08.02.2013	2.4	Freigabe	Geschäftsführung
24.09.2014	2.5	1. Neue Standorte aufgenommen 2.2 Angebot und Dienstleitungen aktualisiert 7.3 Process Map aktualisiert 6.1 Ziele der Informationssicherheit angepasst 8. Ergebnis der Prüfung ergänzt Generell: Verwendung des Begriffs „QMB“ (ehem. QAO) vereinheitlicht	Detlef Wedekind, Lutz Wilhalm
25.09.2014	2.5	Prüfung durch den QMB	S. Tomas
26.09.2014	2.5	Freigabe	Geschäftsführung
06.07.2015	2.7	In neues Format übertragen. 1.2 Geltungsbereich gestrafft. 2.2.1 Cyber Security ergänzt. 6. Schutzklassen angepasst. Abbildungen 2, 4, 5 und 6 entfernt.	Detlef Wedekind
09.10.2015	2.7	Prüfung durch den QMB	S. Tomas
12.10.2015	2.7	Freigabe	Geschäftsführung

05.09.2016	2.8	Generell: Austausch „Kontinuierliche Verbesserung“ durch „fortlaufende Verbesserung“ 2.1.1 Strategischer Rahmen der OS aktualisiert. 4. Vier neue Führungskompetenzen eingefügt. 4.2 Führung und Verpflichtung der obersten Leitung ergänzt. 5. Qualitätspolitik: risikobasierter Ansatz ergänzt.	D. Wedekind, L. Wilhalm
27.09.2016	2.8	Prüfung durch den QMB	S. Tomas
28.09.2016	2.8	Freigabe	Geschäftsführung
22.09.2017	2.9	1. Wegfall Hoyerswerda, Aufnahme Senftenberg 7.8. Maßnahmenverfolgung durch die GF ergänzt. Vorlage im MTIMS und KTIMS.	D. Wedekind
22.09.2017	2.9	Freigabe	Geschäftsführung
26.02.2018	3.0	Das Kapitel Integriertes Managementsystem neu strukturiert. Referenzierung von Richtlinien.	D. Wedekind, L. Wilhalm
26.02.2018	3.1	Datenschutz gemäß DS-GVO aufgenommen.	Eckhard Becker
18.06.2018	3.2	Freigabe	Geschäftsführung

Es wird darauf hingewiesen, dass die ggf. im Dokument verwendeten Begrifflichkeiten nicht als diskriminierend im Sinne des Allgemeinen Gleichbehandlungsgesetzes zu verstehen sind. Bezeichnungen und Begriffe werden einheitlich geschlechtsneutral entsprechend der Funktion oder Tätigkeit verwendet; diese Funktions- und/oder Tätigkeitsbezeichnungen haben nicht die Absicht, nur Frauen oder nur Männer zu erfassen. Jede Form der Ungleichbehandlung ist ausgeschlossen.

INHALTSVERZEICHNIS

1 EINFÜHRUNG

Die operational services GmbH & Co. KG ist am 01. Juli 2005 unter dem Namen gedas operational services GmbH Co. KG gestartet. Im Jahr 2008 erfolgte die Umfirmierung auf den heutigen Namen operational services GmbH & Co. KG (nachfolgend OS). In der OS wurden die Kompetenzen des IT-Betriebes der Fraport AG und der früheren gedas Deutschland GmbH gebündelt. Heute tragen die Fraport AG und die T-Systems International GmbH das Unternehmen als Joint Venture zu je 50 %.

Unsere Aktivitäten steuern wir von unserem Firmensitz in Frankfurt, sowie von unseren Standorten in Berlin, Braunschweig, Dresden, München, Nürnberg, Senftenberg, Wolfsburg und Zwickau aus. Wir sind sowohl mit eigenem Vertrieb und Auftritt im Markt präsent, als auch eingebunden in die Aktivitäten unseres Gesellschafters T-Systems.

Die OS ist ein mittelständisches Unternehmen der Informationstechnologie mit einer starken Gesellschafterstruktur. Das gibt unseren Kunden Sicherheit. Als Partner mit kurzen Entscheidungswegen haben wir genau die Flexibilität, die unsere Kunden in einer sich schnell wandelnden Welt benötigen.

Als Unternehmen bringen wir mehr als 20 Jahre Erfahrung im professionellen IT-Betrieb mit. Über 850 hochqualifizierte und motivierte Mitarbeiterinnen und Mitarbeiter sorgen heute für den reibungslosen Betrieb der Informationstechnik bei unseren Kunden. Darüber hinaus liefern wir weitergehende IT-Service und Support Dienstleistungen bis hin zu kompletten IT-Realisierungsprojekten; einen wesentlichen Teil davon unmittelbar vor Ort bei unseren Kunden.

Unser Leitbild drückt das Selbstverständnis unserer Gesellschaft aus: „Wir stellen eine verlässliche und geachtete Größe im Markt dar. Unsere Kunden werden mit und durch uns erfolgreicher. Unser Erfolg basiert auf leistungsorientierten, und motivierten Mitarbeiterinnen und Mitarbeiter. Unser Handeln ist stets bestimmt von den Verhaltensnormen und den fünf Leitlinien, die in unserem Code of Conduct beschreiben sind."

Konkurrenzfähige Preise, überdurchschnittliche Qualität und die Gewährleistung der Sicherheit der Informationen sind ausschlaggebend, um langfristige Kundenbindungen einzugehen und zu erhalten. Zur Erreichung dieser Ziele setzen wir auf transparente Geschäftsprozesse, die durch das Integrierte Managementsystem der OS gesteuert werden. Dies schafft die Grundlage, um langfristig als erfolgreiches Unternehmen am Markt zu bestehen und zu wachsen.

Das Integrierte Managementsystem (IMS) der OS umfasst Qualitätsmanagement (QM) Informationssicherheitsmanagement (ISMS) und Datenschutz. QM und ISMS sind entsprechend den Anforderungen der internationalen Normen ISO 9001 und ISO 27001 aufgebaut. Es sind keine Ausschlüsse definiert.

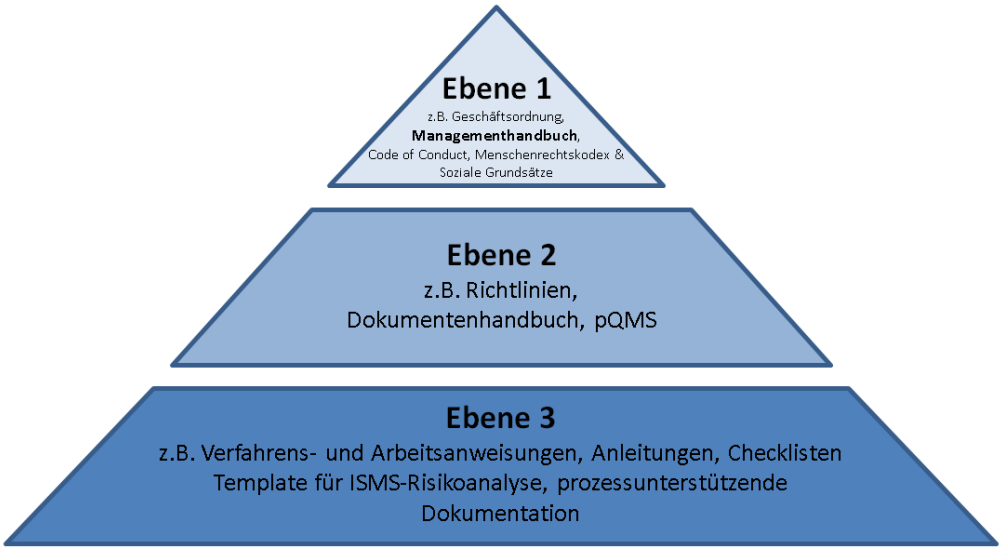
1.1 ZIELSETZUNG

Dieses Management-Handbuch beschreibt Politik und Strategie der OS in Bezug auf das IMS. Es ist damit Grundlage und Leitdokument des IMS. Zu einzelnen inhaltlichen Schwerpunkten wird auf die entsprechenden weiterführenden Dokumente und Richtlinien verwiesen.

1.2 GELTUNGSBEREICH

Dieses Handbuch ist gültig für alle Organisationseinheiten an allen Standorten der operational services GmbH & Co. KG.

1.3 EINORDNUNG DIESES DOKUMENTS



Das Management-Handbuch stellt gemeinsam u.a. mit der Geschäftsordnung der Geschäftsführung, dem Code of Conduct und des „Menschenrechtskodex und Soziale Grundsätze" die höchste Ebene des Regelwerks des IMS der OS dar. Alle anderen Dokumente, Richtlinien, Anweisungen etc. der Ebenen 2 und 3 müssen im Einklang mit den Dokumenten der Ebene 1 stehen.

1.4 DEFINITIONEN UND ABKÜRZUNGEN

- CISO Chief Information Security Officer
- CMS Compliance Managementsystem
- CO Compliance Officer
- DSB Datenschutzbeauftragter
- IMS Integriertes Managementsystem
- KTIMS Kernteam IMS
- MTIMS Managementteam IMS
- OS operational services GmbH & Co. KG
- PO Process Owner
- pQMS prozessorientiertes Qualitätsmanagementsystem
- PRT Process Review Team
- QISR Quality and Information Security Representative
- QMA Qualitätsmanagementauditor
- QMB Qualitätsmanagementbeauftragter

2 UNTERNEHMENSDARSTELLUNG

Die OS hat unter dem Namen gedas operational services GmbH & Co. KG (gedas os) am 01.07.2005 als Joint Venture Unternehmen der früheren gedas Deutschland GmbH und der Fraport AG Ihre geschäftlichen Aktivitäten aufgenommen. Zur selben Zeit wurde ein IT-Servicevertrag mit einer Laufzeit von 10 Jahren zwischen der Fraport AG und der gedas os geschlossen, der 2011 vorzeitig bis 2018 verlängert und der in 2017 mit einer Laufzeit bis Mitte 2023 neu abgeschlossen wurde. Gegenstand dieses Vertrags ist die Bereitstellung eines Userhelpdesks, der Betrieb von Netzwerk-, Server, Backup- und Datenbank-Infrastrukturen, die Erbringung eines SAP-Basis-Betriebs und das Management des Rechenzentrums für den Flughafen Frankfurt am Main.

