Informationssicherheitsreglement (ISMS) der Yushin-Ryu AG

Kapitel 1 – Allgemeine Bestimmungen

Art. 1 Zweck

Dieses Informationssicherheitsreglement regelt die Grundsätze, Verantwortlichkeiten, Verfahren und organisatorischen Maßnahmen zur Gewährleistung der Informationssicherheit innerhalb der Yushin-Ryu AG.

Es dient dem Schutz sämtlicher Informationen, Informationssysteme, Forschungsdaten, Lehrunterlagen, medizinischer Daten, Verwaltungsinformationen sowie weiterer schutzwürdiger Informationswerte der Gesellschaft.

Art. 2 Zielsetzung

Das Informationssicherheitsmanagement gewährleistet insbesondere:

- den Schutz der Vertraulichkeit;
- den Schutz der Integrität;
- den Schutz der Verfügbarkeit;
- den Schutz der Authentizität;
- den Schutz der Nachvollziehbarkeit;
- die Unterstützung von Forschung, Lehre, Medizin und Verwaltung;
- den Schutz wissenschaftlicher Erkenntnisse;
- den Schutz kritischer Informationswerte;
- die kontinuierliche Verbesserung der Informationssicherheit.

Art. 3 Oberster Grundsatz

Der Schutz des menschlichen Lebens, der Menschenwürde sowie der langfristigen Lebensgrundlagen der Gesellschaft besitzt innerhalb der Yushin-Ryu AG höchste Priorität.

Sämtliche Entscheidungen in Forschung, Lehre, Medizin, Entwicklung, Informationssicherheit sowie im operativen Handeln sind unter Beachtung dieses Grundsatzes zu treffen.

Können erhebliche Gefahren für Leben oder grundlegende Lebensinteressen entstehen, haben Schutzmaßnahmen Vorrang vor wissenschaftlichen, wirtschaftlichen oder organisatorischen Interessen.

Art. 4 Grundsatz der Schutzgüter

Bei allen Entscheidungen im Bereich der Informationssicherheit sind die Schutzgüter entsprechend ihrer Priorität zu berücksichtigen.

Informationssicherheit dient dem Schutz von Menschen, wissenschaftlicher Arbeit, gesellschaftlicher Verantwortung sowie den Informationswerten der Yushin-Ryu AG.

Die Schutzmaßnahmen sind risikoorientiert, verhältnismäßig und entsprechend der festgelegten Schutzprioritäten umzusetzen.

Art. 5 Priorität der Schutzgüter

Die Yushin-Ryu AG legt für sämtliche Entscheidungen folgende Priorität der Schutzgüter fest:

Priorität	Schutzgut
7	Schutz des menschlichen Lebens
6	Schutz der Menschenwürde sowie der Grund- und Freiheitsrechte
5	Schutz der öffentlichen Gesundheit und Sicherheit
4	Schutz von Umwelt, Natur und langfristigen Lebensgrundlagen
3	Schutz wissenschaftlicher Integrität und verantwortungsvoller Forschung
2	Schutz kritischer Infrastrukturen, Informationen und Systeme
1	Schutz materieller und wirtschaftlicher Werte

Diese Prioritäten bilden die Grundlage sämtlicher sicherheitsrelevanter Entscheidungen innerhalb der Yushin-Ryu AG.

Art. 6 Informationsklassifizierung

Zur Klassifizierung von Informationen verwendet die Yushin-Ryu AG ein universitätsweites Sicherheitsklassifizierungssystem.

Die Informationsklassifizierung erfolgt mittels **Level 0 bis Level 20**.

Je höher das Level, desto höher sind der Schutzbedarf, die Sicherheitsanforderungen sowie die organisatorischen und technischen Schutzmaßnahmen.

Die detaillierte Definition der einzelnen Level wird in einer gesonderten **Sicherheitsklassifizierungsrichtlinie** geregelt.

Art. 7 Trennung von Priorität und Level

Die Priorität der Schutzgüter sowie die Informationsklassifizierung stellen zwei eigenständige Steuerungssysteme dar.

- Die **Priorität** beschreibt die Rangfolge der zu schützenden Rechtsgüter.
- Das **Level** beschreibt den Schutzbedarf einer Information, eines Systems oder eines Informationswertes.

Beide Systeme sind gemeinsam bei sicherheitsrelevanten Entscheidungen anzuwenden.

Art. 8 Geltungsbereich

Dieses Reglement gilt für:

- den Verwaltungsrat;
- den Präsidenten des Verwaltungsrates;
- den Chief Executive Officer (CEO);
- den Chief Information Officer (CIO);
- den Chief Information Security Officer (CISO);
- sämtliche Mitglieder der Geschäftsleitung;
- alle Mitarbeitenden;
- alle Forschenden;
- alle Dozierenden;
- alle Studierenden;
- sämtliche Fakultäten, Institute und Fachbereiche;
- sämtliche Tochtergesellschaften und internationalen Standorte der Yushin-Ryu AG;
- externe Personen, soweit sie Zugang zu Informationswerten der Gesellschaft erhalten.

Art. 9 Einbindung in das Managementsystem

Das Informationssicherheitsmanagement ist Bestandteil des integrierten Managementsystems der Yushin-Ryu AG.

Es arbeitet insbesondere mit folgenden Bereichen zusammen:

- Qualitätsmanagement;
- Risikomanagement;
- Compliance;
- Datenschutz;

- Ethikmanagement;
- Forschungs- und Laborsicherheit;
- Business Continuity Management;
- Internes Kontrollsystem (IKS).

Art. 10 Strategische Bedeutung

Informationssicherheit ist ein strategischer Erfolgsfaktor der Yushin-Ryu AG.

Sie unterstützt den Schutz von Forschung, Lehre, Medizin, Innovation, Verwaltung, geistigem Eigentum sowie internationaler wissenschaftlicher Zusammenarbeit und trägt zur langfristigen Sicherheit und Stabilität der Gesellschaft bei.

Kapitel 2 – Grundsätze der Informationssicherheit

Art. 11 Grundsatz der Informationssicherheit

Informationssicherheit dient dem Schutz sämtlicher Informationswerte der Yushin-Ryu AG.

Sie gewährleistet die sichere Durchführung von Forschung, Lehre, Medizin, Verwaltung sowie aller weiteren Geschäftsprozesse und bildet einen wesentlichen Bestandteil der Corporate Governance.

Art. 12 Schutzziele

Das Informationssicherheitsmanagement verfolgt insbesondere folgende Schutzziele:

• Vertraulichkeit;

• Integrität;

• Verfügbarkeit;

• Authentizität;

• Nachvollziehbarkeit;

• Resilienz;

• Verantwortlichkeit.

Diese Schutzziele sind bei sämtlichen sicherheitsrelevanten Entscheidungen angemessen zu berücksichtigen.

Art. 13 Vertraulichkeit

Informationen dürfen ausschließlich denjenigen Personen zugänglich gemacht werden, welche aufgrund ihrer Funktion oder einer ausdrücklich erteilten Berechtigung Zugriff benötigen.

Der Zugriff erfolgt nach den Grundsätzen des **Need-to-know-Prinzips** sowie des **Least-Privilege-Prinzips**.

Art. 14 Integrität

Informationen sind gegen unbefugte Veränderung, Manipulation, Beschädigung oder Verfälschung zu schützen.

Die Richtigkeit, Vollständigkeit und Nachvollziehbarkeit von Informationen sind jederzeit sicherzustellen.

Art. 15 Verfügbarkeit

Informationswerte, Systeme und Dienstleistungen sind entsprechend ihrer Kritikalität verfügbar zu halten.

Geeignete organisatorische, personelle und technische Maßnahmen sind vorzusehen, um Unterbrechungen möglichst zu vermeiden oder deren Auswirkungen auf ein vertretbares Maß zu begrenzen.

Art. 16 Authentizität

Die Herkunft von Informationen sowie die Identität von Personen, Systemen und Kommunikationspartnern sind durch geeignete organisatorische und technische Verfahren sicherzustellen.

Elektronische Identitäten sind eindeutig zuzuordnen und angemessen zu schützen.

Art. 17 Nachvollziehbarkeit

Sicherheitsrelevante Vorgänge, Änderungen und Zugriffe sind entsprechend ihrer Schutzklassifizierung nachvollziehbar zu dokumentieren und zu protokollieren.

Die Aufbewahrung der Protokolle richtet sich nach den geltenden gesetzlichen sowie internen Vorgaben.

