YUSHIN-RYU AG

Organisationsreglement

Integrierte Vollfassung – Arbeitsentwurf

Abgestimmt auf den erarbeiteten Statutenentwurf der Yushin-Ryu AG

Dokumentenlenkung

Feld	Eintrag	Bemerkung
Dokument	Organisationsreglement der Yushin-Ryu AG	Internes Führungs- und Organisationsdokument
Fassung	Vollfassung Arbeitsentwurf	Ausformulierte Gesamtfassung
Schrift / Format	Arial 12 pt, Zeilenabstand 1,5, Blocksatz	gemäss Vorgabe
Geltung	nach Beschluss des Verwaltungsrates	Statuten bleiben vorrangig

Inhaltsübersicht

I. Grundlagen

Art. 1 Zweck des Organisationsreglements

Dieses Organisationsreglement regelt die interne Organisation, die Führungsstruktur, die Delegation der Geschäftsführung, die Kompetenzordnung sowie die Zusammenarbeit der Organe, Geschäftsleitungsfunktionen und Organisationseinheiten der Yushin-Ryu AG.

Es konkretisiert die Statuten organisatorisch und dient als übergeordnetes internes Führungsdokument der Gesellschaft. Es ersetzt weder die Statuten noch Spezialreglemente, sondern bildet den verbindenden Rahmen zwischen rechtlicher Grundordnung und operativer Umsetzung.

Art. 2 Geltungsbereich

Dieses Organisationsreglement gilt für die Yushin-Ryu AG sowie für alle durch sie kontrollierten Gesellschaften, Niederlassungen, Projektstrukturen, Geschäftsbereiche und organisatorischen Einheiten, soweit keine zwingenden gesetzlichen Vorschriften entgegenstehen.

Für rechtlich selbständige Einheiten gilt dieses Organisationsreglement als konzernweiter Mindeststandard, sofern die jeweilige Einheit durch die Yushin-Ryu AG geführt oder kontrolliert wird.

Art. 3 Führungsgrundsätze

Die Gesellschaft wird nach den Grundsätzen der Rechtmässigkeit, Integrität, Verantwortlichkeit, Nachvollziehbarkeit, Wirtschaftlichkeit, Qualität, Sicherheit, Nachhaltigkeit und Compliance geführt.

Jede Organisationseinheit hat ihre Aufgaben so wahrzunehmen, dass Entscheidungen dokumentiert, Verantwortlichkeiten klar zugeordnet und Risiken angemessen gesteuert werden.

Art. 4 Verhältnis zu den Statuten

Die Statuten bilden die rechtliche Grundordnung der Gesellschaft. Dieses Organisationsreglement regelt die interne organisatorische Umsetzung innerhalb des durch Statuten, Gesetz und Verwaltungsratsbeschlüsse vorgegebenen Rahmens.

Bei Widersprüchen gehen die Statuten diesem Organisationsreglement vor. Spezialreglemente dürfen diesem Organisationsreglement nicht widersprechen, ausser der Verwaltungsrat beschliesst ausdrücklich eine vorrangige Sonderregelung im zulässigen Rahmen.

Art. 5 Dokumentenhierarchie

Die interne Dokumentenhierarchie dient der Klarheit und Nachvollziehbarkeit. Sie legt fest, welche Regelungen im Konfliktfall Vorrang haben.

16. Zwingendes Recht
17. Statuten
18. Organisationsreglement
19. Spezialreglemente
20. Verwaltungsratsbeschlüsse
21. Geschäftsleitungsbeschlüsse
22. Prozessbeschreibungen und Arbeitsanweisungen

II. Führungs- und Organisationsstruktur

Art. 6 Oberste Führung

Die strategische Führung der Gesellschaft obliegt dem Verwaltungsrat. Der Verwaltungsrat legt die Grundausrichtung, die Führungsstruktur, die wesentlichen Governance-Standards sowie die übergeordneten Kontrollmechanismen fest.

Die operative Führung erfolgt durch die Geschäftsleitung im Rahmen der ihr übertragenen Kompetenzen.

Art. 7 Verwaltungsrat

Der Verwaltungsrat ist das oberste Leitungs- und Verwaltungsorgan der Gesellschaft. Er erlässt dieses Organisationsreglement und genehmigt wesentliche Änderungen der Organisationsstruktur.

Der Verwaltungsrat kann die Geschäftsführung ganz oder teilweise delegieren, soweit dies nach den Statuten und dem geltenden Recht zulässig ist. Die Delegation wird durch dieses Organisationsreglement, Spezialreglemente, Stellenbeschriebe oder Einzelbeschlüsse konkretisiert.

Art. 8 Geschäftsleitung

Die Geschäftsleitung führt die laufenden Geschäfte der Gesellschaft. Sie setzt die strategischen Vorgaben des Verwaltungsrates um und stellt die operative Koordination der Geschäftsbereiche sicher.

Die Geschäftsleitung ist für eine geordnete Berichterstattung, eine angemessene interne Kontrolle, die Umsetzung von Compliance-Anforderungen sowie die Einhaltung der internen Reglemente verantwortlich.