Am 1. April 2006 übernahm T-Systems von der Volkswagen AG die Anteile an der gedas AG – einschließlich 50 % Beteiligung der gedas Deutschland GmbH an der OS. Die gedas Deutschland GmbH wurde zum 01.07.2007 mit der T-Systems Enterprise Services GmbH (heute T-Systems International GmbH) verschmolzen. Am 30.05.2008 erfolgte die Umfirmierung der gedas operational services GmbH & Co. KG in operational services GmbH & Co. KG.

T-Systems ist die Großkundensparte der Deutschen Telekom. Auf Basis einer weltumspannenden Infrastruktur aus Rechenzentren und Netzen betreibt das Unternehmen Informations- und Kommunikationstechnik (engl. kurz ICT) für multinationale Konzerne und öffentliche Institutionen. Mit Niederlassungen in über 20 Ländern und globaler Lieferfähigkeit betreut T-Systems Unternehmen aus allen Branchen – von der Automobilindustrie über Telekommunikation, den Finanzsektor, Handel, Dienstleistungen, Medien, Energie und Fertigungsindustrie bis zur öffentlichen Verwaltung und dem Gesundheitswesen. Rund 47.600 Mitarbeiterinnen und Mitarbeiter weltweit setzen sich mit ihrer Branchenkompetenz und ihrem ICT-Know-how für höchste Servicequalität ein.

Die OS ist wirtschaftlich voll in die T-Systems konsolidiert und arbeitet operativ eng mit den Bereichen der Gesellschaft zusammen.

2.1 STRATEGIE UND ZIELE

2.1.1 Strategischer Rahmen der OS

Der strategische Rahmen der OS enthält die aufeinander abgestimmten Elemente Vision, Leitbild, Leitkennzahlen, Strategischer Fahrplan, BSC und Masterplan.

Abbildung 1: Strategischer Rahmen der OS

2.1.2 Vision / Mission

Wir sind eine eigenständige Gesellschaft mit profitablem Wachstum.

Wir setzen um, was wir versprechen. Dafür stehen wir mit unserem Namen!

Wir betreiben ICT-Strukturen zentral, remote und auch vor Ort!

Wir führen innovative Lösungen ein und orchestrieren Cloud-Umgebungen!

Wir machen unsere Kunden fit für die digitale Zukunft!

2.1.3 Leitbild

Wir stellen eine verlässliche und geachtete Größe im Markt dar.

Unsere Kunden werden mit und durch uns erfolgreicher.

Unser Erfolg basiert auf leistungsorientierten, motivierten Mitarbeiterinnen und Mitarbeitern.

Unser Handeln ist stets bestimmt von den Verhaltensnormen und den fünf Leitlinien der OS, die in unserem Code of Conduct beschrieben sind.

2.2 ANGEBOT UND DIENSTLEISTUNGEN

Als einer der führenden mittelständischen Anbieter von IT Dienstleistungen ist operational services (OS) seit 2005 sehr erfolgreich am Markt vertreten.

Vom Back Office bis zur Vorstandsetage, vom Produktionsband bis zum Lagerregal, vom Desktop bis hin zum mobilen Endgerät – die OS unterstützt Menschen und Organisationen darin, effizient zu arbeiten.

Unser Kerngeschäft sind Managed IT Services. Darin sind wir gut und erhalten regelmäßig Bestnoten von unseren Kunden. Wir beraten in IT-Strategiefragen, betreiben ein eigenes, hochverfügbares Rechenzentrum „Made in Germany", Applikationen, Netzwerke und andere Betriebsumgebungen sowie dazugehörige Dienstleistungen wie Service Desk, Call Center und Client Services.

Als Joint Venture von der Fraport AG und der T-Systems International GmbH haben wir unseren Hauptsitz am Frankfurter Flughafen und sind mit über 850 Professionals an neun Standorten vertreten.

Weitere Informationen finden Sie unter: www.operational-services.de

Das aktuelle Produktportfolio setzt sich aus drei Produktdimensionen zusammen: Beratung, Services und Lösungen.

2.2.1 Beratung

Unsere Beratungskompetenz kommt nicht von ungefähr. Sie ist Ergebnis einer 25-jährigen Unternehmenshistorie als Full-Service-Dienstleister für Entwicklung, Systemintegration und dem Betrieb von ICT-Lösungen für Kunden aus den unterschiedlichsten Branchen.

Wir begleiten unsere Kunden in allen Phasen von Infrastrukturprojekten und übernehmen auch Verantwortung für eine Umsetzung im Betrieb. Vorhaben zur individuellen Anpassung von ICT-Systemen unterstützt die OS mit professionellen Leistungen zu Projektmanagement, ICT-Kommunikation sowie Transition und Transformation. Den Betrieb von unternehmensweiten ICT-Infrastrukturen optimieren wir im Rahmen unserer Beratungsmodule ICT-Servicemanagement und ICT-Sicherheit.

Unser erfahrenes Beraterteam begleitet unsere Kunden bei der Umsetzung individueller ICT-Strategien und dem Umstieg auf Cloud-Lösungen im Konzern.

2.2.2 Services

ICT Services der OS sind effizient, sicher und hoch verfügbar. Unsere Leistungen sind „Made in Germany" und gewährleisten so die Einhaltung deutscher Gesetze und Sicherheitsbestimmungen.

Die OS betreibt zentrale und dezentrale Standard- und Individualapplikationen, Netzwerk- und andere Betriebsumgebungen. Unsere ICT Services werden nach standardisiertem ITIL Vorgehen erbracht.

Die ICT-Systeme unserer Kunden betreiben wir bei unseren Kunden vor Ort (On Premise) mit zugeschnittenen Teams und der Übernahme von Betriebsverantwortung, im Remote-Betrieb und in unseren eigenen Data Centers in Deutschland.

Unser professioneller Service Desk unterstützt optimal auch kleinere Benutzerzahlen, besondere Anwendungen oder auch kurzzeitig als Verstärkung des Supports in Projekten.

Der besondere Mehrwert für die Kunden der OS liegt in der langjährigen Erfahrung eines Full-Service-Providers verbunden mit unseren Anforderungen an einen hohen Standard. Das lassen wir uns regelmäßig zertifizieren (ISO 9001, ISO 27001).

2.2.3 Lösungen

Die Lösungen der OS sind ausgereifte Ergebnisse, die aus der gemeinsamen Arbeit mit unseren Kunden entstanden sind. Mit dem Einsatz einer Lösung von OS erhalten unsere Kunden ein vordefiniertes, dedizierten Set an Beratungsleistungen, ICT Services und ggfs. Lizenzen, die zusammen ICT-Projektziele schnell und in einem hervorragenden Preis-Leistungsverhältnis erreichen.

Zurzeit bieten die ICT-Experten der OS folgende Lösungsmodule an:

- ServiceNow: Cloud-basiertes Service Management aus Deutschland
- Virtual Training Solutions: Schnelle und flexible Infrastruktur für Schulungen und Seminare
- Secure Data Distribution: weltweit sichere „vor Ort" Bereitstellung von kritischen Daten mit eigenem Verteilersystem (Box)
- Supplier Connectivity: Managed Network Access für Partner
- Managed Print Solutions: Standortübergreifendes, gesichertes Drucken
- HP Service Manager: Migration, Anpassung und Betrieb von HSPM Plattformen

Die Lösungen haben einen hohen Automatisierungs- und Standardisierungsgrad, werden jedoch auf die individuellen Bedarfe unser meist mittelständischen Kunden angepasst.

2.2.4 Zielmärkte

Die OS fokussiert sich auf Bestands- und Neukunden in den Bereichen Transportwirtschaft, Logistik sowie Automobil- und Fertigungsindustrie, Zulieferindustrie und öffentliche Dienstleistung. Dabei spricht OS vor allem mittelständische Unternehmen und Organisationen in diesen Märkten an.

3 KUNDENORIENTIERUNG

Kundenorientierung bestimmt das Handeln unserer Mitarbeiterinnen und Mitarbeiter.

Dafür stehen die Leitlinien

- „Kunden begeistern",
- „Integrität und Wertschätzung leben" und
- „Ich bin OS – auf mich ist Verlass"

unseres Leitbildes Kapitel 2.1.3.

Die Kundenzufriedenheit als Messgröße der Kundenorientierung wird jährlich bei ausgewählten Kunden gemessen und geht als ein wichtiger Faktor in die Zielvereinbarungen für außertarifliche Angestellte ein.

4 MITARBEITERINNEN UND MITARBEITER

Gute Mitarbeiterinnen und Mitarbeiter sind der Erfolgsfaktor Nummer eins. Auf Basis der Leitlinien

- „Offen zur Entscheidung – geschlossen umsetzen" und
- „Leistung anerkennen – Chancen bieten"

ermöglichen wir den Beschäftigten attraktive, die Persönlichkeitsentwicklung unterstützende berufliche Perspektiven und fördern konsequent interne Talente. Mit einheitlichen und möglichst einfachen Prozessen und Instrumenten gewinnt, begeistert und qualifiziert die operational services Fach- und Führungspersonal, entwickelt Talente, und sichert damit die Zukunftsfähigkeit unseres Unternehmens.