Art. 18 Sicherheitsbewusstsein

Informationssicherheit ist Aufgabe sämtlicher Organe, Führungskräfte, Mitarbeitenden, Forschenden, Lehrenden, Studierenden sowie externer Personen mit Zugang zu Informationswerten der Yushin-Ryu AG.

Jede Person trägt im Rahmen ihrer Aufgaben Verantwortung für den Schutz der ihr anvertrauten Informationen.

Art. 19 Sicherheitskultur

Die Yushin-Ryu AG fördert eine Sicherheitskultur, die auf Verantwortung, Vertrauen, Aufmerksamkeit, Transparenz und kontinuierlicher Verbesserung basiert.

Sicherheitsrelevante Beobachtungen, Schwachstellen und Vorfälle sind unverzüglich über die vorgesehenen Meldewege zu melden.

Art. 20 Kontinuierliche Weiterentwicklung

Das Informationssicherheitsmanagement ist fortlaufend an neue wissenschaftliche Erkenntnisse, technologische Entwicklungen, gesetzliche Anforderungen sowie veränderte Bedrohungslagen anzupassen.

Die Wirksamkeit der Informationssicherheitsmaßnahmen ist regelmäßig zu überprüfen und kontinuierlich weiterzuentwickeln.

Kapitel 3 – Informationssicherheitsorganisation

Art. 21 Grundsatz

Die Informationssicherheitsorganisation der Yushin-Ryu AG gewährleistet eine klare Zuweisung von Verantwortlichkeiten, Kompetenzen und Entscheidungswegen.

Sie stellt sicher, dass Informationssicherheit als integraler Bestandteil von Forschung, Lehre, Medizin, Verwaltung und allen unterstützenden Geschäftsprozessen umgesetzt wird.

Art. 22 Verantwortung des Verwaltungsrates

Der Verwaltungsrat trägt die oberste Verantwortung für die strategische Ausrichtung des Informationssicherheitsmanagements.

Er genehmigt die Informationssicherheitsstrategie sowie die wesentlichen Reglemente und überwacht deren Umsetzung.

Art. 23 Verantwortung der Geschäftsleitung

Die Geschäftsleitung ist für die operative Umsetzung der Informationssicherheitsstrategie verantwortlich.

Sie stellt die personellen, organisatorischen, technischen und finanziellen Ressourcen für ein wirksames Informationssicherheitsmanagement bereit.

Art. 24 Chief Information Officer (CIO)

Der Chief Information Officer (CIO) trägt die Gesamtverantwortung für das Informationsmanagement sowie die strategische Weiterentwicklung der Informations- und Kommunikationstechnologie der Yushin-Ryu AG.

Er koordiniert die Umsetzung des Informationssicherheitsmanagements in Zusammenarbeit mit den zuständigen Organisationseinheiten.

Art. 25 Chief Information Security Officer (CISO)

Der Chief Information Security Officer (CISO) verantwortet die operative Umsetzung, Überwachung und kontinuierliche Weiterentwicklung des Informationssicherheitsmanagementsystems.

Er berät den Verwaltungsrat, die Geschäftsleitung sowie den CIO in allen Fragen der Informationssicherheit.

Art. 26 Zusammenarbeit mit weiteren Managementsystemen

Das Informationssicherheitsmanagement arbeitet eng mit folgenden Bereichen zusammen:

• Qualitätsmanagement;

• Risikomanagement;

• Compliance;

• Datenschutz;

• Ethikmanagement;

• Forschungs- und Laborsicherheit;

• Business Continuity Management;

• Internes Kontrollsystem.

Art. 27 Verantwortung der Führungskräfte

Führungskräfte sind innerhalb ihres Verantwortungsbereiches für die Umsetzung und Einhaltung der Anforderungen dieses Reglements verantwortlich.

Sie stellen sicher, dass Mitarbeitende angemessen informiert, geschult und in sicherheitsrelevante Prozesse eingebunden werden.

Art. 28 Verantwortung der Mitarbeitenden

Alle Mitarbeitenden, Forschenden, Lehrenden, Studierenden sowie externe Personen mit Zugang zu Informationswerten der Yushin-Ryu AG sind verpflichtet, dieses Reglement einzuhalten.

Sicherheitsrelevante Ereignisse, Schwachstellen oder Verstöße sind unverzüglich über die vorgesehenen Meldewege zu melden.

Art. 29 Informationssicherheitsgremien

Zur Unterstützung des Informationssicherheitsmanagements können permanente oder projektbezogene Gremien eingerichtet werden.

Ihre Aufgaben, Kompetenzen und Zusammensetzung werden durch die Geschäftsleitung festgelegt.

Art. 30 Überprüfung der Organisationsstruktur

Die Informationssicherheitsorganisation ist regelmäßig auf ihre Wirksamkeit, Angemessenheit und Aktualität zu überprüfen.

Erforderliche organisatorische Anpassungen sind zeitnah umzusetzen.

Kapitel 4 – Informationsklassifizierung

Art. 31 Grundsatz

Sämtliche Informationswerte der Yushin-Ryu AG sind entsprechend ihrem Schutzbedarf zu klassifizieren.

Die Klassifizierung dient der Festlegung angemessener organisatorischer, personeller, technischer und rechtlicher Schutzmaßnahmen.

Art. 32 Informationsklassifizierungssystem

Die Yushin-Ryu AG verwendet ein einheitliches Informationsklassifizierungssystem mit den Sicherheitsstufen **Level 0 bis Level 20**.

Je höher das Level, desto höher sind die Anforderungen an Vertraulichkeit, Integrität, Verfügbarkeit sowie die organisatorischen und technischen Schutzmaßnahmen.

Die Detailregelungen werden in der Sicherheitsklassifizierungsrichtlinie festgelegt.

Art. 33 Klassifizierungspflicht

Jeder Informationswert ist vor seiner Erstellung, Bearbeitung oder Nutzung hinsichtlich seines Schutzbedarfs angemessen zu klassifizieren.

Die Klassifizierung ist während des gesamten Informationslebenszyklus regelmäßig zu überprüfen und erforderlichenfalls anzupassen.

Art. 34 Schutzbedarf

Bei der Festlegung des Schutzbedarfs sind insbesondere zu berücksichtigen:

• die Priorität der Schutzgüter;

• gesetzliche Anforderungen;

• vertragliche Verpflichtungen;

• wissenschaftliche Bedeutung;

• medizinische Relevanz;

• wirtschaftliche Auswirkungen;

• Risiken für Menschen, Umwelt und Gesellschaft.

Art. 35 Informationskategorien

Informationswerte sind zusätzlich einer geeigneten Informationskategorie zuzuordnen.

Hierzu gehören insbesondere:

• Forschung;

• Lehre;

• Medizin;

• Personal;

• Finanzen;

• Recht;

• Governance;

• Qualitätsmanagement;

• Informationssicherheit;

• Risikomanagement;

• kritische Infrastruktur;

• weitere durch die Geschäftsleitung festgelegte Kategorien.

Art. 36 Verantwortlichkeit

Für die Klassifizierung eines Informationswertes ist dessen fachlich verantwortliche Organisationseinheit verantwortlich.

Der Informationseigentümer stellt sicher, dass Klassifizierung, Kennzeichnung und Schutzmaßnahmen angemessen umgesetzt werden.

Art. 37 Änderung der Klassifizierung

Ändert sich der Schutzbedarf eines Informationswertes, ist dessen Klassifizierung unverzüglich anzupassen.

Bereits getroffene Schutzmaßnahmen sind entsprechend zu überprüfen und erforderlichenfalls zu ergänzen.

Art. 38 Kennzeichnung

Informationswerte sind entsprechend ihrer Klassifizierung eindeutig und nachvollziehbar zu kennzeichnen.

Die Form der Kennzeichnung wird in der Sicherheitsklassifizierungsrichtlinie geregelt.

Art. 39 Überprüfung

Die Informationsklassifizierung ist regelmäßig sowie bei wesentlichen Änderungen von Inhalt, Nutzung oder Risiko zu überprüfen.

Die Ergebnisse der Überprüfung sind angemessen zu dokumentieren.

Art. 40 Ausführungsbestimmungen

Die Geschäftsleitung erlässt auf Antrag des Chief Information Officer (CIO) und unter Mitwirkung des Chief Information Security Officer (CISO) die erforderlichen Richtlinien zur praktischen Umsetzung der Informationsklassifizierung.