Art. 9 Organigramm

Das Organigramm bildet die organisatorische Struktur der Gesellschaft ab. Es zeigt die wesentlichen Berichtslinien, Führungsbereiche und funktionalen Zuordnungen.

Das Organigramm wird durch den Verwaltungsrat genehmigt und bei wesentlichen organisatorischen Änderungen angepasst.

Art. 10 Fachgremien

Zur fachlichen Unterstützung können beratende oder operative Gremien eingesetzt werden. Hierzu gehören insbesondere Wissenschaftsrat, Universitätsrat, Akademische Leitung, Dekanat, Stiftungs- oder Projektgremien sowie weitere vom Verwaltungsrat eingesetzte Fachgremien.

Beratende Gremien besitzen keine Organstellung, sofern ihnen diese nicht ausdrücklich durch Statuten, Verwaltungsratsbeschluss oder separates Reglement zugewiesen wird.

III. Geschäftsleitung und C-Level-Funktionen

Art. 11 Grundsatz der C-Level-Struktur

Die Gesellschaft kann C-Level-Funktionen einrichten, soweit dies für Führung, Kontrolle, Skalierung, Sicherheit, Qualität und operative Steuerung erforderlich ist.

Jede C-Level-Funktion handelt innerhalb der übertragenen Aufgaben und Kompetenzen. Aufgaben, Stellvertretung, Budget- und Entscheidungsbefugnisse können in einem separaten Funktions- und Kompetenzreglement präzisiert werden.

Art. 12 CVO – Chief Visionary Officer

Der CVO verantwortet Vision, langfristige strategische Ausrichtung, Identitätslinie, Innovationsentwicklung und strategische Zukunftsfragen der Gesellschaft. Er wirkt an der Grundausrichtung der Gruppe, an wesentlichen Partnerschaften und an der kulturellen und konzeptionellen Entwicklung mit.

Art. 13 CEO – Chief Executive Officer

Der CEO verantwortet die operative Gesamtführung der Gesellschaft. Er koordiniert die Geschäftsleitung, setzt die strategischen Vorgaben des Verwaltungsrates um und sorgt für eine geordnete operative Steuerung.

Art. 14 VCEO – Vice Chief Executive Officer

Der VCEO unterstützt und vertritt den CEO im Rahmen der übertragenen Kompetenzen. Umfang, Stellvertretung und Entscheidungsbefugnisse werden durch Verwaltungsratsbeschluss oder Kompetenzreglement festgelegt.

Art. 15 CFO – Chief Financial Officer

Der CFO verantwortet Finanzplanung, Budgetierung, Liquidität, Controlling, Finanzierung, Rechnungswesen, Steuern und finanzielle Berichterstattung. Er stellt sicher, dass finanzielle Entscheidungen dokumentiert und kontrolliert erfolgen.

Art. 16 COO – Chief Operating Officer

Der COO verantwortet operative Prozesse, Betriebsorganisation, Ressourceneinsatz, Standortkoordination und Umsetzung operativer Standards. Er stellt die funktionsfähige Durchführung der laufenden Tätigkeiten sicher.

Art. 17 CTO – Chief Technology Officer

Der CTO verantwortet Technologieentwicklung, technische Roadmaps, technische Infrastruktur, Labor- und Entwicklungsstandards sowie die Koordination technischer Projekte.

Art. 18 CIO – Chief Information Officer

Der CIO verantwortet IT-Strategie, IT-Infrastruktur, digitale Systeme, Backup-Strukturen, Disaster-Recovery-Anforderungen und die technische Unterstützung digitaler Geschäftsprozesse.

Art. 19 CISO – Chief Information Security Officer

Der CISO verantwortet Informationssicherheit, Cybersecurity, digitale Schutzkonzepte, Sicherheitsüberwachung, technische Zugriffssicherung und Sicherheitsprüfungen im digitalen Bereich.

Art. 20 CSO – Chief Security Officer

Der CSO verantwortet die physische, organisatorische und betriebliche Sicherheit der Gesellschaft. Dazu gehören Werkschutz, Objektschutz, Zutritts- und Zugangskontrollen, Besucher- und Lieferantenmanagement, Sicherheitskontrollen, Prävention gegen Sabotage, Diebstahl und Wirtschaftsspionage, Sicherheitsorganisation von Hochrisikobereichen, Zusammenarbeit mit Behörden und Einsatzorganisationen sowie die Koordination der Werkfeuerwehr. Der CSO arbeitet eng mit dem CISO zusammen, insbesondere an Schnittstellen zwischen physischer Sicherheit und Cybersecurity.

Art. 21 CDO – Chief Data Officer

Der CDO verantwortet Datenstrategie, Datenqualität, Datenmodelle, Datenarchitektur und Daten-Governance. Er wirkt an der rechtmässigen, sicheren und zweckgebundenen Nutzung von Daten mit.

Art. 22 CQMO – Chief Quality Management Officer

Der CQMO verantwortet Qualitätsmanagement, Audits, Dokumentenlenkung, Managementsysteme, kontinuierliche Verbesserung und akkreditierungsbezogene Qualitätssicherung.

Art. 23 CHRO – Chief Human Resources Officer

Der CHRO verantwortet Personalstrategie, Recruiting, Personalentwicklung, Nachfolgeplanung, Führungskultur, arbeitsbezogene Standards und die Umsetzung des Personalreglements.