Wir sind leistungsorientiert und setzen uns konsequent für das bestmögliche Ergebnis ein. Wir anerkennen und honorieren gute Leistungen. Dabei ist die individuell unterschiedliche Leistungsfähigkeit zu beachten. Das ist eine große Verpflichtung für alle Führungskräfte.

Wir schaffen ein Klima, in dem sich jeder von uns wertgeschätzt fühlt, sich persönlich und zum Wohl unseres Unternehmens weiterentwickeln kann und Freude an der Arbeit hat. Wir fördern Verhaltensweisen, die eine Wertsteigerung unseres Unternehmens und die Bestätigung unserer Werte sicherstellen. Hierbei ist es wichtig, die richtigen Menschen mit den richtigen Aufgaben zu betrauen. Führungskräfte unterstützen ihre Mitarbeiterinnen und Mitarbeiter dabei, Beruf und Privatleben vereinbaren zu können und schaffen somit die Basis für produktives Arbeiten.

Wir bauen auf motivierte und qualifizierte Beschäftigte, die Verantwortung für die eigene Entwicklung übernehmen und Veränderungen als Chance begreifen.

Wir fördern aus sozialer Verantwortung heraus in einer sich stetig wandelnden Arbeitswelt die Beschäftigungsfähigkeit der Mitarbeiterinnen und Mitarbeiter und erwarten hierbei auch deren Eigeninitiative.

OS-Führungskompetenzen

Team: Die Führungskraft verfolgt die Unternehmensziele durch enge bereichsübergreifende Zusammenarbeit. Sie bezieht die Meinungen ihrer Führungskräfte, Kolleginnen und Kollegen und Mitarbeiterinnen und Mitarbeiter in Entscheidungen ein. Die Führungskraft kennt die Ziele der anderen Bereiche und bindet diese in die eigene Arbeit mit ein. Sie zeigt sich bei sachlicher Argumentation kompromissbereit.

Mitarbeiterinnen und Mitarbeiter: Die Führungskraft fordert und fördert eigenverantwortliches Arbeiten und entwickelt so die Fähigkeiten ihrer Mitarbeiterinnen und Mitarbeiter weiter. Sie übernimmt Verantwortung für ihre Mitarbeiterinnen und Mitarbeiter und deren Leistungen. Sie gibt regelmäßig Feedback und fördert damit den regelmäßigen Austausch. Sie macht ihren Mitarbeiterinnen und Mitarbeitern deutlich, was sie erwartet. Durch Handlungsspielräume fördert sie das Potential ihrer Mitarbeiterinnen und Mitarbeiter.

Verbindlichkeit: Die Führungskraft steht hinter den Leistungen der OS. Sie hält Vereinbarungen ein – sowohl intern als auch gegenüber Kunden. Sie gibt präzise Anweisungen, die keinen Interpretationsspielraum offen lassen. Die Führungskraft trägt die Konsequenzen ihrer Handlungen. Sie nimmt die Anliegen und Probleme ihrer Mitarbeiterinnen und Mitarbeiter ernst.

Leistungs- und Ergebnisorientierung: Die Führungskraft führt ergebnisorientiert. Sie erkennt und lobt gute Leistungen. Kritik wird angesprochen, sachlich und offen. Die Führungskraft hat keine Scheu vor Konflikten, sondern geht sie lösungsorientiert an. Die Führungskraft ist Vorbild bei der systematischen Verbesserung von Arbeitsweise und –qualität. Die Führungskraft schafft eine Arbeitsatmosphäre, in der konstruktiv gearbeitet werden kann.

Lernende Organisation: Die Führungskraft arbeitet ständig an der Verbesserung von Abläufen und Qualität. Sie erkennt Verbesserungspotentiale und setzt sie um. Sie begreift Veränderungen als Chance und gestaltet sie aktiv. Die Führungskraft bindet Beteiligte in Veränderungsprozesse ein. Sie erläutert Veränderungen für die Betroffenen nachvollziehbar.

Strategisches Denken und Handeln: 24-Monats-Fokus: Die Führungskraft betrachtet ihre Ziele im Kontext der mittel- und langfristigen Unternehmensziele und orientiert ihr Handeln daran. Sie denkt vorausschauend und leitet Maßnahmen ab, um mit OS auch mittel- und langfristig erfolgreich zu sein. Sie erkennt frühzeitig die Wünsche und Bedürfnisse der Kunden und reagiert entsprechend. Sie steuert und entwickelt ihre Mitarbeiterinnen und Mitarbeiter und deren Kompetenz auch im Hinblick auf langfristige Markterfordernisse.

Kundenorientierung: Die Führungskraft stellt die Interessen und Bedürfnisse von Kunden in den Vordergrund, ohne dabei die OS-Interessen zu vernachlässigen. Die Führungskraft übernimmt Verantwortung für die Qualität von Dienstleistungen und Produkten. Sie erfüllt die Erwartungen der Kunden pünktlich und erwartungsgemäß.

Kommunikationseffizienz: Die Führungskraft passt ihre Kommunikation dem Empfänger an:

- Tempo
- Detaillierungsgrad
- Validität

Der Informationsgehalt ihrer Aussagen ist präzise und klar verständlich. Sie gewinnt andere Personen für ihre Ideen und Vorhaben. Sie kommuniziert offen und ehrlich – besser nichts, als nicht die Wahrheit! Präsentation und Medieneinsatz werden zielführend gewählt

Fachkompetenz: Das Wissen der Führungskraft bringt die OS weiter und ist stets auf dem aktuellen Stand. Die Führungskraft erlangt aktiv Wissen, auch über Ihren eigenes Fachthema hinaus. Die Führungskraft setzt ihre Fachkompetenz auch zur Weitergabe von Wissen ein. Die Führungskraft weiß, welches Wissen morgen und übermorgen wichtig ist, versteht technologische Zukunftsthemen und macht diese für OS nutzbar.

4.1 FÜHRUNGSORGANISATION

Wir führen in einfachen Strukturen und achten darauf, dass geeignete Mitarbeiterinnen und Mitarbeiter zum optimalen Nutzen für unsere Kunden richtig eingesetzt werden. Flexible Arbeitszeitmodelle fördern die Anpassung an die Kundenbedürfnisse und den Geschäftsverlauf. Durch fortlaufende Verbesserungsprozesse und vernetzte Zusammenarbeit wird die Lernfähigkeit unserer Organisation ständig erhöht.

4.2 VERANTWORTUNG DER FÜHRUNGSKRÄFTE, MITARBEITERINNEN UND MITARBEITER

Die oberste Leitung der OS zeigt in Bezug auf das IMS Führung und Verpflichtung. Führungskräfte und alle Mitarbeiterinnen und Mitarbeiter der OS übernehmen die Verantwortung für die Qualität ihrer Arbeit. Die Führungskräfte schaffen in ihren Organisationseinheiten die Voraussetzungen zur Umsetzung der Qualitäts-, Informationssicherheits- und Datenschutzpolitik des Unternehmens.

Die Führungskräfte tragen in Ihrem Zuständigkeitsbereich die Verantwortung dafür, dass beim Umgang mit Informationen und Informationssystemen jederzeit eine angemessene Informationssicherheit und der Schutz von personenbezogenen Daten gewährleistet ist. Daraus ergibt sich für alle Führungskräfte die Aufgabe, in ihrem Verantwortungsbereich die Regelungen des IMS umzusetzen, daraus abgeleitete

Maßnahmen durchzusetzen und bei Notwendigkeit mit anderen Unternehmensbereichen und bei Bedarf mit dem Kunden abzustimmen.

Jede Mitarbeiterin und jeder Mitarbeiter, der mit Informationen umgeht, sie erzeugt oder einbringt, ist für deren Kennzeichnung und Klassifizierung im Rahmen von Vorgaben des Unternehmens verantwortlich. Jede Mitarbeiterin und jeder Mitarbeiter, der Informationen nutzt, ist verpflichtet mit Informationen und Informationssystemen sorgfältig umzugehen sowie diese ausschließlich im Sinne der zugewiesenen Aufgaben und im Rahmen der gültigen Prozesse, Richtlinien und Regelungen zu nutzen.

4.3 BEWUSSTSEIN

Qualität, Informationssicherheit und Datenschutz werden von allen Mitarbeiterinnen und Mitarbeitern umgesetzt, die hierbei von den geltenden Prozessen, Richtlinien und Schulungen unterstützt werden. Deshalb verpflichten sich die Geschäftsleitung, die Führungskräfte, sowie alle Mitarbeiterinnen und Mitarbeiter die durch das Regelwerk des IMS getroffenen Festlegungen entsprechend umzusetzen und an der fortlaufenden Weiterentwicklung mitzuwirken. Das erfordert die Entwicklung einer Unternehmenskultur, in der Qualität, Informationssicherheit und Datenschutz einen hohen Stellenwert haben und von allen Unternehmensangehörigen gelebt werden.

5 COMPLIANCE MANAGEMENTSYSTEM

Das Compliance Management System (CMS) ist die Gesamtheit der in der OS eingerichteten Maßnahmen und Prozesse, um Regelkonformität sicherzustellen.

Das CMS der OS ist an die CMS der Gesellschafter Fraport AG und T-Systems gekoppelt. Die OS arbeitet in den CMS-Prozessen der T-Systems und hat mehrere Compliance-Richtlinien des Telekom-Konzerns für sich übernommen.