Diese Richtlinien regeln insbesondere die Definition der einzelnen Level, Kennzeichnungsvorgaben, Zugriffsregelungen sowie organisatorische und technische Schutzmaßnahmen.

Kapitel 5 – Identitäts- und Berechtigungsmanagement

Art. 41 Grundsatz

Der Zugriff auf Informationen, Informationssysteme und sonstige Informationswerte der Yushin-Ryu AG ist ausschließlich autorisierten Personen im Rahmen ihrer Aufgaben und Zuständigkeiten zu gestatten.

Die Vergabe von Berechtigungen erfolgt nach den Grundsätzen der Informationssicherheit, der Verhältnismäßigkeit sowie der festgelegten Schutzprioritäten und Informationsklassifizierungen.

Art. 42 Identitätsmanagement

Für jede natürliche oder technische Person ist eine eindeutige Identität einzurichten.

Gemeinschaftskonten sind grundsätzlich unzulässig. Ausnahmen bedürfen einer schriftlichen Genehmigung des Chief Information Security Officer (CISO) und sind zu dokumentieren.

Art. 43 Benutzerkonten

Benutzerkonten dürfen ausschließlich nach erfolgreicher Identitätsprüfung eingerichtet werden.

Einrichtung, Änderung, Sperrung und Löschung von Benutzerkonten sind nachvollziehbar zu dokumentieren.

Art. 44 Berechtigungsvergabe

Berechtigungen werden ausschließlich auf Antrag der zuständigen Führungskraft oder des Informationseigentümers vergeben.

Die Vergabe erfolgt entsprechend:

• der Funktion;

• der Aufgabe;

• der Informationsklassifizierung;

• dem Need-to-know-Prinzip;

• dem Least-Privilege-Prinzip.

Art. 45 Überprüfung von Berechtigungen

Sämtliche Berechtigungen sind regelmäßig sowie bei organisatorischen Veränderungen zu überprüfen.

Nicht mehr benötigte Berechtigungen sind unverzüglich anzupassen oder zu entziehen.

Art. 46 Authentifizierungsverfahren

Für den Zugang zu Informationssystemen sind geeignete Authentifizierungsverfahren einzusetzen.

Abhängig von der Informationsklassifizierung können insbesondere Mehrfaktor-Authentifizierung, kryptographische Verfahren oder weitere geeignete Sicherheitsmaßnahmen vorgeschrieben werden.

Art. 47 Privilegierte Zugriffe

Administrative oder sonstige privilegierte Zugriffe sind auf das notwendige Mindestmaß zu beschränken.

Ihre Nutzung ist besonders zu schützen, zu dokumentieren und regelmäßig zu überprüfen.

Art. 48 Beendigung von Zugriffsrechten

Beim Austritt, Funktionswechsel oder Wegfall des dienstlichen Bedarfs sind sämtliche Berechtigungen unverzüglich anzupassen oder zu entziehen.

Die verantwortliche Organisationseinheit stellt die vollständige Umsetzung sicher.

Art. 49 Protokollierung

Sicherheitsrelevante Anmeldungen, Berechtigungsänderungen sowie privilegierte Zugriffe sind entsprechend der Informationsklassifizierung zu protokollieren.

Die Protokolle sind gegen unbefugte Veränderung zu schützen.

Art. 50 Kontinuierliche Verbesserung

Das Identitäts- und Berechtigungsmanagement ist regelmäßig hinsichtlich Wirksamkeit, Sicherheit und Aktualität zu überprüfen.

Erforderliche Verbesserungsmaßnahmen sind zeitnah umzusetzen.

Kapitel 6 – Informationswerte und Schutzobjekte

Art. 51 Grundsatz

Sämtliche Informationswerte und Schutzobjekte der Yushin-Ryu AG sind entsprechend ihrem Schutzbedarf zu identifizieren, zu klassifizieren und angemessen zu schützen.

Die Schutzmaßnahmen richten sich nach der Priorität der Schutzgüter sowie der jeweiligen Informationsklassifizierung.

Art. 52 Informationswerte

Zu den Informationswerten gehören insbesondere:

• Forschungsdaten;

• Lehr- und Ausbildungsunterlagen;

• medizinische Informationen;

• Personaldaten;

• Studierendendaten;

• Finanz- und Rechnungswesendaten;

• Vertragsunterlagen;

• Verwaltungsinformationen;

• Qualitätsmanagementdokumente;

• Compliance-Unterlagen;

• Risikomanagementdokumentationen;

• weitere schutzwürdige Informationen.

Art. 53 Schutzobjekte

Zu den Schutzobjekten gehören insbesondere:

• Informationssysteme;

• Server;

• Netzwerke;

• Cloud-Dienste;

• Datenbanken;

• Endgeräte;

• mobile Geräte;

• Datenträger;

• Kommunikationssysteme;

• Archive;

• Rechenzentren;

• Laborinformationssysteme.

Art. 54 Forschung und geistiges Eigentum

Forschungsdaten, wissenschaftliche Erkenntnisse, Patente, Prototypen, Entwicklungsunterlagen, Quellcodes sowie sonstiges geistiges Eigentum sind als besonders schutzwürdige Informationswerte zu behandeln.

Der Schutz richtet sich nach ihrer Informationsklassifizierung sowie den gesetzlichen und vertraglichen Anforderungen.

Art. 55 Medizinische Informationswerte

Medizinische Informationen sowie gesundheitsbezogene Daten unterliegen einem besonderen Schutz.

Ihre Verarbeitung erfolgt ausschließlich im Rahmen der gesetzlichen Bestimmungen sowie der internen Datenschutz-, Informationssicherheits- und Ethikvorgaben.

Art. 56 Eigentümerschaft

Für jeden Informationswert ist ein verantwortlicher Informationseigentümer zu bestimmen.

Der Informationseigentümer trägt insbesondere Verantwortung für:

• die Klassifizierung;

• die Aktualität;

• die Schutzmaßnahmen;

• die Zugriffsberechtigungen;

• die regelmäßige Überprüfung.

Art. 57 Lebenszyklus

Informationswerte sind während ihres gesamten Lebenszyklus angemessen zu schützen.

Der Lebenszyklus umfasst insbesondere:

• Erstellung;

• Erfassung;

• Bearbeitung;

• Speicherung;

• Nutzung;

• Weitergabe;

• Archivierung;

• Löschung;

• Vernichtung.

Art. 58 Dokumentation

Informationswerte und Schutzobjekte sind in geeigneter Form zu dokumentieren.

Die Dokumentation muss insbesondere Eigentümerschaft, Informationsklassifizierung, Informationskategorie sowie wesentliche Schutzmaßnahmen enthalten.

Art. 59 Regelmäßige Überprüfung

Informationswerte und Schutzobjekte sind regelmäßig hinsichtlich ihres Schutzbedarfs sowie ihrer Aktualität zu überprüfen.

Änderungen sind zeitnah zu dokumentieren und erforderlichenfalls neu zu klassifizieren.

Art. 60 Kontinuierliche Weiterentwicklung

Die Yushin-Ryu AG entwickelt den Schutz ihrer Informationswerte und Schutzobjekte kontinuierlich weiter.

Neue wissenschaftliche Erkenntnisse, technologische Entwicklungen, gesetzliche Anforderungen sowie veränderte Bedrohungslagen sind angemessen zu berücksichtigen.

Kapitel 7 – IT-Infrastruktur und Systemschutz

Art. 61 Grundsatz

Die IT-Infrastruktur der Yushin-Ryu AG ist entsprechend ihrer Kritikalität sowie ihrer Informationsklassifizierung zu planen, zu betreiben, zu überwachen und kontinuierlich weiterzuentwickeln.

Sie muss den Anforderungen an Verfügbarkeit, Integrität, Vertraulichkeit, Authentizität und Nachvollziehbarkeit entsprechen.

Art. 62 Geltungsbereich

Zur IT-Infrastruktur gehören insbesondere:

• Rechenzentren;

• Server;

• Arbeitsplatzsysteme;

• mobile Endgeräte;

• Netzwerke;

• Kommunikationssysteme;

• Cloud-Dienste;

• Speicher- und Archivsysteme;

• Labor- und Forschungsinfrastrukturen;

• medizinische Informationssysteme;

• weitere informationsverarbeitende Systeme.