Art. 24 CCO – Chief Communications Officer

Der CCO verantwortet interne und externe Kommunikation, Kommunikationsstrategie, Stakeholder-Kommunikation, Reputationsmanagement, Krisenkommunikation und die Koordination öffentlicher Aussagen.

Art. 25 CMO – Chief Marketing Officer

Der CMO verantwortet Marketingstrategie, Markenführung, Kampagnen, Marktanalyse und Positionierung der Gesellschaft.

Art. 26 CSO-Sales – Chief Sales Officer

Der Chief Sales Officer verantwortet Vertrieb, Kundengewinnung, Key Accounts, Umsatzplanung und vertriebsbezogene Geschäftsentwicklung. Zur Vermeidung von Verwechslungen mit dem Chief Security Officer kann intern die Bezeichnung CSO-Sales verwendet werden.

Art. 27 CMSO – Chief Marketing / Sales / Services Officer

Der CMSO kann für kombinierte Marketing-, Vertriebs- und Servicefunktionen eingesetzt werden, sofern diese Bündelung organisatorisch zweckmässig ist.

Art. 28 CRO – Chief Risk Officer

Der CRO verantwortet Risikomanagement, Risikoanalysen, Risikoberichterstattung, Notfallplanung und Business-Continuity-Schnittstellen.

Art. 29 CLO – Chief Legal Officer

Der CLO verantwortet Recht, Verträge, Gesellschaftsrecht, Datenschutzschnittstellen, Immaterialgüterrecht, externe Anwälte und rechtliche Risikobewertung.

Art. 30 CLO Learning – Chief Learning Officer

Der CLO Learning verantwortet Lernarchitektur, Weiterbildung, Curricula, Ausbildungsqualität und lernbezogene Standards.

Art. 31 CKO – Chief Knowledge Officer

Der CKO verantwortet Wissensmanagement, Archive, Dokumentation, Wissenstransfer und langfristige Sicherung von Organisationswissen.

Art. 32 CAO – Chief Administrative Officer

Der CAO verantwortet Administration, interne Verwaltung, Büroorganisation, administrative Standards und bereichsübergreifende Koordination administrativer Abläufe.

Art. 33 CHO – Chief Health / Human Care Officer

Der CHO kann für gesundheits-, betreuungs-, pflege- oder care-bezogene Aufgaben eingesetzt werden. Die konkrete Ausgestaltung erfolgt durch Funktionsbeschrieb oder Spezialreglement.

Art. 34 Public Affairs und Medienkommunikation

Die Gesellschaft kann eine Funktion Director Public Affairs & Media Relations oder eine gleichwertige Kommunikationsfunktion einrichten.

Diese Funktion unterstützt den CCO bei Medienarbeit, Pressekommunikation, öffentlicher Positionierung, Reputationsmanagement, Krisenkommunikation und Koordination externer Stellungnahmen.

Art. 35 Stellvertretung der C-Level-Funktionen

Für wesentliche C-Level-Funktionen sind geeignete Stellvertretungen zu bestimmen. Eine Stellvertretung übernimmt nur jene Kompetenzen, die ihr ausdrücklich übertragen wurden.

Bei sicherheits-, finanz-, qualitäts- oder krisenrelevanten Funktionen ist die Stellvertretung so zu organisieren, dass kritische Prozesse auch bei Ausfall einer Schlüsselperson handlungsfähig bleiben.

IV. Operative Organisation und Geschäftsbereiche

Art. 36 Operative Geschäftsbereiche

Die Gesellschaft gliedert ihre Tätigkeiten in operative Geschäftsbereiche. Jeder Geschäftsbereich besitzt eine definierte Aufgabenbeschreibung, Führung, Budgetverantwortung und Berichtslinie.

Die organisatorische Zuordnung wird durch Verwaltungsrat, Geschäftsleitung oder Organigramm festgelegt.

Art. 37 Mögliche Geschäftsbereiche

Die Gesellschaft kann insbesondere Geschäftsbereiche für Bildung, Wissenschaft, Universität, Forschung und Entwicklung, Medizin und Gesundheit, Projektmanagement, Produktion, Dienstleistungen, Immobilien und Infrastruktur, Energie, Umwelttechnik, IT, Sicherheit, Logistik und Transport, Stiftungen und gemeinnützige Projekte sowie weitere Aufgabenfelder führen.

Die konkrete Ausgestaltung richtet sich nach Strategie, Ressourcen und Verwaltungsratsbeschlüssen.

Art. 38 Bereichsleitungen

Jeder Geschäftsbereich wird durch eine Bereichsleitung geführt. Diese trägt Verantwortung für Zielerreichung, Budgeteinhaltung, Personalführung, Qualität, Sicherheit, Berichtswesen und kontinuierliche Verbesserung.

Bereichsleitungen handeln innerhalb ihrer übertragenen Kompetenzen und berichten an die zuständige Geschäftsleitungsfunktion.

Art. 39 Projektorganisation

Für bereichsübergreifende oder zeitlich befristete Vorhaben können Projekte eingerichtet werden.