Der Compliance Officer der OS berichtet regelmäßig an beide Gesellschafter.

S.a. Richtlinie „Einhaltung und Überwachung von Vorgaben".

6 INTEGRIERTES MANAGEMENTSYSTEM (IMS) DER OS

Ein Managementsystem kann aus betriebswirtschaftlicher Sicht definiert werden als formal verankertes System für die Gestaltung, Lenkung und Entwicklung von Unternehmen und anderen Organisationen verschiedenster Art. In der Regel enthält es detaillierte Aussagen über die Organisation des Unternehmens, Ziele und Strategien, Auswahl und Qualifizierung der Mitarbeiterinnen und Mitarbeiter, Prozesse, Regeln und Richtlinien, Monitoring, Kontrolle und Berichterstattung sowie den Umgang mit Lieferanten.

6.1 INHALT UND UMFANG DES INTEGRIERTEN MANAGEMENTSYSTEMS (IMS)

Das IMS der OS ist ausgerichtet auf Qualitätsmanagement, Informationssicherheitsmanagement und Datenschutz. Es ist prozessorientiert gestaltet und basiert auf den Strukturvorgaben, die sich aus den internationalen Normen ISO 9001, ISO 27001 und der DS-GVO ableiten. Das Managementsystem der OS ist dokumentiert in Form von Prozessbeschreibungen und Richtlinien, welche im „prozessorientierten Qualitäts-Managementsystem" (pQMS) visualisiert sind.

Im Compliance Register sind alle gültigen Dokumente der 1. und 2. Ebene dokumentiert.

Das Information Security Register (ISR; enthält das Statement of Applicability, SOA) beschreibt die konkrete Umsetzung der Anforderungen aus der Norm ISO 27001 und die Weiterentwicklung bezogen auf das Informationssicherheitsmanagement.

Bezogen auf das IMS der OS werden keine Normforderungen der ISO 9001 und ISO 27001 ausgeschlossen.

6.2 ORGANISATION DES INTEGRIERTEN MANAGEMENTSYSTEMS

6.2.1 Verantwortung der Geschäftsführung für Qualität, Informationssicherheit und Datenschutz

Die Geschäftsführung der OS verpflichtet sich zur Entwicklung, Verwirklichung und ständigen Verbesserung der Effektivität des IMS. Mit der Erstellung, Weiterentwicklung und Bekanntgabe von Richtlinien des IMS auf Basis der entsprechenden Gesetze und Normen wurden der QMB, der CISO und der DSB zusammen mit den beratenden und prüfenden Gremien MTIMS und KTIMS beauftragt s.a. Richtlinie „Organisation des Integrierten Managementsystems".

6.2.2 Operative Steuerung

Um der Komplexität der Anforderungen an das IMS gerecht zu werden, erfolgt eine organisatorische Trennung der Verantwortlichkeit für Entscheidungen zum Qualitätsmanagement, zur Informationssicherheit und zum Datenschutz. Die Integration bei der Weiterentwicklung wird gewährleistet durch enge Abstimmung des QMB, des CISO und des DSB und durch gegenseitige Teilnahme der Verantwortlichen in den jeweiligen Gremien.

Die detaillierten Beschreibungen der Aufgaben der nachfolgend beschriebenen Rollen befinden sich in den Rollenbeschreibungen im OS-internen Portal.

6.2.3 Der Qualitätsmanagementbeauftragte (QMB)

Der QMB ist verantwortlich für:

- Aufbau, Umsetzung und Weiterentwicklung des QM-Systems
- Ausbau / die Weiterentwicklung der Qualitätssicherungsmethoden
- Definition und Reporting von Qualitätskennzahlen
- Definition und Messung der Qualitätsziele in Zusammenarbeit mit den Fachbereichen und der Geschäftsführung

Der QMB hat die Befugnisse:

- Definition und Umsetzung von Maßnahmen zur Verbesserung des QM-Systems
- Definition und Umsetzung von Maßnahmen zur Qualitätsverbesserung

6.2.4 Der Chief Information Security Officer (CISO)

Der CISO ist verantwortlich für:

Die Bereitstellung von Verfahren und Methoden im Bereich der Informationssicherheit, z. B. für die Erstellung von Sicherheitskonzepten, die Durchführung von Risikoanalysen oder Security Reviews und deren Durchführung. Als Mitglied des Managementteam Integriertes Managementsystem (MT IMS)

berichtet der CISO dort, wie auch gegenüber der Geschäftsführung, über den Status der Informationssicherheit.

Im Weiteren ergeben sich die folgenden Aufgaben für den CISO:

- Umsetzung der Vorgaben der Informationssicherheitspolitik
- Koordination des MT IMS und Ansprechpartner des MT IMS für die Umsetzung der Vorgaben des Regelwerks der Informationssicherheit in Bezug auf die eingesetzte Informationstechnik
- Erstellen von Berichten für die Geschäftsführung
- Erstellen der Jahresplanung und des –budgets für den Bereich Informationssicherheit
- Verantwortet die Erstellung und Pflege von Sicherheitsrichtlinien
- Verantwortet die Erstellung von Security Awareness Materialien
- Ansprechpartner für die Interessen Dritter hinsichtlich der Informationssicherheit innerhalb der OS
- Überwacht die Behandlung von Sicherheitsvorfällen, Definition und Überwachung von Meldewegen
- Bereitstellung von Methoden zur Erstellung von Sicherheitskonzepten und zur Durchführung von Risikoanalysen
- Überwacht die Einarbeitung notwendiger Verbesserungen aus den Ergebnissen von Audits und Reviews
- Verantwortet die regelmäßige Überprüfung des Umsetzungsstandes des Regelwerks der Informationssicherheit in Zusammenarbeit mit QM
- Koordination von Plänen, Aktivitäten und Ressourcen, um die Anforderungen zu erfüllen, die sich aus der Informationssicherheitspolitik und daraus abgeleiteten Dokumenten ergeben
- Verantwortet die Erstellung und Pflege von Sicherheitssystemstandards und Handlungsanweisungen
- Unterstützung der Fachbereiche bei der Ermittlung von Sicherheitsanforderungen
- Unterstützung der Fachbereiche bei der Ausarbeitung von Service Requirements und Service Deliveries (siehe Richtlinie „Werteverwaltung und Risikobehandlung“)
- Unterstützung von Projekten in Fragen zur Informationssicherheit
- Beaufsichtigt die Durchführung von Sicherheitsanalysen und Security Reviews seitens QM

Der CISO hat die Befugnisse:

- Veranlassen der Umsetzung der Anforderungen des ISMS sowie sicher stellen, dass das ISMS den Anforderungen der ISO27001 entspricht.
- Veranlassen und durchführen von Reviews bzgl. ISMS
- Einberufen des Sicherheitsvorfallsteams
- Steuern des MT IMS
- Steuern und beauftragen der QISR
- Beauftragen von Maßnahmenumsetzungen bzgl. IMS (z.B. im IMS-Risikomanagement) und der Behandlung von Sicherheitsvorfällen
- Durchführung von IMS-Schulungen
- Berichterstatten zur Leistung des ISMS gegenüber der Geschäftsführung

6.2.5 Der Datenschutzbeauftragte

Dem Datenschutzbeauftragten obliegen folgende gesetzliche Aufgaben:

Unterrichtung und Beratung des Verantwortlichen und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach dieser Verordnung sowie nach sonstigen Datenschutzvorschriften der Union bzw. der Mitgliedstaaten.

Überwachung der Einhaltung der Anforderungen der EU-Datenschutzgrundverordnung, anderer Datenschutzvorschriften der Union bzw. der Mitgliedstaaten sowie der Strategien des Verantwortlichen für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiterinnen und Mitarbeiter und der diesbezüglichen Überprüfungen.

Beratung – auf Anfrage – im Zusammenhang mit der Datenschutz- Folgenabschätzung und Überwachung ihrer Durchführung gemäß Artikel 35 DS-GVO.

Zusammenarbeit mit der Aufsichtsbehörde.

Tätigkeit als Anlaufstelle für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen, einschließlich der vorherigen Konsultation gemäß Artikel 36 DS-GVO, und gegebenenfalls Beratung zu allen sonstigen Fragen.

Der Datenschutzbeauftragte trägt bei der Erfüllung seiner Aufgaben dem mit den Verarbeitungsvorgängen verbundenen Risiko gebührend Rechnung, wobei er die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung berücksichtigt.

Die Bereitstellung von Verfahren und Methoden im Bereich des Datenschutzes, z. B. für die Erstellung von Datenschutzkonzepten, die Durchführung von Risikoanalysen oder Datenschutz Audit und deren Durchführung. Als Mitglied des Managementteams Integriertes Managementsystem (MT IMS) berichtet der DSB dort, wie auch gegenüber der Geschäftsführung, über den Status des Datenschutzes. Der DSB ist in seiner Tätigkeit weisungsfrei.