Art. 63 Sicherheitsanforderungen

Informationssysteme sind entsprechend ihrer Informationsklassifizierung sowie ihrem Schutzbedarf durch geeignete organisatorische, personelle, physische und technische Maßnahmen zu schützen.

Die Schutzmaßnahmen sind regelmäßig auf ihre Wirksamkeit zu überprüfen.

Art. 64 Netzwerksicherheit

Netzwerke sind nach dem Stand der Technik gegen unbefugte Zugriffe, Manipulationen, Ausfälle und sonstige Gefährdungen zu schützen.

Netzwerksegmente mit erhöhtem Schutzbedarf sind logisch oder physisch voneinander zu trennen.

Art. 65 Server- und Systembetrieb

Server und zentrale Informationssysteme sind nach dokumentierten Betriebs- und Sicherheitsstandards zu betreiben.

Konfigurationen, Änderungen und Wartungsmaßnahmen sind nachvollziehbar zu dokumentieren.

Art. 66 Endgeräte

Endgeräte dürfen ausschließlich entsprechend den geltenden Sicherheitsvorgaben betrieben werden.

Hierzu gehören insbesondere:

• sichere Konfiguration;

• Zugriffsschutz;

• Verschlüsselung;

• regelmäßige Aktualisierung;

• Schutz vor Schadsoftware.

Art. 67 Datensicherung

Für alle informationskritischen Systeme sind angemessene Datensicherungen durchzuführen.

Backup- und Wiederherstellungsverfahren sind regelmäßig zu testen und entsprechend der Informationsklassifizierung auszulegen.

Art. 68 Systemüberwachung

Informationssysteme sind entsprechend ihrem Schutzbedarf kontinuierlich zu überwachen.

Sicherheitsrelevante Ereignisse sind zu protokollieren, auszuwerten und erforderlichenfalls unverzüglich zu bearbeiten.

Art. 69 Wartung und Änderungen

Wartungsarbeiten sowie Änderungen an informationsverarbeitenden Systemen sind kontrolliert, dokumentiert und nach einem geregelten Änderungsverfahren durchzuführen.

Sicherheitsrelevante Auswirkungen sind vor der Umsetzung zu bewerten.

Art. 70 Resilienz der IT-Infrastruktur

Die IT-Infrastruktur ist so auszulegen, dass sie auch bei technischen Störungen, Sicherheitsvorfällen oder außergewöhnlichen Ereignissen möglichst funktionsfähig bleibt.

Hierzu sind angemessene Maßnahmen zur Redundanz, Ausfallsicherheit und Wiederherstellung vorzusehen.

Kapitel 8 – Cybersecurity und technische Informationssicherheit

Art. 71 Grundsatz

Die Yushin-Ryu AG schützt ihre Informationssysteme, Netzwerke und digitalen Infrastrukturen durch angemessene organisatorische, personelle und technische Sicherheitsmaßnahmen gegen Cyberbedrohungen.

Die Maßnahmen richten sich nach der Informationsklassifizierung, der Priorität der Schutzgüter sowie dem jeweiligen Risikopotenzial.

Art. 72 Cybersecurity-Strategie

Die Yushin-Ryu AG verfolgt eine risikoorientierte Cybersecurity-Strategie.

Diese umfasst insbesondere:

• Prävention;

• Erkennung;

• Reaktion;

• Wiederherstellung;

• kontinuierliche Verbesserung.

Art. 73 Schutz vor Schadsoftware

Informationssysteme sind durch geeignete Schutzmaßnahmen gegen Schadsoftware, Ransomware, Spyware, Trojaner und vergleichbare Bedrohungen zu sichern.

Sicherheitslösungen sind regelmäßig zu aktualisieren und auf ihre Wirksamkeit zu überprüfen.

Art. 74 Schwachstellenmanagement

Bekannte Schwachstellen in Hard- und Software sind systematisch zu erfassen, zu bewerten und zeitnah zu beheben.

Sicherheitskritische Schwachstellen sind entsprechend ihrer Kritikalität priorisiert zu behandeln.

Art. 75 Patchmanagement

Sicherheitsrelevante Aktualisierungen sind nach einem geregelten Verfahren zu planen, zu testen und zeitnah einzuspielen.

Ausnahmen sind zu begründen, zu dokumentieren und regelmäßig zu überprüfen.

Art. 76 Schutz vor Social Engineering

Die Yushin-Ryu AG trifft geeignete Maßnahmen zum Schutz vor Social Engineering, Phishing, Identitätsmissbrauch sowie vergleichbaren Angriffsmethoden.

Mitarbeitende sind regelmäßig für entsprechende Bedrohungen zu sensibilisieren.

Art. 77 Sicherheitsüberwachung

Informationssysteme sind entsprechend ihrer Informationsklassifizierung kontinuierlich auf sicherheitsrelevante Ereignisse zu überwachen.

Auffälligkeiten sind unverzüglich zu analysieren und nach den geltenden Incident-Response-Verfahren zu behandeln.

Art. 78 Penetrationstests und Sicherheitsprüfungen

Informationssysteme mit erhöhtem Schutzbedarf sind regelmäßig durch geeignete Sicherheitsüberprüfungen zu bewerten.

Hierzu können insbesondere gehören:

• Schwachstellenanalysen;

• Penetrationstests;

• Konfigurationsprüfungen;

• technische Sicherheitsbewertungen.

Art. 79 Cybersecurity-Vorfälle

Cybersecurity-Vorfälle sind unverzüglich zu melden, zu dokumentieren und nach festgelegten Verfahren zu bearbeiten.

Schwere Sicherheitsvorfälle sind entsprechend den internen Eskalations- und Krisenmanagementprozessen zu behandeln.

Art. 80 Kontinuierliche Weiterentwicklung

Die Yushin-Ryu AG entwickelt ihre Cybersecurity-Maßnahmen kontinuierlich weiter.

Neue Bedrohungen, technologische Entwicklungen, wissenschaftliche Erkenntnisse sowie internationale Standards sind regelmäßig zu bewerten und bei Bedarf in das Informationssicherheitsmanagement zu integrieren.

Kapitel 9 – Kryptographie und Verschlüsselung

Art. 81 Grundsatz

Kryptographische Verfahren dienen dem Schutz der Vertraulichkeit, Integrität, Authentizität und Nachvollziehbarkeit von Informationen.

Sie sind entsprechend der Informationsklassifizierung, der Priorität der Schutzgüter sowie dem Stand der Technik einzusetzen.

Art. 82 Anwendungsbereich

Kryptographische Verfahren sind insbesondere anzuwenden bei:

• Speicherung schutzwürdiger Informationen;

• Übertragung von Informationen;

• Authentifizierung;

• digitalen Signaturen;

• Datensicherungen;

• mobilen Datenträgern;

• Cloud-Diensten;

• weiteren informationskritischen Anwendungen.

Art. 83 Verschlüsselung

Informationen mit erhöhtem Schutzbedarf sind während der Speicherung und Übertragung durch geeignete Verschlüsselungsverfahren zu schützen.

Art und Umfang der Verschlüsselung richten sich nach der jeweiligen Informationsklassifizierung.

Art. 84 Schlüsselmanagement

Kryptographische Schlüssel sind während ihres gesamten Lebenszyklus angemessen zu schützen.

Die Erzeugung, Speicherung, Verteilung, Nutzung, Erneuerung, Archivierung und Vernichtung kryptographischer Schlüssel erfolgt nach dokumentierten Verfahren.

Art. 85 Digitale Signaturen

Digitale Signaturen können eingesetzt werden, um Authentizität, Integrität und Nachvollziehbarkeit elektronischer Dokumente und Transaktionen sicherzustellen.

Ihre Verwendung richtet sich nach den geltenden gesetzlichen sowie internen Vorgaben.

Art. 86 Zertifikatsmanagement

Digitale Zertifikate sind ordnungsgemäß zu verwalten.

Ungültige, abgelaufene oder kompromittierte Zertifikate sind unverzüglich zu sperren oder zu ersetzen.

Art. 87 Kryptographische Verfahren

Es dürfen ausschließlich kryptographische Verfahren eingesetzt werden, die dem anerkannten Stand der Technik entsprechen.

Veraltete oder als unsicher eingestufte Verfahren sind zeitnah außer Betrieb zu nehmen.

Art. 88 Schutz kryptographischer Informationen

Kryptographische Schlüssel, Zertifikate und vergleichbare Sicherheitsinformationen sind entsprechend ihrer Informationsklassifizierung besonders zu schützen.