Für jedes Projekt sind Projektauftrag, Projektleitung, Stellvertretung, Budget, Meilensteine, Risiken, Berichtswege, Dokumentation und Abschluss schriftlich festzulegen.

Art. 40 Projektfreigaben

Projekte mit erhöhter finanzieller, rechtlicher, sicherheitsrelevanter, reputationsbezogener oder strategischer Bedeutung bedürfen einer ausdrücklichen Freigabe durch die zuständige Stelle.

Details zu Projektfreigaben werden im Kompetenzreglement, Finanzreglement oder Projektmanagementreglement geregelt.

V. Tochtergesellschaften, internationale Standorte und zellulares System

Art. 41 Tochtergesellschaften

Tochtergesellschaften werden organisatorisch in die Konzernstruktur eingebunden. Sie verfügen über eine definierte Leitung, Berichtsstruktur, Finanzverantwortung, Compliance-Struktur, Risikobewertung und Qualitätssicherung.

Die rechtliche Selbständigkeit einer Tochtergesellschaft bleibt unberührt; konzernweite Mindeststandards sind einzuhalten, soweit keine zwingenden lokalen Vorschriften entgegenstehen.

Art. 42 Internationale Standorte

Internationale Standorte, Niederlassungen und lokale Einheiten beachten die jeweils anwendbaren lokalen Rechtsvorschriften.

Die von der Yushin-Ryu AG festgelegten Mindeststandards in Governance, Qualität, Sicherheit, Datenschutz, Compliance und Berichterstattung dürfen nicht unterschritten werden.

Art. 43 Zellulares System

Die internationale Entwicklung der Gesellschaft folgt dem Grundsatz eines zellularen Systems. Jede operative Einheit soll lokal funktionsfähig sein, bleibt aber über Strategie, Governance, Standards, Reporting und Qualitätssicherung mit der Holding verbunden.

Dieses Prinzip dient Skalierbarkeit, Redundanz, Resilienz und Nachvollziehbarkeit.

Art. 44 Mindestbestandteile operativer Einheiten

Jede operative Einheit benötigt eine definierte Leitung, Aufgabenbeschreibung, Finanz- und Ressourcenplanung, Compliance-Verantwortung, Risiko- und Sicherheitsbewertung, Qualitätsanforderungen und Berichtssystem.

Details werden je nach Einheit durch Mandat, Projektauftrag, Geschäftsplan oder Spezialreglement geregelt.

Art. 45 Redundanzprinzip

Kritische Funktionen, Systeme und Prozesse sind angemessen redundant zu planen. Dies betrifft insbesondere Finanzen, IT, Daten, Forschung, Infrastruktur, Sicherheit, Qualitätsmanagement, Krisenkommunikation und Hochrisikobereiche.

Die konkrete Redundanz wird nach Risiko, Kritikalität und Standortanforderung festgelegt.

VI. Kompetenzordnung, Zeichnung und Entscheidungen

Art. 46 Grundsatz der Kompetenzbindung

Jede Person handelt ausschliesslich innerhalb der ihr übertragenen Kompetenzen. Mündliche Absprachen ersetzen keine schriftliche Kompetenzzuweisung, soweit es um finanzielle, rechtliche, strategische oder sicherheitsrelevante Entscheidungen geht.

Art. 47 Kompetenzübertragung

Kompetenzen werden schriftlich übertragen. Sie können dauerhaft, befristet, projektbezogen oder auf bestimmte Betrags- und Risikogrenzen beschränkt sein.

Die Einzelheiten werden im Kompetenzreglement geregelt.

Art. 48 Finanzkompetenzen

Finanzielle Entscheidungsbefugnisse richten sich nach dem Finanzreglement und den Beschlüssen des Verwaltungsrates.

Finanzielle Verpflichtungen sind nach Betrag, Laufzeit, Risiko, strategischer Bedeutung und Gegenpartei zu klassifizieren.

Art. 49 Zeichnungsberechtigung

Die externe Zeichnungsberechtigung wird durch den Verwaltungsrat festgelegt. Interne Kompetenz und externe Zeichnungsberechtigung sind zu unterscheiden.

Einträge im Handelsregister richten sich nach den gesetzlichen und registerrechtlichen Vorgaben.

Art. 50 Interessenkonflikte

Interessenkonflikte sind unverzüglich offenzulegen. Betroffene Personen nehmen an Beratung und Beschlussfassung nur teil, soweit dies zulässig und vom zuständigen Organ genehmigt ist.

Art. 51 Dokumentationspflicht bei Entscheidungen

Wesentliche Entscheidungen sind nachvollziehbar zu dokumentieren. Die Dokumentation enthält insbesondere Gegenstand, Zuständigkeit, Entscheidungsgrundlage, Beschluss, Verantwortlichkeiten, Fristen und allfällige Vorbehalte.

VII. Qualitätsmanagement und Dokumentenlenkung

Art. 52 Qualitätsgrundsatz

Die Gesellschaft betreibt ein integriertes Qualitätsmanagementsystem. Dieses dient der Standardisierung, Nachvollziehbarkeit, kontinuierlichen Verbesserung, Auditfähigkeit und langfristigen Organisationsentwicklung.