Im Einzelnen ergeben sich die folgenden Aufgaben für den DSB:

- Beratung und Empfehlungen zu Umsetzung der Datenschutzpolitik
- Ansprechpartner des MT IMS für die Umsetzung der Vorgaben des Regelwerks der Datensicherheit in Bezug auf die eingesetzte Informationstechnik
- Erstellen von Berichten für die Geschäftsführung
- Erstellen der Jahresplanung und des –budgets für den Bereich Datenschutz
- Verantwortet die Erstellung und Pflege von Datenschutzrichtlinien
- Durchführung von Mitarbeiterschulungen
- Verantwortet die Erstellung von Datenschutz Awareness Materialien
- Ansprechpartner für die Interessen Dritter hinsichtlich des Datenschutzes innerhalb und außerhalb der OS
- Überwacht die Behandlung von Datenschutzvorfällen, Definition und Überwachung der Meldewege und Einhaltung der Meldefristen
- Bereitstellung von Methoden zur Erstellung von Datenschutzkonzepten und zur Durchführung von Risikoanalysen
- Überwacht die Einarbeitung notwendiger Verbesserungen aus den Ergebnissen von Audits und Reviews
- Verantwortet die regelmäßige Überprüfung des Umsetzungsstandes des Regelwerks des Datenschutzes in Zusammenarbeit mit QM und CISO

- Unterstützung der Fachbereiche bei der Ermittlung von Datenschutzanforderungen
- Unterstützung von Projekten in Fragen zum Datenschutz
- Begleitung bzw. Koordination von externen Datenschutzaudits

6.2.6 Der Compliance Officer (CO)

Der CO ist verantwortlich für:

Der Compliance Officer (CO) der OS ist für die Einhaltung von Verpflichtungen und Vorgaben, auch in Bezug auf die Erstellung, Weiterleitung und Verarbeitung von Informationen, im Rahmen seiner Möglichkeiten verantwortlich. Als Owner des Prozesses Compliance-Management ist er für die Implementation und Weiterentwicklung dieses Prozesses verantwortlich.

Der CO hat die Befugnisse:

Melden von Compliance Verstößen - insbesondere, wenn Hinweise auf einen Compliance Verstoß durch die Geschäftsführung selbst vorliegen - an die Compliance Management Systeme der Gesellschafter der OS. Bearbeitung von Compliance Verstößen innerhalb der OS, bei Bedarf mit Unterstützung der Compliance Management Systeme der Gesellschafter.

6.2.7 Die Process Owner (PO)

Ein PO ist verantwortlich für:

- Ermittlung aller relevanten normativen und gesetzlichen Anforderungen und Anforderungen aus Richtlinien der OS und deren Anwendung im Prozess.
- Die Definition, Weiterentwicklung, Implementierung (inkl. Schulung) und Optimierung (laufende Verbesserung) seines Prozesses.
- Sicherstellen der Prozessanwendbarkeit und –anwendung.
- Die Integration der auf seinen Prozess anwendbaren Ziele der BSC, der Informationssicherheit und des Qualitätsmanagement in seinen Prozess.
- Die Effektivität und Effizienz des Prozesses.
- Die Überwachung seines Prozesses mittels Key Performance Indikatoren (KPI) zur Erreichung der Prozessziele.
- Analyse und Überwachung von Prozessrisiken und –chancen. Bereitstellung von Ressourcen für die Maßnahmenumsetzung.
- Umsetzen von Maßnahmen bzgl. des Prozesses aus der Risikoanalyse und z.B. aus internen und externen Audits.
- Das Prüfen und Einarbeiten von Verbesserungspotenzialen z.B. aus Lessons Learned und Anregungen von Prozessanwendern.
- Das Management von Wissen, das in seinem Prozess entstanden ist und/oder benötigt wird.
- Einberufen des Process Review Team (PRT) zur Prüfung von Änderungen.
  Freigabe und Kommunikation der vom PRT geprüften Änderungen.

Ein PO hat die Befugnisse:

- Prozess benennen, Ablauf entwerfen (modellieren).
- Koordination der Schnittstellen zu anderen Prozessen.
- Prozessdokumente erstellen:
- Prozess-Steckbrief incl. Risiko- und Chancenanalyse
- In das Process Review Team (PRT) zur Prüfung einbringen.
- Prozess(änderung) freigeben und in Kraft setzen.
- Prozess im Unternehmen schulen und einführen.
- Kommunikation über die Einführung des Prozesses.
- Auf Basis der definierten KPI den Prozess überwachen und evtl. Maßnahmen einleiten.
- Prozessabläufe regelmäßig analysieren und auf Gültigkeit und Risiken und Chancen prüfen .
- Verbesserungsmaßnahmen (KVP) planen und umsetzen.

6.2.8 Die Quality and Information Security Representatives (QISR)

Ein QISR ist verantwortlich für:

- Die Pflege und Weiterentwicklung des Integrierten Managementsystems im eigenen Verantwortungsbereich
- Schnittstelle vom IMS in den jeweiligen Fachbereich
- Schnittstelle vom jeweiligen Fachbereich in Projekte im Fachbereich
- Unterstützung des/der FBL, FGL, QMB, DSB, SKIP, CISO und des Notfallverantwortlichen

Ein QISR hat die Befugnisse:

- Veranlassen der Umsetzung der Anforderungen des IMS im eigenen Bereich sowie am eigenen Standort in Abstimmung mit dem FGL/FBL
- Veranlassen und durchführen von Reviews bzgl. IMS im eigenen Bereich in Abstimmung mit dem FGL/FBL
- Beauftragen von Maßnahmenumsetzungen bzgl. IMS (z.B. im IMS-Risikomanagement) und der Behandlung von Sicherheitsvorfällen im eigenen Bereich sowie am eigenen Standort in Abstimmung mit dem FGL/FBL
- Durchführung von IMS-Schulungen in Abstimmung mit dem CISO
- Absagen des PRB-Termins bei unzureichender Qualität der PRB-Unterlagen.

6.3 QUALITÄTSPOLITIK

Der Erfolg der OS wird maßgeblich dadurch bestimmt, wie gut und wie schnell wir die Bedürfnisse unserer Kunden verstehen und in attraktive Lösungen umsetzen. Der entscheidende Wettbewerbsvorteil ist die Qualität und deren marktgerechter Preis. Ein hoher Qualitätsstandard unserer Leistungen für die Kunden setzt voraus, dass unsere internen Abläufe, die Zusammenarbeit untereinander und die mit dem Kunden schnell, zielgerichtet und nachvollziehbar erfolgen. Wir setzen daher Methoden und Verfahren ein, die

- sichere und beherrschte Arbeitsprozesse ermöglichen,
- den Kundennutzen sichtbar machen und
- den Erfolg der Portfolioelemente der Geschäftsfelder verdeutlichen.

Die erfolgreiche Umsetzung dieser Qualitätspolitik durch alle Mitarbeiterinnen und Mitarbeiter der OS ist eine wesentliche Voraussetzung zur langfristigen Sicherung der Wettbewerbsfähigkeit unseres Unternehmens und unserer Kunden. Die Qualitätspolitik für das Unternehmen ist ausgerichtet an den Zielen unseres Unternehmens formuliert in der Balanced Scorecard (BSC).

Wesentlicher Bestandteil der Qualitätspolitik der OS ist der sogenannte „risikobasierte Ansatz". Er dient zur Prävention, um „unerwartete Effekte" bezogen auf fehlerfreie Produkte und Dienstleistungen, sowohl bei der Planung des IMS als auch bei der Ausführung der Prozesse zu vermeiden oder zu mindestens zu verringern und in die tägliche Arbeit zu übernehmen. Das Konzept der „vorbeugenden Maßnahmen" ist konsequent auf das gesamte IMS ausgeweitet und betrachtet sowohl Risiken als auch Chancen.

6.3.1 Qualitätsziele

Die Qualitätsziele der OS sind Teil der Unternehmensziele und in der BSC in den Finanz-, Prozess-, Kunden- und Mitarbeiterperspektiven dokumentiert.

6.3.2 Leitsätze zur Qualität

Das Verhalten aller Mitarbeiterinnen und Mitarbeiter der OS orientiert sich an folgenden Leitsätzen:

- Unsere Kunden entscheiden über die Qualität unserer Dienstleistungen.
- Denken und Handeln in Prozessen ist die Basis für optimierte Arbeitsabläufe, die es uns ermöglichen, den Anforderungen unserer Kunden zu entsprechen.
- Qualifizierung und Engagement unserer Mitarbeiterinnen und Mitarbeiter sind wesentliche Voraussetzungen, um Dienstleistungen im geforderten Qualitätsstandard zu erstellen.
- Qualität bedeutet, Fehler zu vermeiden und Fehlerursachen frühzeitig zu beseitigen.
- Qualität bedeutet ständige Verbesserung.

Die Umsetzung der Leitbilder erfordert ein hohes Maß an Qualitätsbewusstsein. Die Geschäftsleitung, Führungskräfte und die Qualitätsorganisation fördern aktiv Maßnahmen, um den Mitarbeiterinnen und Mitarbeitern bewusst zu machen, was die Erstellung von Dienstleistungen auf hohem Qualitätsniveau für das Unternehmen und seine Kunden bedeutet. Dabei ist Qualitätsbewusstsein durch folgendes Verhalten gekennzeichnet:

- Jede Mitarbeiterin und jeder Mitarbeiter hat die Verpflichtung, die Erwartungen seiner Kunden (extern und intern) zu erfüllen.
- Wir vereinbaren von Anfang an mit unseren Kunden den erwarteten Leistungsumfang.
- Jede Mitarbeiterin und jeder Mitarbeiter übernimmt die Verantwortung für seine Leistung.
- Die Erstellung unserer Dienstleistungen erfolgt systematisch und unter Anwendung bewährter Methoden und Verfahren.
- Wir tun die Dinge beim ersten Mal richtig. Durch Fehlervermeidung und Beseitigung von Fehlerursachen in jeder Phase der Leistungserstellung verringern wir die Kosten der Qualität.
- Qualitätsmanagement verstehen die Führungskräfte als eine Führungsaufgabe, um ein optimales Umfeld zu schaffen, welches die Mitarbeiterinnen und Mitarbeiter motiviert, Ihren Beitrag zur Erfüllung der Unternehmensziele zu leisten.