Der Zugriff ist auf ausdrücklich autorisierte Personen oder Systeme zu beschränken.

Art. 89 Überprüfung

Der Einsatz kryptographischer Verfahren ist regelmäßig hinsichtlich Wirksamkeit, Aktualität und Sicherheit zu überprüfen.

Erforderliche Anpassungen sind zeitnah umzusetzen.

Art. 90 Kontinuierliche Weiterentwicklung

Die Yushin-Ryu AG entwickelt ihre kryptographischen Verfahren unter Berücksichtigung neuer wissenschaftlicher Erkenntnisse, technischer Entwicklungen sowie international anerkannter Sicherheitsstandards kontinuierlich weiter.

Kapitel 10 – Physische Informationssicherheit und Zutrittsschutz

Art. 91 Grundsatz

Informationswerte, Informationssysteme sowie kritische Infrastrukturen der Yushin-Ryu AG sind durch geeignete physische und organisatorische Sicherheitsmaßnahmen gegen unbefugten Zutritt, Beschädigung, Sabotage, Diebstahl und sonstige Gefährdungen zu schützen.

Art. 92 Sicherheitsbereiche

Gebäude, Räume und Anlagen sind entsprechend ihrem Schutzbedarf in geeignete Sicherheitsbereiche einzuteilen.

Die Einteilung richtet sich insbesondere nach der Informationsklassifizierung, der Kritikalität der Infrastruktur sowie den betrieblichen Risiken.

Art. 93 Zutrittsberechtigungen

Der Zutritt zu Sicherheitsbereichen ist ausschließlich autorisierten Personen zu gestatten.

Zutrittsberechtigungen sind nach dem Need-to-know-Prinzip sowie entsprechend der jeweiligen Funktion zu vergeben und regelmäßig zu überprüfen.

Art. 94 Zutrittskontrollsysteme

Für sicherheitsrelevante Bereiche sind geeignete Zutrittskontrollsysteme einzusetzen.

Hierzu können insbesondere gehören:

• elektronische Zutrittskontrollen;

• Identifikationssysteme;

• biometrische Verfahren;

• mechanische Schließsysteme;

• Mehrfaktor-Authentifizierung.

Art. 95 Besucherregelung

Besucherinnen und Besucher dürfen Sicherheitsbereiche ausschließlich nach vorheriger Genehmigung und unter Beachtung der geltenden Sicherheitsvorschriften betreten.

Soweit erforderlich, sind Besucher zu registrieren und zu begleiten.

Art. 96 Schutz kritischer Infrastruktur

Rechenzentren, Serverräume, Netzwerkverteiler, Archive, Laborbereiche sowie sonstige kritische Einrichtungen sind gegen unbefugten Zutritt und äußere Einwirkungen besonders zu schützen.

Hierbei sind bauliche, organisatorische und technische Schutzmaßnahmen miteinander zu kombinieren.

Art. 97 Schutz vor Umwelt- und Betriebsrisiken

Geeignete Maßnahmen sind vorzusehen, um Informationswerte und Informationssysteme insbesondere vor folgenden Risiken zu schützen:

• Brand;

• Wasser;

• Rauch;

• Stromausfall;

• Überspannung;

• Klimaeinflüssen;

• technischen Ausfällen;

• sonstigen betrieblichen Gefährdungen.

Art. 98 Mitnahme und Entfernung von Informationswerten

Die Mitnahme oder Entfernung von Datenträgern, Geräten oder sonstigen Informationswerten aus Sicherheitsbereichen bedarf einer entsprechenden Berechtigung.

Schutzmaßnahmen richten sich nach der jeweiligen Informationsklassifizierung.

Art. 99 Überwachung und Kontrolle

Physische Sicherheitsmaßnahmen sind regelmäßig auf ihre Wirksamkeit zu überprüfen.

Sicherheitsrelevante Feststellungen sind zu dokumentieren und erforderlichenfalls unverzüglich zu beheben.

Art. 100 Kontinuierliche Verbesserung

Die physische Informationssicherheit ist unter Berücksichtigung neuer Bedrohungen, technischer Entwicklungen sowie organisatorischer Veränderungen kontinuierlich weiterzuentwickeln.

Kapitel 11 – Forschung, Lehre und Schutz wissenschaftlicher Informationen

Art. 101 Grundsatz

Forschungs-, Lehr- und Entwicklungsinformationen der Yushin-Ryu AG sind entsprechend ihrer wissenschaftlichen Bedeutung, ihrer Informationsklassifizierung sowie ihrem Schutzbedarf angemessen zu schützen.

Der Schutz wissenschaftlicher Informationen dient insbesondere der Sicherung wissenschaftlicher Integrität, der Forschungsfreiheit sowie des geistigen Eigentums.

Art. 102 Schutz wissenschaftlicher Informationen

Wissenschaftliche Informationen sind gegen unbefugte Kenntnisnahme, Veränderung, Verlust, Manipulation oder Zerstörung zu schützen.

Der Umfang der Schutzmaßnahmen richtet sich nach der jeweiligen Informationsklassifizierung.

Art. 103 Forschungsdaten

Forschungsdaten sind während ihres gesamten Lebenszyklus sicher zu erfassen, zu speichern, zu bearbeiten, zu übertragen, zu archivieren und – soweit zulässig – zu löschen.

Hierbei sind wissenschaftliche Standards sowie gesetzliche Anforderungen einzuhalten.

Art. 104 Geistiges Eigentum

Patente, Erfindungen, wissenschaftliche Konzepte, Entwicklungsunterlagen, Prototypen, Software, Algorithmen sowie sonstiges geistiges Eigentum sind entsprechend ihrem Schutzbedarf besonders zu sichern.

Die Rechte der Yushin-Ryu AG sowie der beteiligten Forschenden bleiben hiervon unberührt.

Art. 105 Internationale Forschungskooperationen

Bei internationalen Forschungsprojekten sind die Anforderungen dieses Reglements sowie die jeweils geltenden gesetzlichen und vertraglichen Bestimmungen einzuhalten.

Informationsaustausch und Datenübermittlung erfolgen ausschließlich entsprechend der festgelegten Informationsklassifizierung.

Art. 106 Drittmittelprojekte

Forschungsinformationen aus Drittmittelprojekten sind entsprechend den vertraglichen Verpflichtungen sowie den Anforderungen dieses Reglements zu schützen.

Vertraulichkeitsvereinbarungen und Schutzrechte sind angemessen zu berücksichtigen.

Art. 107 Veröffentlichung wissenschaftlicher Ergebnisse

Die Veröffentlichung wissenschaftlicher Ergebnisse erfolgt unter Wahrung der wissenschaftlichen Integrität sowie der Schutzinteressen der Yushin-Ryu AG.

Vor einer Veröffentlichung sind bestehende Schutzrechte, Vertraulichkeitsverpflichtungen sowie sicherheitsrelevante Aspekte angemessen zu prüfen.

Art. 108 Informationsaustausch

Der Austausch wissenschaftlicher Informationen innerhalb und außerhalb der Yushin-Ryu AG erfolgt ausschließlich über zugelassene und angemessen geschützte Kommunikationswege.

Die Informationsklassifizierung ist hierbei jederzeit zu beachten.

Art. 109 Verantwortung der Forschenden

Forschende tragen Verantwortung für den Schutz der ihnen anvertrauten wissenschaftlichen Informationen.

Sie haben insbesondere die Vorgaben zur Informationsklassifizierung, zum Datenschutz sowie zur Informationssicherheit einzuhalten.

Art. 110 Kontinuierliche Weiterentwicklung

Die Verfahren zum Schutz wissenschaftlicher Informationen sind regelmäßig zu überprüfen und unter Berücksichtigung wissenschaftlicher, technischer sowie rechtlicher Entwicklungen kontinuierlich weiterzuentwickeln.

Kapitel 12 – Medizinische Informationssicherheit

Art. 111 Grundsatz

Medizinische Informationen unterliegen aufgrund ihres besonderen Schutzbedarfs erhöhten Anforderungen an Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität.

Der Schutz der Patientinnen und Patienten sowie der Schutz des menschlichen Lebens besitzen hierbei höchste Priorität.

Art. 112 Geltungsbereich

Dieses Kapitel gilt insbesondere für:

• Patientendaten;

• Gesundheitsdaten;

• klinische Forschungsdaten;

• diagnostische Informationen;

• medizinische Bilddaten;

• Laborbefunde;

• Biobankdaten;

• genetische Informationen;

• weitere medizinische Informationswerte.