Art. 53 Verantwortung des CQMO

Der CQMO koordiniert das Qualitätsmanagement der Gesellschaft. Die operative Verantwortung für die Umsetzung der Qualitätsanforderungen verbleibt bei den jeweiligen Führungskräften und Organisationseinheiten.

Art. 54 Dokumentenlenkung

Sämtliche verbindlichen Dokumente unterliegen einer geregelten Dokumentenlenkung. Dokumente sind eindeutig zu kennzeichnen, zu versionieren, freizugeben, zu archivieren und regelmässig auf Aktualität zu überprüfen.

Änderungen an verbindlichen Dokumenten müssen nachvollziehbar dokumentiert werden.

Art. 55 Audits

Interne Audits werden regelmässig durchgeführt. Der Verwaltungsrat oder die Geschäftsleitung können externe Audits, Sonderprüfungen oder Review-Verfahren anordnen.

Auditergebnisse sind zu dokumentieren, zu bewerten und in Massnahmenpläne zu überführen.

Art. 56 Kontinuierliche Verbesserung

Verbesserungspotenziale aus Audits, Projekten, Fehleranalysen, Reklamationen, Sicherheitsmeldungen, Forschungsergebnissen und internen Vorschlägen werden systematisch bewertet und in geeignete Verbesserungsmassnahmen überführt.

VIII. Risiko-, Sicherheits- und Hochrisikomanagement

Art. 57 Risikomanagement

Die Gesellschaft betreibt ein unternehmensweites Risikomanagement zur Identifikation, Bewertung, Steuerung und Überwachung wesentlicher Risiken.

Das Risikomanagement umfasst strategische, finanzielle, operative, rechtliche, IT-, Cyber-, Forschungs-, Sicherheits-, Reputations-, Standort- und Länderrisiken.

Art. 58 Verantwortung des CRO

Der CRO koordiniert das unternehmensweite Risikomanagement und berichtet regelmässig an Geschäftsleitung und Verwaltungsrat.

Die operative Risikoerkennung bleibt Aufgabe der jeweiligen Führungskräfte und Organisationseinheiten.

Art. 59 Physische Sicherheit

Die physische Sicherheit der Gesellschaft umfasst den Schutz von Personen, Gebäuden, Anlagen, Infrastruktur, Sachwerten, Forschungseinrichtungen und sicherheitskritischen Bereichen.

Der CSO verantwortet die Sicherheitsorganisation, den Werkschutz, den Objektschutz, Zutrittskontrollen, Sicherheitsüberprüfungen, Prävention und physische Sicherheitsmassnahmen.

Art. 60 Werkschutz und Objektschutz

Der Werkschutz sichert Standorte, Gebäude, Anlagen, Zugänge und interne Sicherheitsbereiche. Objektschutzmassnahmen sind risikobasiert zu planen und regelmässig zu überprüfen.

Personal im Werkschutz ist entsprechend seiner Aufgaben auszubilden, zu dokumentieren und laufend weiterzuentwickeln.

Art. 61 Zutritts- und Zugangskontrollen

Zutritts- und Zugangskontrollen werden nach Schutzbedarf, Funktion, Sicherheitsstufe und Standortanforderung eingerichtet.

Besucher, Lieferanten und externe Dienstleister unterliegen kontrollierten Zugangsprozessen.

Art. 62 Werkfeuerwehr und interne Einsatzorganisation

Für sicherheitskritische Standorte kann die Gesellschaft eine Werkfeuerwehr oder vergleichbare interne Einsatzorganisation einrichten.

Organisation, Ausbildung, Alarmierung, Einsatzgrundsätze und Schnittstellen zu Behörden werden in einem separaten Sicherheits- oder Werkfeuerwehrreglement geregelt.

Art. 63 Hochrisikobereiche

Für Forschungs-, Labor-, Energie-, Reaktor-, radiologische, nukleartechnische oder sonstige Hochrisikobereiche können erhöhte Sicherheits-, Zutritts-, Kontroll-, Audit- und Freigabeanforderungen festgelegt werden.

Details werden in Spezialreglementen geregelt, insbesondere Sicherheitsreglement, Hochrisikobereichsreglement, Laborreglement, Notfallreglement und Krisenmanagementreglement.

Art. 64 Zusammenarbeit CSO und CISO

Der CSO und der CISO arbeiten an allen Schnittstellen zwischen physischer Sicherheit und Informations- bzw. Cybersicherheit eng zusammen.

Dies betrifft insbesondere Zutrittssysteme, Überwachungssysteme, Sicherheitsvorfälle, Sabotageprävention, kritische Infrastruktur, Wirtschaftsspionage und Hochrisikobereiche.

IX. Informationssicherheit und Geheimhaltungsstufen

Art. 65 Grundsatz der Informationssicherheit

Informationssicherheit dient dem Schutz sämtlicher Informationen, Daten, Systeme und Kommunikationsmittel der Gesellschaft.

Sie gewährleistet Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit geschäftsrelevanter Informationen.

Art. 66 Verantwortung des CISO

Der CISO verantwortet Informations- und Cybersicherheit. Er koordiniert Sicherheitskonzepte, Zugriffsschutz, Sicherheitsprüfungen, Sicherheitsüberwachung und Bearbeitung digitaler Sicherheitsvorfälle.