6.4 INFORMATIONSSICHERHEITSPOLITIK

Informationen gehören zum wichtigen Kapital der OS. Sie liegen in unterschiedlichsten Formen vor – auf Papier, als Telefax oder E-Mail, als gesprochenes Wort oder Know-how und insbesondere in digitaler Form in Verbindung mit informationsverarbeitenden IT-Systemen. Informationen werden aus unterschiedlichsten Quellen erhoben, erfasst, gespeichert, verarbeitet, ausgewertet, archiviert und entsprechend gesetzlicher Fristen gelöscht bzw. vernichtet. Die Informationssicherheit erfährt nicht nur durch den Schutz der Unternehmenswerte der OS einen hohen Stellenwert für den Geschäftserfolg, sondern auch durch den Schutz der für Kunden betriebenen Dienstleistungen.

Bei der Verarbeitung von Informationen ist eine Fülle von Rechtsvorschriften zu beachten. Die Nicht-Verfügbarkeit, der Verlust, die Verfälschung oder die nicht autorisierte Offenlegung auch von nur Teilen dieser Informationen kann mit hohen materiellen oder auch immateriellen Schäden für die OS, ihren Gesellschaftern oder ihren Kunden verbunden sein. Geht den Schäden ein Verstoß gegen Gesetze, Richtlinien oder sonstigen Regelungen der OS voraus, werden diese vom Compliance Officer bearbeitet und bei Bedarf an die Gesellschafter gemeldet s.a. 6.2.6. Deshalb ist es erforderlich, dass diese Informationen – unabhängig von der Form, in der sie vorliegen – einschließlich ihrer Verarbeitungsprozesse durch geeignete Sicherheitsmaßnahmen geschützt werden.

Erreicht wird dies durch ein angemessenes Bewusstsein bzgl. der Informationssicherheit bei allen Mitarbeiterinnen und Mitarbeitern sowie einer Einbettung der Informationssicherheit in die Geschäftsprozesse, in den Aufbau von Infrastruktur und in Entwicklung, Implementierung und Betrieb von Informationssystemen.

6.4.1 Informationssicherheitsziele

Die Informationssicherheitsziele der OS sind Teil der Unternehmensziele und in der BSC in den Prozess-, Kunden- und Mitarbeiterperspektiven der OS dokumentiert

Die Nutzung des Potenzials eines funktionierenden Informationssicherheitsmanagementsystems als Bestandteil des IMS ist eine wichtige Aufgabe zur Erhaltung der Wettbewerbsfähigkeit und unterstützt damit die strategischen Ziele der OS (s.a. BSC Ziel 13).

Das Unternehmen hat festgelegt und in einer Anlage zu diesem Managementhandbuch dokumentiert, welche externen und internen Angelegenheiten für seinen Zweck relevant sind und sich auf seine Fähigkeit auswirken, um die beabsichtigten Ergebnisse seines Informationssicherheitsmanagementsystems (ISMS) zu erreichen. Diese Anforderungen fließen in die Informationssicherheitsziele ein. Die Ermittlung dieser Angelegenheiten bezieht sich auf die Festlegung des externen und internen Kontexts des Unternehmens.

Seitens der Unternehmensleitung wurde definiert:

a) welche interessierten Parteien im Hinblick auf das ISMS relevant sind; und

b) welche Anforderungen diese interessierten Parteien in Bezug auf die Informationssicherheit haben können.

c) die Schnittstellen und Abhängigkeitsverhältnisse zwischen den Tätigkeiten, die von der Organisation selbst durchgeführt werden, und den Tätigkeiten anderer Organisationen.

Diese Anforderungen wurden auch bei der Festlegung des Geltungsbereiches berücksichtigt.

S.a. Anhang „Interessierte Parteien".

Daraus ergibt sich die Notwendigkeit, dass während des gesamten Lebenszyklus der IT-Dienstleistungen Maßnahmen für den Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen durchzuführen sind.

Ziel der OS ist es, sämtliche Informationen bezogen auf ihren Schutzbedarf in angemessenem Maß zu schützen. Angemessen bedeutet dabei, dass die Gesamtheit der Maßnahmen zum Schutz der Informationen gemessen an ihrem Schutzbedarf nach wirtschaftlichen Gesichtspunkten auszurichten sind.

Um Art und Umfang der Maßnahmen zum Schutz der Informationen festzulegen, ist es notwendig, den Schutzbedarf und die Risiken festzustellen. Dafür wendet die OS ein erprobtes Verfahren an, welches in der Richtlinie Werteverwaltung & Risikobehandlung beschrieben ist. Dabei erfolgt eine Abstimmung der aktuellen Risikolage mit den Informationssicherheitszielen.

Ergänzend zum Verfahren der Schutzbedarfs- und Risikoanalyse sind Aktivitäten im Rahmen des IT-Continuity Managements definiert, die beim Eintritt von schwerwiegenden Betriebsstörungen wirksam werden.

6.4.2 Leitsätze zur Informationssicherheit

Das Verhalten aller Mitarbeiterinnen und Mitarbeiter der OS orientiert sich für den Bereich der Informationssicherheit an folgenden Leitsätzen:

- Jeder, der Informationen nutzt, ist im Rahmen der unternehmensseitigen Vorgaben für deren Sicherheit verantwortlich.
- Jede Information muss bei der Erstellung im Rahmen der unternehmensseitigen Vorgaben klassifiziert werden.
- Jede schützenswerte Information muss gesichert werden.
- Nur eindeutig ausgewiesene Personen mit entsprechender Befugnis erhalten Zutritt und Zugang zu sowie Zugriff auf schützenswerte Informationen.
- Ein Zugriff auf Informationen muss je nach Geschäftszweck verbindlichen Charakter besitzen, so dass Maßnahmen zur Identifikation, Nachvollziehbarkeit und Unabstreitbarkeit von Zutritten, Zugängen und Zugriffen erforderlich werden können.

Die Umsetzung der Leitbilder erfordert ein hohes Maß an Sicherheitsbewusstsein. Die Geschäftsleitung, Führungskräfte und die Informationssicherheitsorganisation fördern aktiv Maßnahmen, um den Mitarbeiterinnen und Mitarbeitern bewusst zu machen, was die Informationssicherheit für das Unternehmen und seinen Kunden bedeutet. Dabei ist Sicherheitsbewusstsein durch folgendes Verhalten gekennzeichnet:

- Erkennen, dass eine effektive Informationssicherheit ein wesentliches Element der Unternehmensphilosophie ist.
- Stets vorhandenes Sicherheitsbewusstsein bei der Verrichtung aller Arbeitsabläufe.
- Persönliche Verantwortlichkeit für die Gewährleistung der Informationssicherheit in den täglichen Geschäftsabläufen wie auch bei Schadensvorfällen und in Notfallsituationen s.a. Richtlinien „Sicherheit im Personalwesen“ und „Management von Sicherheitsvorfällen“.
- Neu zu beschaffende oder zu entwickelnde Informationssysteme unterliegen den Regelungen der Richtlinie „Beschaffung und Entwicklung von Informationssystemen“.

6.5 DATENSCHUTZPOLITIK

Die Datenschutzpolitik der OS schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten. Diese Daten werden aus unterschiedlichsten Quellen erhoben, verarbeitet und genutzt und entsprechend gesetzlicher Fristen gelöscht bzw. vernichtet.

Bei der Verarbeitung von Daten ist eine Fülle von Rechtsvorschriften zu beachten. Die Nicht-Verfügbarkeit, der Verlust, die Verfälschung oder die nicht autorisierte Offenlegung auch von nur Teilen dieser Daten kann mit hohen materiellen oder auch immateriellen Schäden für die betroffene Person verbunden sein.

Geht den Schäden ein Verstoß gegen Gesetze, Richtlinien oder sonstigen Regelungen der OS voraus, werden diese vom Datenschutzbeauftragten bearbeitet und bei Bedarf an die zuständige Aufsichtsbehörde gemeldet. Deshalb ist es erforderlich, dass diese Daten – unabhängig von der Form, in der sie vorliegen – einschließlich ihrer Verarbeitungsprozesse durch geeignete technische und organisatorische Maßnahmen geschützt werden.

Erreicht wird dies durch ein angemessenes Bewusstsein bzgl. des Datenschutzes bei allen Mitarbeiterinnen und Mitarbeitern sowie einer Einbettung des Datenschutzes in die Geschäftsprozesse, in den Aufbau von Infrastruktur und in Entwicklung, Implementierung und Betrieb von Informationssystemen.

S.a. Richtlinie „Datenschutz in der OS“

6.5.1 Datenschutzziele

Die Datenschutzziele der OS sind:

- Integrität (Unversehrtheit)
- Verfügbarkeit (Ordnungsmäßigkeit und zeitgerechter Zugriff auf personenbezogene oder personenbeziehbare Daten)
- Vertraulichkeit
- Aktualität
- Richtigkeit
- Rechtssicherheit
- Authentizität
- Transparenz
- Zweckbindung

Die für den Bereich Datenschutz festgelegten Schutzziele finden sich teilweise in der Informationssicherheit wieder.