Art. 113 Schutz medizinischer Informationen

Medizinische Informationen dürfen ausschließlich im Rahmen der gesetzlichen Bestimmungen sowie der internen Reglemente verarbeitet werden.

Die Verarbeitung erfolgt entsprechend ihrer Informationsklassifizierung und ihrem Schutzbedarf.

Art. 114 Zugriffsberechtigungen

Der Zugriff auf medizinische Informationen ist ausschließlich autorisierten Personen gestattet.

Die Vergabe von Berechtigungen erfolgt nach den Grundsätzen des Need-to-know-Prinzips sowie des Least-Privilege-Prinzips.

Art. 115 Vertraulichkeit

Alle Personen mit Zugang zu medizinischen Informationen sind zur Wahrung der Vertraulichkeit verpflichtet.

Die Schweigepflicht sowie gesetzliche Geheimhaltungsvorschriften bleiben hiervon unberührt.

Art. 116 Speicherung und Übertragung

Medizinische Informationen sind während der Speicherung, Verarbeitung und Übertragung durch geeignete organisatorische und technische Maßnahmen zu schützen.

Die Schutzmaßnahmen richten sich nach der jeweiligen Informationsklassifizierung sowie den gesetzlichen Anforderungen.

Art. 117 Klinische Forschung

Bei klinischen Forschungsvorhaben sind neben den Anforderungen dieses Reglements insbesondere die Vorgaben des Ethikreglements, des Datenschutzreglements sowie der einschlägigen gesetzlichen Bestimmungen einzuhalten.

Art. 118 Protokollierung

Zugriffe auf medizinische Informationssysteme sowie sicherheitsrelevante Änderungen sind entsprechend der Informationsklassifizierung nachvollziehbar zu protokollieren.

Die Protokolle sind vor unbefugter Einsicht oder Veränderung zu schützen.

Art. 119 Sicherheitsvorfälle

Sicherheitsvorfälle mit Bezug zu medizinischen Informationen sind unverzüglich nach den geltenden Melde-, Eskalations- und Incident-Response-Verfahren zu behandeln.

Soweit erforderlich, sind die zuständigen internen und externen Stellen einzubeziehen.

Art. 120 Kontinuierliche Weiterentwicklung

Die medizinische Informationssicherheit ist regelmäßig hinsichtlich ihrer Wirksamkeit zu überprüfen und unter Berücksichtigung neuer medizinischer, technischer, wissenschaftlicher und gesetzlicher Entwicklungen kontinuierlich weiterzuentwickeln.

Kapitel 13 – Hochsicherheitsbereiche und besonders schutzwürdige Informationen

Art. 121 Grundsatz

Informationswerte aus Hochsicherheitsbereichen unterliegen den höchsten Anforderungen an Informationssicherheit.

Sie sind entsprechend ihrer Informationsklassifizierung, ihres Schutzbedarfs sowie ihrer Bedeutung für Mensch, Forschung, Gesellschaft und kritische Infrastrukturen besonders zu schützen.

Art. 122 Hochsicherheitsbereiche

Als Hochsicherheitsbereiche gelten insbesondere:

• biologische Forschung;

• chemische Forschung;

• nukleartechnische Forschung;

• radiologische Forschung;

• medizinische Hochrisikobereiche;

• sicherheitskritische Forschungsprojekte;

• kritische Infrastrukturen;

• weitere durch den Verwaltungsrat oder die Geschäftsleitung bestimmte Bereiche.

Art. 123 Besondere Schutzmaßnahmen

Für Hochsicherheitsbereiche sind zusätzliche organisatorische, personelle, physische und technische Schutzmaßnahmen vorzusehen.

Diese richten sich nach der jeweiligen Informationsklassifizierung sowie den festgelegten Sicherheitsrichtlinien.

Art. 124 Zugriffsregelungen

Der Zugang zu Informationen aus Hochsicherheitsbereichen ist auf ausdrücklich autorisierte Personen zu beschränken.

Die Zugriffsberechtigungen sind regelmäßig zu überprüfen und unverzüglich anzupassen, wenn sich Aufgaben oder Verantwortlichkeiten ändern.

Art. 125 Informationsaustausch

Informationen aus Hochsicherheitsbereichen dürfen ausschließlich über zugelassene und angemessen gesicherte Kommunikationswege ausgetauscht werden.

Vor jeder Weitergabe ist zu prüfen, ob die empfangende Stelle über die erforderliche Berechtigung verfügt.

Art. 126 Speicherung

Informationen aus Hochsicherheitsbereichen sind auf besonders geschützten Informationssystemen oder Datenträgern zu speichern.

Die Schutzmaßnahmen richten sich nach der jeweiligen Informationsklassifizierung sowie den geltenden Sicherheitsrichtlinien.

Art. 127 Transport

Der Transport oder die Übermittlung von Informationen aus Hochsicherheitsbereichen bedarf geeigneter organisatorischer und technischer Schutzmaßnahmen.

Hierbei sind insbesondere Verschlüsselung, Integritätsschutz und sichere Nachverfolgbarkeit sicherzustellen.

Art. 128 Sicherheitsüberprüfung

Für besonders schutzwürdige Informationen sind regelmäßige Sicherheitsüberprüfungen durchzuführen.

Dabei sind insbesondere die Wirksamkeit der Schutzmaßnahmen, mögliche Bedrohungen sowie neue Risiken zu bewerten.

Art. 129 Zusammenarbeit mit weiteren Reglementen

Für Hochsicherheitsbereiche gelten ergänzend insbesondere:

• das Ethikreglement;

• das Datenschutzreglement;

• das Forschungs- und Laborsicherheitsreglement;

• das Compliance-Reglement;

• das Risikomanagement-Reglement;

• weitere einschlägige Reglemente der Yushin-Ryu AG.

Art. 130 Kontinuierliche Weiterentwicklung

Die Sicherheitsmaßnahmen für Hochsicherheitsbereiche sind regelmäßig an neue wissenschaftliche Erkenntnisse, technologische Entwicklungen, gesetzliche Anforderungen sowie veränderte Bedrohungslagen anzupassen.

Kapitel 14 – Informationssicherheitsvorfälle und Incident Management

Art. 131 Grundsatz

Informationssicherheitsvorfälle sind unverzüglich zu erkennen, zu melden, zu bewerten und angemessen zu behandeln.

Ziel ist es, Schäden für Menschen, Forschung, Lehre, Medizin, Verwaltung sowie die Informationswerte der Yushin-Ryu AG möglichst zu verhindern oder auf ein Mindestmaß zu begrenzen.

Art. 132 Informationssicherheitsvorfälle

Als Informationssicherheitsvorfälle gelten insbesondere:

• unbefugte Zugriffe;

• Verlust oder Diebstahl von Informationswerten;

• Datenmanipulationen;

• Datenschutzverletzungen;

• Cyberangriffe;

• Schadsoftware;

• Systemausfälle;

• Sabotage;

• sonstige sicherheitsrelevante Ereignisse.

Art. 133 Meldepflicht

Alle Mitarbeitenden, Forschenden, Lehrenden, Studierenden sowie externe Personen mit Zugang zu Informationswerten sind verpflichtet, Informationssicherheitsvorfälle unverzüglich über die vorgesehenen Meldewege zu melden.

Art. 134 Erstbewertung

Jeder gemeldete Informationssicherheitsvorfall ist unverzüglich hinsichtlich seiner Auswirkungen, Kritikalität sowie seines Schutzbedarfs zu bewerten.

Die Bewertung erfolgt unter Berücksichtigung:

• der Priorität der Schutzgüter;

• der Informationsklassifizierung;

• der möglichen Auswirkungen auf Forschung, Lehre, Medizin und Verwaltung.

Art. 135 Incident Response

Für Informationssicherheitsvorfälle sind geeignete Incident-Response-Verfahren vorzuhalten.

Diese umfassen insbesondere:

• Erkennung;

• Analyse;

• Eindämmung;

• Beseitigung;

• Wiederherstellung;

• Nachbereitung.

Art. 136 Eskalation

Informationssicherheitsvorfälle mit erheblichem Schadenspotenzial sind unverzüglich an die zuständigen Stellen zu eskalieren.

Erforderlichenfalls sind der CIO, der CISO, die Geschäftsleitung, das Krisenmanagement sowie weitere zuständige Stellen einzubeziehen.