Der CISO arbeitet eng mit CSO, CIO, CRO, CQMO und den Bereichsleitungen zusammen.

Art. 67 Informationsklassifizierung

Alle Informationen werden entsprechend ihrem Schutzbedarf klassifiziert. Die Klassifizierung bestimmt den zulässigen Umgang mit Information, insbesondere Zugriff, Speicherung, Übermittlung, Aufbewahrung, Archivierung und Vernichtung.

Art. 68 Geheimhaltungsstufen

Stufe	Bezeichnung	Beschreibung
1	Öffentlich	Informationen ohne besonderen Schutzbedarf, deren Veröffentlichung

		zulässig ist.
2	Intern	Informationen für Mitarbeitende oder autorisierte interne Personenkreise.
3	Vertraulich	Informationen mit erhöhtem Schutzbedarf; Zugriff nur für berechtigte Personen.
4	Streng vertraulich (Eyes Only)	Informationen mit hohem Schutzbedarf; Zugriff nur für ausdrücklich benannte Personen.
5	Verschlusssache (Top Eyes Only)	Informationen mit höchstem Schutzbedarf; Zugriff nur aufgrund ausdrücklicher Freigabe mit besonderen Schutz-, Dokumentations- und Aufbewahrungspflichten.

Art. 69 Need-to-Know-Prinzip

Der Zugriff auf Informationen erfolgt ausschliesslich nach dem Need-to-Know-Prinzip. Jede Person erhält nur Zugriff auf diejenigen Informationen, die zur Erfüllung ihrer Aufgaben erforderlich sind.

Art. 70 Berechtigungsmanagement

Benutzer- und Zugriffsrechte werden dokumentiert, regelmässig überprüft und bei Funktionswechsel oder Austritt unverzüglich angepasst.

Für besonders schutzbedürftige Informationen können zusätzliche Freigaben, Protokollierungen und Kontrollmechanismen vorgesehen werden.

Art. 71 Sicherheitsvorfälle

Informations- und Sicherheitsvorfälle sind unverzüglich dem CISO oder CSO zu melden. Sicherheitsvorfälle werden dokumentiert, bewertet, bearbeitet und nach Abschluss ausgewertet.

X. Datenschutz und Datenmanagement

Art. 72 Datenschutz

Personendaten werden ausschliesslich im Rahmen der anwendbaren Datenschutzbestimmungen bearbeitet. Bearbeitungen müssen rechtmässig, zweckgebunden, verhältnismässig, sicher und nachvollziehbar erfolgen.

Art. 73 Datensicherheit

Die Gesellschaft trifft angemessene technische und organisatorische Massnahmen zum Schutz personenbezogener und geschäftskritischer Daten.

Dazu gehören insbesondere Zugriffsschutz, Verschlüsselung, Backup, Wiederherstellung, Protokollierung, Berechtigungsmanagement und sichere Archivierung.

Art. 74 Datenverantwortung

Datenverantwortlichkeiten werden nach Funktion, Prozess und System festgelegt. Der CDO, CISO, CIO und CLO arbeiten bei datenbezogenen Governance-Fragen zusammen.

XI. Compliance, interne Kontrolle und Hinweisgebersystem

Art. 75 Compliance-Grundsatz

Alle Organe, Führungskräfte, Mitarbeitenden und Beauftragten sind verpflichtet, gesetzliche Vorschriften, Statuten, dieses Organisationsreglement, Spezialreglemente und interne Weisungen einzuhalten.

Art. 76 Compliance-System

Die Gesellschaft betreibt ein Compliance-System. Dieses umfasst Rechtskonformität, interne Richtlinien, Schulungen, Kontrollen, Dokumentation, Berichterstattung und Massnahmen bei Verstössen.

Art. 77 Internes Kontrollsystem

Die Gesellschaft betreibt ein internes Kontrollsystem. Dieses umfasst organisatorische, finanzielle und funktionale Kontrollen, Vier-Augen-Prinzipien, Freigabeprozesse, Dokumentationspflichten und regelmässige Wirksamkeitsprüfungen.

Art. 78 Hinweisgebersystem

Die Gesellschaft kann ein internes Hinweisgebersystem betreiben. Hinweise werden vertraulich behandelt und nach festgelegten Verfahren geprüft.

Repressalien gegen Personen, die in gutem Glauben Hinweise geben, sind unzulässig.

Art. 79 Umgang mit Verstössen

Verstösse gegen gesetzliche Vorgaben, Statuten oder interne Reglemente werden geprüft, dokumentiert und angemessen behandelt.

Massnahmen können organisatorischer, arbeitsrechtlicher, vertraglicher, technischer oder rechtlicher Art sein.

XII. Krisenmanagement, Business Continuity und Notfallorganisation

Art. 80 Krisenorganisation

Die Gesellschaft unterhält eine Krisenorganisation zur Bewältigung aussergewöhnlicher Ereignisse. Ziel ist der Schutz von Menschen, Umwelt, Infrastruktur, Informationen, Reputation und Handlungsfähigkeit der Organisation.

Art. 81 Krisenstab

Der Verwaltungsrat oder die Geschäftsleitung können jederzeit einen Krisenstab einsetzen. Zusammensetzung, Befugnisse und Einsatzverfahren werden im Krisenmanagementreglement geregelt.