6.5.2 Leitsätze zum Datenschutz

Das Verhalten aller Mitarbeiterinnen und Mitarbeiter der OS orientiert sich für den Bereich des Datenschutzes an folgenden Leitsätzen:

- Die Verantwortung für die Einhaltung und Umsetzung der gesetzlichen Anforderungen innerhalb der OS zum Datenschutz obliegt den Verantwortlichen der Organisation (Geschäftsführung)
- Jeder, der personenbezogene oder personenbeziehbare Daten im Sinne des Artikels 4 DS-GVO erhebt, verarbeitet und nutzt, ist im Rahmen der unternehmensseitigen Vorgaben für deren Schutz verantwortlich.
- Personenbezogene oder personenbeziehbare Daten sind immer mindestens als „Vertraulich“ zu klassifizieren und im Rahmen der Verarbeitung zu kennzeichnen.
- Nach Ablauf des Verarbeitungszweck oder Ablauf von vorgeschriebenen Aufbewahrungspflichten sind personenbezogene oder personenbeziehbare Daten rechtskonform zu löschen bzw. zu vernichten.
- Nur eindeutig ausgewiesene Personen mit entsprechender Befugnis erhalten Zutritt und Zugang zu sowie Zugriff auf personenbezogene oder personenbeziehbare Daten.

- Der Zugang und Zugriff bzw. die Möglichkeit zur Erhebung, Verarbeitung und Nutzung von personenbezogenen oder personenbeziehbaren erfolgt auf Grundlage eines aufgabenabhängigen Rollen- und Berechtigungskonzepts
- Die Umsetzung der Leitbilder erfordert ein hohes Maß an Datenschutzbewusstsein. Die Geschäftsleitung, Führungskräfte und die Datenschutzorganisation fördern aktiv Maßnahmen, um den Mitarbeiterinnen und Mitarbeitern bewusst zu machen, was Datenschutz für die betroffenen Personen bedeutet. Dabei ist Datenschutzbewusstsein durch folgendes Verhalten gekennzeichnet:
  - Erkennen, dass effektiver Datenschutz ein wesentliches Element der Unternehmensphilosophie ist.
  - Stets vorhandenes Datenschutzbewusstsein bei der Verrichtung aller Arbeitsabläufe.
  - Persönliche Verantwortlichkeit für die Gewährleistung die Einhaltung des Datenschutzes in den täglichen Geschäftsabläufen wie auch bei Schadensvorfällen und in Notfallsituationen s.a. Richtlinien „Sicherheit im Personalwesen" und „Management von Sicherheitsvorfällen".

6.6 PROZESSMANAGEMENT

Alle relevanten Geschäftsprozesse sind in einem konsolidierten Geschäftsprozess-Modell, dem pQMS, dargestellt. In mehreren Prozessebenen werden sämtliche Geschäftsaktivitäten der OS in Form von zusammenhängenden Wertschöpfungsketten und Prozessdarstellungen beschrieben.

Es wird sichergestellt, dass die Prozesse unter beherrschbaren Bedingungen ablaufen. Dies wird erreicht durch

- die Benennung von Rollen und Verantwortlichkeiten
- die im pQMS festgelegte Art und Weise der Prozess- bzw. Tätigkeitsdurchführung,
- die Erfüllung relevanter Gesetze und Normen sowie des Regelwerks der OS.

Alle erforderlichen kunden- und unternehmensrelevanten, sowie wiederkehrenden Aufgaben und Aktivitäten der Leistungserbringung sind beschrieben und dargestellt.

Die Verantwortung für die Effektivität und die Effizienz der Prozesse obliegt dem Process Owner (PO) s.a. 6.2.7.

6.6.1 Prozessmodell (pQMS)

Die Prozesse des IMS berücksichtigen die Anforderungen relevanter Gesetze und Normen sowie des Regelwerks der OS. Auf dieser Basis wurden die grundlegenden Prozesse der OS modelliert. Das pQMS der OS wird fortlaufend angepasst und weiterentwickelt. Kundenspezifische Ausprägungen von Prozessen können in Abstimmung mit dem QMB außerhalb des pQMS dargestellt werden.

6.6.2 Ausgegliederte Prozesse

Ausgegliederte Prozesse werden bezüglich ihrer Leistungserbringung gesteuert und überwacht. Im pQMS sind die ausgegliederten Prozesse farblich hervorgehoben.

6.7 MANAGEMENT VON RISIKEN

6.7.1 Schutzbedarf

Jedes Sicherheitskriterium kann einen von mehreren Werten annehmen, der den Schutzbedarf auf das jeweilige Kriterium beschreibt. Die Metriken der einzelnen Sicherheitskriterien werden als Verfügbarkeits-, Vertraulichkeits- und Integritätsstufe bezeichnet. Die Vertraulichkeitsstufe unterscheidet z. B. die Werte "öffentlich", "intern", "vertraulich" und "geheim". Der Schutzbedarf einer Information ist entsprechend durch ein Quadrupel von Schutzbedarfswerten gekennzeichnet. Die Ermittlung des Schutzbedarfs erfolgt durch ein Bewertungsverfahren.

S.a. Richtlinie „Werteverwaltung und Risikobehandlung" und „Dokumentenhandbuch".

6.7.2 Sicherheitsverfahren

Sicherheitsverfahren sind funktionale Abläufe, die entscheidend dazu beitragen, dem Schutzbedarf einer Information bzw. der in der Informationsverarbeitung involvierten Systeme zu entsprechen. Zur Gewährleistung der Informationssicherheit sind folgende Sicherheitsverfahren anzuwenden:

- Autorisierung: Der Zutritt zu Räumen, der Zugang zu Anwendungen und der Zugriff auf Informationen ist nur Befugten respektive deren digitalen Identitäten zu gewähren und auf den für die Tätigkeit notwendigen Umfang zu beschränken.
- Authentisierung: Die eindeutige Identifikation von Befugten bzw. deren digitalen Identitäten und die Prüfung der Autorisierung bei Zutritten zu Räumen, bei Zugängen zu Anwendungen und beim Zugriff auf Informationen ist sicherzustellen.
- Protokollierung: Protokollierung ist die Aufzeichnung der Authentisierung bei Zutritt zu Räumen, Zugang zu Anwendungen und Zugriff auf Informationen mit festgelegten Merkmalen, um im Nachhinein die Verbindlichkeit von Zutritten, Zugängen und Zugriffen zu ermöglichen.
- Auditierung: Die Maßnahmen der Autorisierung, Authentisierung und Protokollierung sind auf Effizienz und Effektivität zu überprüfen

S.a. Richtlinien „Beschaffung und Entwicklung von Informationssystemen", „Physische und infrastrukturelle Sicherheit", „Benutzer- und Berechtigungsmanagement" und „Sicherer Betrieb von Informationssystemen".

Die Positionierung als ICT-Dienstleister verlangt, dass die Informationsverarbeitung in der OS ein hohes Maß an Vertrauenswürdigkeit aufweist. Das Vertrauen der Mitarbeiterinnen und Mitarbeiter, Gesellschafter und Kunden in eine sichere Informationsverarbeitung gründet sich auf der Art und Weise, wie die Aspekte der Informationssicherheit bei Ausführung der Dienstleistungen berücksichtigt werden. Um ein möglichst hohes Maß an Vertrauenswürdigkeit zu erzielen, ist die Informationssicherheit durch einen mehrstufigen Schutzansatz realisiert. Dieser Schutzansatz sieht zwei komplementäre Ansätze vor:

- Proaktiver Schutz

Zunächst wirkt der proaktive Schutz, indem Sicherheitsmaßnahmen im baulichen, technischen, organisatorischen und personellen Bereich festgelegt und umgesetzt werden, um unter Beachtung der Kosten-/Nutzen-Relation das Risiko des Eintretens von Sicherheitsvorfällen möglichst zu minimieren. Der proaktive Schutz ist zweistufig realisiert. Neben einem unternehmensweiten Grundschutz zur Gewährleistung der niedrigen und mittleren Schutzbedürfnisse dient der Individualschutz zur Absicherung des hohen und sehr hohen Schutzbedarfs.

S.a. Richtlinie „Physische und infrastrukturelle Sicherheit“ und „Management von Sicherheitsvorfällen“.

- Reaktiver Schutz

Die Restrisiken des proaktiven Schutzes werden durch die Betriebs- bzw. Notfallorganisation kompensiert. Im Notfallschutz sind Verfahren definiert und ergänzende Vorkehrungen getroffen, die im Falle eines Sicherheitsvorfalls dazu dienen, den Schadensvorfall und die evtl. Notfallsituation beherrschen zu können.

Die Dualität des proaktiven und reaktiven Schutzes wird durch eine enge Kopplung und Harmonisierung der deklarativen und operativen Vorgaben aus dem Sicherheits- bzw. Notfallmanagement erzielt.

S.a. Richtlinie „Aufrechterhaltung des Geschäftsbetriebs“.

6.7.3 Individualschutz

Für hohen und sehr hohen Schutzbedarf ist die Umsetzung von individuellen Sicherheitsmaßnahmen notwendig, um das verbleibende Restrisiko auf ein akzeptables Niveau zu senken. Diese Maßnahmen werden in einem Sicherheitskonzept dokumentiert und der Nachweis über die Wirksamkeit erbracht.

S.a. Richtlinie „Werteverwaltung und Risikobehandlung“.

6.7.4 Notfallschutz

Der Notfallschutz wird nach Eintritt eines notfallauslösenden Ereignisses aktiviert. Dazu sind alle erforderlichen Informationen, Handlungsanweisungen und Verhaltensregeln im Notfallhandbuch dokumentiert. Der Notfallschutz ist vorrangig auf die möglichst schnelle Wiederherstellung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen ausgerichtet.

S.a. Richtlinie „Aufrechterhaltung des Geschäftsbetriebs“.

6.8 AUFZEICHNUNGEN UND DOKUMENTE

6.8.1 Erstellen und Freigeben von Dokumenten

Grundsätzlich verantwortlich für die Erstellung und die inhaltliche Aktualität einer Prozessbeschreibung ist immer der Eigentümer des Prozesses (Process Owner). Die zentrale Verwaltung der Dokumentation aller Prozesse obliegt dem QMB.