Art. 137 Beweissicherung

Bei sicherheitsrelevanten Vorfällen sind geeignete Maßnahmen zur Sicherung von Beweisen zu treffen.

Die Beweissicherung erfolgt nachvollziehbar, vollständig und unter Wahrung gesetzlicher Anforderungen.

Art. 138 Dokumentation

Informationssicherheitsvorfälle sind vollständig und revisionssicher zu dokumentieren.

Die Dokumentation umfasst insbesondere:

• Zeitpunkt;

• Art des Vorfalls;

• betroffene Informationswerte;

• Ursachen;

• eingeleitete Maßnahmen;

• Ergebnisse;

• Verbesserungsmaßnahmen.

Art. 139 Lessons Learned

Nach Abschluss eines Informationssicherheitsvorfalls ist eine strukturierte Nachbereitung durchzuführen.

Festgestellte Schwachstellen sind zu bewerten und geeignete Verbesserungsmaßnahmen einzuleiten.

Art. 140 Kontinuierliche Verbesserung

Erkenntnisse aus Informationssicherheitsvorfällen sind in das Informationssicherheitsmanagement einzubringen.

Prozesse, Schutzmaßnahmen und Sicherheitsrichtlinien sind regelmäßig anhand der gewonnenen Erfahrungen weiterzuentwickeln.

Kapitel 15 – Business Continuity Management und Disaster Recovery

Art. 141 Grundsatz

Die Yushin-Ryu AG stellt durch geeignete organisatorische, personelle und technische Maßnahmen sicher, dass kritische Geschäftsprozesse, Forschungsaktivitäten, Lehrveranstaltungen, medizinische Leistungen sowie Verwaltungsaufgaben auch bei außergewöhnlichen Ereignissen fortgeführt oder innerhalb angemessener Fristen wiederhergestellt werden können.

Art. 142 Business Continuity Management

Für sämtliche kritischen Geschäftsprozesse ist ein Business Continuity Management (BCM) einzurichten und fortlaufend weiterzuentwickeln.

Das BCM ist Bestandteil des integrierten Managementsystems der Yushin-Ryu AG.

Art. 143 Kritische Geschäftsprozesse

Kritische Geschäftsprozesse sind hinsichtlich ihrer Bedeutung für:

• den Schutz des menschlichen Lebens;

• Forschung;

• Lehre;

• Medizin;

• Verwaltung;

• kritische Infrastrukturen;

• Informationssysteme;

• gesetzliche Verpflichtungen

zu identifizieren und regelmäßig zu bewerten.

Art. 144 Notfallplanung

Für kritische Geschäftsprozesse sowie informationsverarbeitende Systeme sind dokumentierte Notfallpläne zu erstellen.

Diese enthalten insbesondere:

• Verantwortlichkeiten;

• Alarmierungswege;

• Eskalationsverfahren;

• Wiederanlaufverfahren;

• Kommunikationswege;

• Ersatzmaßnahmen.

Art. 145 Disaster Recovery

Für informationskritische Systeme sind geeignete Disaster-Recovery-Verfahren einzurichten.

Diese gewährleisten die Wiederherstellung von Informationen, Anwendungen und technischen Infrastrukturen innerhalb der festgelegten Wiederanlaufzeiten.

Art. 146 Datensicherung

Datensicherungen sind regelmäßig entsprechend der Informationsklassifizierung durchzuführen.

Die Wiederherstellbarkeit der Datensicherungen ist in angemessenen Zeitabständen zu überprüfen und zu dokumentieren.

Art. 147 Krisenorganisation

Bei schwerwiegenden Informationssicherheitsvorfällen oder Ausfällen tritt die zuständige Krisenorganisation gemäß Krisenmanagementreglement in Kraft.

Das Business Continuity Management arbeitet hierbei eng mit dem Krisenmanagement zusammen.

Art. 148 Übungen

Business-Continuity- und Disaster-Recovery-Pläne sind regelmäßig durch Übungen, Simulationen oder Tests zu überprüfen.

Erkenntnisse aus den Übungen sind zu dokumentieren und für Verbesserungsmaßnahmen zu nutzen.

Art. 149 Dokumentation

Sämtliche Business-Continuity- und Disaster-Recovery-Maßnahmen sind nachvollziehbar, vollständig und revisionssicher zu dokumentieren.

Die Dokumentation ist regelmäßig zu aktualisieren.

Art. 150 Kontinuierliche Verbesserung

Das Business Continuity Management ist regelmäßig hinsichtlich seiner Wirksamkeit zu überprüfen.

Neue Risiken, technologische Entwicklungen, organisatorische Änderungen sowie Erkenntnisse aus Notfällen und Übungen sind in die Weiterentwicklung des BCM einzubeziehen.

Kapitel 16 – Schulung, Sensibilisierung und Sicherheitsbewusstsein

Art. 151 Grundsatz

Informationssicherheit ist Bestandteil der Unternehmenskultur der Yushin-Ryu AG.

Alle Organe, Führungskräfte, Mitarbeitenden, Forschenden, Lehrenden, Studierenden sowie externe Personen mit Zugang zu Informationswerten sind entsprechend ihren Aufgaben regelmäßig für Informationssicherheit zu sensibilisieren und zu qualifizieren.

Art. 152 Schulungspflicht

Alle Beschäftigten der Yushin-Ryu AG nehmen an den für ihren Tätigkeitsbereich erforderlichen Schulungen zur Informationssicherheit teil.

Die Teilnahme ist regelmäßig zu wiederholen und zu dokumentieren.

Art. 153 Zielgruppenorientierte Schulungen

Schulungen sind entsprechend den jeweiligen Aufgaben und Verantwortlichkeiten durchzuführen.

Besondere Schulungen sind insbesondere vorzusehen für:

• Führungskräfte;

• Forschende;

• medizinisches Personal;

• Laborpersonal;

• IT-Personal;

• Administratoren;

• Mitglieder der Geschäftsleitung;

• externe Dienstleister.

Art. 154 Inhalte der Schulungen

Die Schulungen umfassen insbesondere:

• Informationsklassifizierung;

• Priorität der Schutzgüter;

• Datenschutz;

• Cybersecurity;

• sichere Kommunikation;

• Passwort- und Authentifizierungsverfahren;

• Umgang mit Informationswerten;

• Meldepflichten;

• Verhalten bei Sicherheitsvorfällen.

Art. 155 Sicherheitsbewusstsein

Die Yushin-Ryu AG fördert ein dauerhaftes Sicherheitsbewusstsein durch regelmäßige Informationsmaßnahmen, Schulungen, Übungen sowie interne Kommunikationsmaßnahmen.

Informationssicherheit ist als gemeinsame Verantwortung aller Organisationsmitglieder zu verstehen.

Art. 156 Sensibilisierungsmaßnahmen

Zur Stärkung des Sicherheitsbewusstseins können insbesondere durchgeführt werden:

• Informationskampagnen;

• Phishing-Simulationen;

• Sicherheitsübungen;

• Workshops;

• Fachveranstaltungen;

• E-Learning-Angebote;

• Informationsveranstaltungen.

Art. 157 Nachweis der Qualifikation

Die Durchführung von Schulungen sowie der Erwerb sicherheitsrelevanter Qualifikationen sind angemessen zu dokumentieren.

Erforderliche Nachweise sind entsprechend den geltenden Dokumentationsvorgaben aufzubewahren.

Art. 158 Verantwortung der Führungskräfte

Führungskräfte stellen sicher, dass die ihnen unterstellten Mitarbeitenden über die erforderlichen Kenntnisse zur Informationssicherheit verfügen.

Sie fördern aktiv eine Kultur der Verantwortung und des sicherheitsbewussten Handelns.

Art. 159 Wirksamkeitskontrolle

Die Wirksamkeit der Schulungs- und Sensibilisierungsmaßnahmen ist regelmäßig zu überprüfen.

Hierzu können insbesondere Wissensüberprüfungen, Übungen, Audits sowie Auswertungen von Sicherheitsvorfällen herangezogen werden.

Art. 160 Kontinuierliche Weiterentwicklung

Das Schulungs- und Sensibilisierungskonzept ist regelmäßig an neue Bedrohungen, wissenschaftliche Erkenntnisse, technologische Entwicklungen sowie gesetzliche Anforderungen anzupassen und fortlaufend weiterzuentwickeln.