Art. 82 Business Continuity

Für kritische Geschäftsprozesse werden Business-Continuity- und Wiederanlaufkonzepte erstellt, gepflegt und regelmässig überprüft.

Die Fortführung kritischer Prozesse besitzt im Ereignisfall hohe Priorität.

Art. 83 Notfall- und Evakuierungsplanung

Für Standorte, Anlagen und Hochrisikobereiche sind angemessene Notfall-, Alarmierungs- und Evakuierungspläne zu führen.

Die Einzelheiten werden im Sicherheitsreglement, Notfallreglement und Krisenmanagementreglement geregelt.

Art. 84 Kommunikation im Krisenfall

Die externe und interne Krisenkommunikation wird durch den CCO koordiniert. Sicherheitsrelevante Inhalte werden mit CSO, CISO, CRO und Geschäftsleitung abgestimmt.

XIII. Spezialreglemente, Dokumentenhierarchie und Schlussbestimmungen

Art. 85 Grundsatz der Spezialreglemente

Dieses Organisationsreglement bildet den übergeordneten organisatorischen Rahmen. Detailregelungen werden in Spezialreglementen geführt, damit das

Organisationsreglement übersichtlich bleibt und einzelne Fachbereiche gezielt angepasst werden können.

Art. 86 Vorgesehene Spezialreglemente

Insbesondere können folgende Spezialreglemente erlassen werden:

23. Kompetenzreglement
24. Finanzreglement
25. Personalreglement
26. Führungsreglement
27. Sicherheitsreglement
28. Informationssicherheitsreglement
29. Cybersecurity-Reglement
30. Datenschutzreglement
31. Compliance-Reglement
32. Risikomanagementreglement
33. IKS-Reglement
34. Krisenmanagementreglement
35. Business-Continuity-Reglement
36. Qualitätsmanagementreglement
37. Dokumentenlenkungsreglement
38. Auditreglement
39. IT-Reglement
40. Forschungsreglement
41. Laborreglement
42. Werkfeuerwehrreglement
43. Hochrisikobereichsreglement
44. Zutritts- und Berechtigungsreglement
45. Beschaffungs- und Vergabereglement
46. Reisekosten- und Spesenreglement
47. Archivierungsreglement
48. Ausbildungs- und Weiterbildungsreglement
49. Verhaltenskodex / Code of Conduct

50. weitere durch den Verwaltungsrat beschlossene Reglemente

Art. 87 Berichtswesen

Alle Organisationseinheiten berichten entsprechend ihrer Verantwortung regelmässig an die jeweils übergeordnete Führungsebene. Berichte dienen Steuerung, Kontrolle, Entscheidungsfindung, Risikoerkennung und kontinuierlicher Verbesserung.

Art. 88 Verbindlichkeit

Dieses Organisationsreglement ist für sämtliche Organe, Führungskräfte, Mitarbeitenden, Beauftragten sowie betroffene Organisationseinheiten verbindlich, soweit es auf sie anwendbar erklärt wurde.

Art. 89 Änderungen

Änderungen dieses Organisationsreglements erfolgen durch Beschluss des Verwaltungsrates. Alle Änderungen sind zu dokumentieren, zu versionieren und den betroffenen Stellen bekanntzugeben.

Art. 90 Inkrafttreten

Dieses Organisationsreglement tritt mit Beschluss des Verwaltungsrates in Kraft. Mit Inkrafttreten ersetzt es frühere Fassungen des Organisationsreglements, soweit der Verwaltungsrat nichts anderes beschliesst.

Anhang A – Übersicht C-Level-Funktionen

Abkürzung	Funktion	Kernverantwortung
CVO	Chief Visionary Officer	Der CVO verantwortet Vision, langfristige strategische Ausrichtung, Identitätslinie, Innovationsentwicklung und strategische Zukunftsfragen der Gesellschaft. Er wirkt an der Grundausrichtung der Gruppe, an wesentlichen Partnerschaften und an der kulturellen und konzeptionellen Entwicklung mit.
CEO	Chief Executive Officer	Der CEO verantwortet die operative Gesamtführung der Gesellschaft. Er koordiniert die Geschäftsleitung, setzt die strategischen Vorgaben des Verwaltungsrates um und sorgt für eine geordnete operative Steuerung.
VCEO	Vice Chief Executive Officer	Der VCEO unterstützt und vertritt den CEO im Rahmen der übertragenen

		Kompetenzen. Umfang, Stellvertretung und Entscheidungsbefugnisse werden durch Verwaltungsratsbeschluss oder Kompetenzreglement festgelegt.
CFO	Chief Financial Officer	Der CFO verantwortet Finanzplanung, Budgetierung, Liquidität, Controlling, Finanzierung, Rechnungswesen, Steuern und finanzielle Berichterstattung. Er stellt sicher, dass finanzielle Entscheidungen dokumentiert und kontrolliert erfolgen.
COO	Chief Operating Officer	Der COO verantwortet operative Prozesse, Betriebsorganisation, Ressourceneinsatz, Standortkoordination und Umsetzung operativer Standards. Er stellt die funktionsfähige Durchführung der laufenden Tätigkeiten sicher.