Das Erstellen von prozessbegleitenden Dokumenten führen die an der Prozesserstellung bzw. -durchführung beteiligten Mitarbeiterinnen und Mitarbeitern durch. Jede Beschreibung muss den Anforderungen des Managementsystems und den Zielen des Unternehmens entsprechen. Die Einzelfreigabe von Prozessen und den begleitenden Dokumenten erfolgt gemeinsam durch den jeweiligen Process Owner und dem Process Review Team (PRT). Das PRT setzt sich zusammen aus dem QMA, dem CISO und einem QISR des einbringenden Fachbereichs. Das Process Review Team prüft gegen die Anforderungen des IMS und gewährleistet, dass die Prozesse gleichartig beschrieben sind und die Schnittstellen zu anderen betroffenen Prozessen beachtet werden.

Bei Veränderungen des Prozessmodells auf Ebene 1, also der Ebene der Prozesslandkarte, erfolgt die Freigabe immer durch die Geschäftsführung.

Die Prozesse des pQMS werden zentral verwaltet und werden im OS-Portal veröffentlicht.

6.8.2 Erstellen und Freigabe von Unternehmensrichtlinien

Richtlinien werden zentral über das Compliance Register gesteuert.

Die Freigabe von Richtlinien erfolgt durch die Geschäftsführung. Ausgenommen davon sind Freigaben für Unternehmensrichtlinien, die bestimmte Themenbereiche betreffen und für die durch die Geschäftsführung die Freigabe anders geregelt wurde. Das betrifft z.B. die Freigabe von Richtlinien zum IMS, welche durch das Managementteam IMS und das Kernteam IMS geprüft und zur Freigabe durch den CISO empfohlen werden s.a. 6.2.1.

6.8.3 Dokumentenmanagement

Das Management aller Dokumente ist umfänglich im Dokumentenhandbuch der OS geregelt.

6.9 FORTLAUFENDE VERBESSERUNG

Um das Auftreten von Fehlern zu vermeiden, ist die OS vorbeugend aktiv. Schulungen der Mitarbeiterinnen und Mitarbeiter, Interne Audits, Begehungen, Kundenzufriedenheitsbefragungen, Beurteilung unserer Lieferanten, Tests und das Proposal Review Board (PRB) zur Freigabe von Angeboten werden als Maßnahmen verstanden, die bei neuen bzw. veränderten Abläufen Fehlern vorbeugen. Die Ergebnisse der Vorbeugemaßnahmen fließen, soweit angemessen, in die Prozessoptimierung ein. So wurde z.B. die Maßnahmenverfolgung hochpriorisierter Themen durch die Geschäftsführung in Form einer speziellen To-Do-Liste umgesetzt, die täglich verfolgt und getrackt wird.

Spezielle Maßnahmen werden als Projekt geplant und umgesetzt, wenn dies aufgrund ihres Ausmaßes angemessen erscheint. Initiator ist i.d.R. die Geschäftsführung, welche die Verantwortlichen festlegt und Projektkompetenzen zuordnet. Die Projektaktivitäten werden nach den Regeln des Projektmanagements durchgeführt. Interne Projekte werden wie externe gehandhabt.

Die Beurteilung unserer Leistungen und des IMS basieren auf der Anwendung der Informationssicherheits- und Qualitätspolitik und den daraus abgeleiteten Zielen, den Ergebnissen von Audits, Begehungen, Kundenzufriedenheitsbefragungen, Datenanalysen, Korrektur- und Vorbeugemaßnahmen sowie auf regelmäßigen Managementreviews. Aus diesen Aktivitäten werden bei Bedarf Erkenntnisse und Maßnahmen zur Verbesserung des bestehenden IMS abgeleitet und umgesetzt.

Dabei arbeiten wir stets nach der Methode:

- Plan (planen): Festlegen der Ziele und Prozesse, die zum Erzielen von Ergebnissen in Übereinstimmung mit den Kundenanforderungen und der Politik der Organisation notwendig sind.
- Do (durchführen): Verwirklichen der Prozesse.
- Check (prüfen): Überwachen und Messen von Prozessen und Produkten anhand der Politik, Ziele und Anforderungen an das Produkt, sowie Berichten der Ergebnisse.
- Act (handeln): Ergreifen von Maßnahmen zur ständigen Verbesserung der Prozessleistung.

6.10 BEWERTUNG DES INTEGRIERTEN MANAGEMENTSYSTEMS

Die Prozesse und das Einhalten geltender Gesetze, Normen und des Regelwerks der OS müssen bezogen auf die sich ständig verändernden Rahmenbedingungen auf die Aktualität und die Zweckmäßigkeit der Inhalte fortlaufend überwacht und ggf. angepasst bzw. umgesetzt werden. Aus diesem Grund werden zur Beurteilung des Managementsystems in festgelegten Abständen interne Audits durchgeführt. Die Durchführung von internen Audits wird vom QMA der OS gesteuert. Sie finden einmal jährlich an den

Standorten der OS statt. Ziel ist es, die Prozesse auf Konformität gegenüber den Kundenanforderungen, Rechtsvorschriften und dem IMS und auf Verbesserungspotentiale hin zu untersuchen. Die Audit-Ergebnisse werden im OS-Portal und dem MTIMS zur Verfügung gestellt und im Rahmen eines Managementreviews und der Prozessentwicklung ausgewertet und berücksichtigt.

S.a. Richtlinie „Einhaltung und Überwachung von Vorgaben".

6.10.1 Managementreview

Die Managementreviews orientieren sich an den Anforderungen der ISO9001, ISO27001 und DV-GVO und berücksichtigen die vorgegebenen Unternehmensziele und benutzen u.a. folgende Berichte und Informationsquellen als Basis:

- Berichte über interne Audits
- Berichte über Begehungen
- Berichte über Kundenzufriedenheitsbefragungen
- Berichte zu Sicherheitsvorfällen
- Ergebnisse der Risikoeinschätzung und Status des Plans für die Risikobehandlung

Die Managementreviews werden mindestens einmal im Kalenderjahr und bei besonderem Bedarf durchgeführt. Einzelne Eingaben zur Bewertung können unterjährig separat behandelt werden.

Die Ergebnisse der Managementreviews und die notwendigen Maßnahmen werden mit den Verantwortlichen der jeweiligen Organisationseinheiten und den Process Ownern abgestimmt, eingeplant und umgesetzt. Die Ergebnisse der Maßnahmenumsetzung werden im darauf folgenden Managementreview erneut bewertet. Damit ist der fortlaufende Verbesserungsprozess gemäß dem Prinzip Plan-Do-Check-Act sichergestellt.

Anhang: Interessierte Parteien

7 VERPFLICHTUNGSERKLÄRUNG ZUM INTEGRIERTEN MANAGEMENTSYSTEM

Bezogen auf das Integrierte Managementsystem der operational services GmbH & Co. KG übt die Geschäftsführung folgende Führungsaufgaben aus:

- Definition und Überprüfung von Zielen,
- Definition und Einhaltung unternehmensweiter Regelungen und Regelwerke,
- Bereitstellung für das Integrierten Managementsystems erforderlicher Ressourcen,
- Schaffung geeigneter Arbeitsbedingungen, Ausstattung und Hilfsmittel sowie
- unternehmensweites Sicherstellen der Einhaltung gesetzlicher Forderungen.

Die Geschäftsführung formuliert die Vision und die Unternehmenspolitik für die operational services GmbH & Co. KG. Die Vorgaben stehen in Übereinstimmung mit der strategischen Ausrichtung und den Grundsätzen, die durch die Gesellschafter in Gesellschaftervertrag und Gesellschaftervereinbarung vereinbart wurden.

Abgeleitet von Leitbild und Leitziel des Unternehmens formuliert die Geschäftsführung gemeinsam mit den Führungskräften die Unternehmensziele.

Mit Hilfe von Informationsveranstaltungen für die Mitarbeitenden, durch das OS-Portal, durch die direkten Vorgesetzten und weiteren Mitteln der internen Kommunikation werden die Mitarbeitenden über Strategie und Ziele und deren Bedeutung für das Unternehmen informiert. Mindestens einmal im Jahr erfolgt ein Review der Ziele durch die Geschäftsführung gemeinsam mit den Führungskräften.

Die im Management-Handbuch beschriebene Qualitäts- Informationssicherheits- und Datenschutzpolitik orientiert sich an den Unternehmenszielen und bildet die Grundlage für die Ausgestaltung des Integrierten Managementsystems.

Im Rahmen von Management-Reviews wird das Integrierte Managementsystem bewertet. Das Ergebnis der Prüfung durch die Geschäftsführung muss Entscheidungen zu Möglichkeiten für die laufende Verbesserung sowie eventuell erforderliche Änderungen am Integrierten Managementsystems beinhalten. Zur Umsetzung von Veränderungen werden die notwendigen Mittel bereitgestellt.

Mit meiner Unterschrift verpflichte ich mich zur Einhaltung und Durchsetzung des gesamten im Management-Handbuch beschriebenen bzw. referenzierten Integrierten Managementsystems, gebe es frei und bringe zum Ausdruck, dass alle darin enthaltenen Regeln und Dokumente für alle Mitarbeitenden der operational services GmbH & Co. KG gültig sind.

Frankfurt am Main im Juni 2018

Dr. Ulrich Müller	Frank Oidtmann	Sandro Tomas	Detlef Wedekind
Geschäftsführer (Sprecher)	Geschäftsführer	QMB	CISO und CO