CTO	Chief Technology Officer	Der CTO verantwortet Technologieentwicklung, technische Roadmaps, technische Infrastruktur, Labor- und Entwicklungsstandards sowie die Koordination technischer Projekte.
CIO	Chief Information Officer	Der CIO verantwortet IT-Strategie, IT-Infrastruktur, digitale Systeme, Backup-Strukturen, Disaster-Recovery-Anforderungen und die technische Unterstützung digitaler Geschäftsprozesse.
CISO	Chief Information Security Officer	Der CISO verantwortet Informationssicherheit, Cybersecurity, digitale Schutzkonzepte, Sicherheitsüberwachung, technische Zugriffssicherung und Sicherheitsprüfungen im digitalen Bereich.
CSO	Chief Security Officer	Der CSO verantwortet die physische, organisatorische und betriebliche Sicherheit der

		Gesellschaft. Dazu gehören Werkschutz, Objektschutz, Zutritts- und Zugangskontrollen, Besucher- und Lieferantenmanagement, Sicherheitskontrollen, Prävention gegen Sabotage, Diebstahl und Wirtschaftsspionage, Sicherheitsorganisation von Hochrisikobereichen, Zusammenarbeit mit Behörden und Einsatzorganisationen sowie die Koordination der Werkfeuerwehr. Der CSO arbeitet eng mit dem CISO zusammen, insbesondere an Schnittstellen zwischen physischer Sicherheit und Cybersecurity.
CDO	Chief Data Officer	Der CDO verantwortet Datenstrategie, Datenqualität, Datenmodelle, Datenarchitektur und Daten-Governance. Er wirkt an der rechtmässigen, sicheren und zweckgebundenen

		Nutzung von Daten mit.
CQMO	Chief Quality Management Officer	Der CQMO verantwortet Qualitätsmanagement, Audits, Dokumentenlenkung, Managementsysteme, kontinuierliche Verbesserung und akkreditierungsbezogene Qualitätssicherung.
CHRO	Chief Human Resources Officer	Der CHRO verantwortet Personalstrategie, Recruiting, Personalentwicklung, Nachfolgeplanung, Führungskultur, arbeitsbezogene Standards und die Umsetzung des Personalreglements.
CCO	Chief Communications Officer	Der CCO verantwortet interne und externe Kommunikation, Kommunikationsstrategie, Stakeholder-Kommunikation, Reputationsmanagement, Krisenkommunikation und die Koordination

		öffentlicher Aussagen.
CMO	Chief Marketing Officer	Der CMO verantwortet Marketingstrategie, Markenführung, Kampagnen, Marktanalyse und Positionierung der Gesellschaft.
CSO-Sales	Chief Sales Officer	Der Chief Sales Officer verantwortet Vertrieb, Kundengewinnung, Key Accounts, Umsatzplanung und vertriebsbezogene Geschäftsentwicklung. Zur Vermeidung von Verwechslungen mit dem Chief Security Officer kann intern die Bezeichnung CSO-Sales verwendet werden.
CMSO	Chief Marketing / Sales / Services Officer	Der CMSO kann für kombinierte Marketing-, Vertriebs- und Servicefunktionen eingesetzt werden, sofern diese Bündelung organisatorisch zweckmässig ist.
CRO	Chief Risk Officer	Der CRO verantwortet

		Risikomanagement, Risikoanalysen, Risikoberichterstattung, Notfallplanung und Business-Continuity-Schnittstellen.
CLO	Chief Legal Officer	Der CLO verantwortet Recht, Verträge, Gesellschaftsrecht, Datenschutzschnittstellen, Immaterialgüterrecht, externe Anwälte und rechtliche Risikobewertung.
CLO Learning	Chief Learning Officer	Der CLO Learning verantwortet Lernarchitektur, Weiterbildung, Curricula, Ausbildungsqualität und lernbezogene Standards.
CKO	Chief Knowledge Officer	Der CKO verantwortet Wissensmanagement, Archive, Dokumentation, Wissenstransfer und langfristige Sicherung von Organisationswissen.
CAO	Chief Administrative Officer	Der CAO verantwortet Administration, interne

		Verwaltung, Büroorganisation, administrative Standards und bereichsübergreifende Koordination administrativer Abläufe.
CHO	Chief Health / Human Care Officer	Der CHO kann für gesundheits-, betreuungs-, pflege- oder care-bezogene Aufgaben eingesetzt werden. Die konkrete Ausgestaltung erfolgt durch Funktionsbeschrieb oder Spezialreglement.

Anhang B – Übersicht Informationsklassifizierung

Stufe	Bezeichnung	Zugriff	Hinweis
1	Öffentlich	unbeschränkt nach Freigabe	Veröffentlichung zulässig
2	Intern	Mitarbeitende/autorisierte Personen	nicht für externe Veröffentlichung
3	Vertraulich	berechtigte Personen	erhöhter Schutzbedarf
4	Streng vertraulich (Eyes Only)	ausdrücklich benannte Personen	hoher Schutzbedarf
5	Verschlusssache (Top Eyes Only)	ausdrückliche Einzelfreigabe	höchster Schutzbedarf