Kapitel 17 – Audits, Kontrollen und Revisionen

Art. 161 Grundsatz

Die Einhaltung dieses Informationssicherheitsreglements ist regelmäßig durch geeignete Kontroll-, Audit- und Revisionsmaßnahmen zu überprüfen.

Ziel ist die kontinuierliche Sicherstellung der Wirksamkeit, Angemessenheit und Weiterentwicklung des Informationssicherheitsmanagementsystems.

Art. 162 Arten der Überprüfung

Überprüfungen erfolgen insbesondere durch:

• interne Audits;

• externe Audits;

• Management-Reviews;

• Compliance-Kontrollen;

• technische Sicherheitsüberprüfungen;

• Risikobewertungen;

• unangekündigte Stichprobenkontrollen.

Art. 163 Auditplanung

Audits sind risikoorientiert sowie unter Berücksichtigung der Informationsklassifizierung zu planen.

Hochkritische Bereiche sind in angemessenen Zeitabständen häufiger zu überprüfen.

Art. 164 Unabhängigkeit

Audits und Revisionen sind unabhängig, objektiv und nachvollziehbar durchzuführen.

Personen dürfen keine Bereiche auditieren, für deren operative Durchführung sie unmittelbar verantwortlich sind.

Art. 165 Prüfungsumfang

Die Überprüfungen können insbesondere umfassen:

• organisatorische Maßnahmen;

• technische Schutzmaßnahmen;

• physische Sicherheit;

• Dokumentation;

• Berechtigungsmanagement;

• Informationsklassifizierung;

• Datenschutz;

• Cybersecurity;

• Business Continuity Management;

• Einhaltung gesetzlicher Anforderungen.

Art. 166 Feststellungen

Festgestellte Abweichungen, Schwachstellen oder Verbesserungspotenziale sind nachvollziehbar zu dokumentieren.

Die verantwortlichen Organisationseinheiten haben geeignete Korrekturmaßnahmen innerhalb angemessener Fristen umzusetzen.

Art. 167 Nachverfolgung

Die Umsetzung beschlossener Maßnahmen ist regelmäßig nachzuverfolgen.

Nicht fristgerecht umgesetzte Maßnahmen sind entsprechend den Eskalationsverfahren zu behandeln.

Art. 168 Berichterstattung

Die Ergebnisse der Audits und Revisionen sind der Geschäftsleitung sowie den zuständigen Governance- und Kontrollorganen in geeigneter Form vorzulegen.

Schwerwiegende Feststellungen sind unverzüglich zu melden.

Art. 169 Externe Prüfungen

Die Yushin-Ryu AG unterstützt externe Prüfungen durch Akkreditierungsstellen, Zertifizierungsorganisationen sowie gesetzlich zuständige Behörden.

Die hierfür erforderlichen Unterlagen sind vollständig und nachvollziehbar bereitzustellen.

Art. 170 Kontinuierliche Verbesserung

Erkenntnisse aus Audits, Revisionen, Managementbewertungen und Kontrollen sind systematisch in das Informationssicherheitsmanagement einzubringen.

Sie bilden eine wesentliche Grundlage für die kontinuierliche Verbesserung des integrierten Governance-, Compliance-, Qualitäts- und Informationssicherheitsmanagementsystems.

Kapitel 18 – Internationale Zusammenarbeit und Informationsaustausch

Art. 171 Grundsatz

Die Yushin-Ryu AG pflegt nationale und internationale Kooperationen in Forschung, Lehre, Entwicklung und weiteren Tätigkeitsbereichen. Dabei sind Informationssicherheit, Datenschutz, Compliance sowie die Einhaltung dieses Reglements jederzeit sicherzustellen.

Art. 172 Internationale Sicherheitsstandards

Bei internationalen Kooperationen sind die Sicherheitsanforderungen der Yushin-Ryu AG grundsätzlich anzuwenden. Abweichende nationale Vorschriften sind zusätzlich zu berücksichtigen, sofern sie ein gleichwertiges oder höheres Schutzniveau gewährleisten.

Art. 173 Informationsaustausch

Der Austausch von Informationen mit externen Partnern erfolgt ausschließlich auf Grundlage definierter Prozesse und unter Berücksichtigung der jeweiligen Informationsklassifizierung.

Die Übermittlung hat über zugelassene und angemessen geschützte Kommunikationswege zu erfolgen.

Art. 174 Vertraulichkeitsvereinbarungen

Vor dem Austausch vertraulicher oder schutzbedürftiger Informationen sind geeignete Vertraulichkeitsvereinbarungen (NDA) oder vergleichbare vertragliche Regelungen abzuschließen.

Diese Vereinbarungen müssen den Anforderungen der Governance-, Compliance- und Informationssicherheitsvorgaben entsprechen.

Art. 175 Internationale Forschungskooperationen

Internationale Forschungsprojekte sind vor Projektbeginn hinsichtlich ihrer rechtlichen, ethischen, sicherheitsrelevanten und informationsschutzbezogenen Anforderungen zu bewerten.

Besondere Aufmerksamkeit gilt Projekten mit erhöhtem Risiko oder sicherheitsrelevanten Technologien.

Art. 176 Exportkontrolle und Technologietransfer

Beim grenzüberschreitenden Austausch von Technologien, Forschungsdaten oder technischen Informationen sind sämtliche anwendbaren Exportkontroll-, Sanktions- und Genehmigungsvorschriften einzuhalten.

Erforderliche Freigaben sind vor der Übermittlung einzuholen.

Art. 177 Internationale Standorte

Alle internationalen Standorte, Institute, Tochtergesellschaften und Forschungseinrichtungen der Yushin-Ryu AG sind in das zentrale Informationssicherheitsmanagement einzubinden.

Lokale Ergänzungen sind zulässig, soweit sie den zentralen Sicherheitsstandard nicht unterschreiten.

Art. 178 Zusammenarbeit mit Behörden und Organisationen

Die Zusammenarbeit mit Behörden, Akkreditierungsstellen, Zertifizierungsorganisationen sowie internationalen Partnerinstitutionen erfolgt transparent, nachvollziehbar und unter Wahrung der gesetzlichen Geheimhaltungs- und Datenschutzpflichten.

Art. 179 Sicherheitsvorfälle mit internationalem Bezug

Sicherheitsvorfälle mit Auswirkungen auf internationale Kooperationen oder Standorte sind unverzüglich den zuständigen Stellen zu melden.

Erforderliche Maßnahmen zur Schadensbegrenzung und Information der betroffenen Partner sind zeitnah einzuleiten.

Art. 180 Internationale Harmonisierung

Die Yushin-Ryu AG verfolgt das Ziel, ihre Informationssicherheitsstandards weltweit nach einheitlichen Governance-, Compliance- und Qualitätsgrundsätzen auszurichten.

Dabei sind internationale Normen, bewährte Verfahren sowie die strategischen Ziele der Organisation kontinuierlich zu berücksichtigen.

Kapitel 19 – Kontinuierliche Verbesserung (KVP)

Art. 181 Grundsatz

Die Informationssicherheit ist als kontinuierlicher Verbesserungsprozess (KVP) zu verstehen. Sämtliche organisatorischen, technischen und personellen Maßnahmen sind regelmäßig hinsichtlich ihrer Wirksamkeit zu überprüfen und fortlaufend weiterzuentwickeln.

Art. 182 Verbesserungsprozess

Erkenntnisse aus Audits, Sicherheitsvorfällen, Risikobewertungen, Managementbewertungen, Forschungsergebnissen sowie gesetzlichen Änderungen sind systematisch in den Verbesserungsprozess einzubringen.

Art. 183 Fehler- und Lernkultur

Die Yushin-Ryu AG fördert eine offene, verantwortungsbewusste Fehler- und Lernkultur. Sicherheitsrelevante Ereignisse und Verbesserungsvorschläge sind sachlich zu analysieren und zur nachhaltigen Optimierung des Informationssicherheitsmanagements zu nutzen.

Art. 184 Maßnahmenmanagement

Festgelegte Verbesserungsmaßnahmen sind zu dokumentieren, Verantwortlichkeiten zuzuweisen, Prioritäten festzulegen und innerhalb definierter Fristen umzusetzen.

Die Umsetzung ist regelmäßig nachzuverfolgen.

Art. 185 Innovationsmanagement

Neue Technologien, wissenschaftliche Erkenntnisse, internationale Standards und bewährte Verfahren sind fortlaufend auf ihre Eignung zur Verbesserung der Informationssicherheit zu prüfen.

Art. 186 Kennzahlen

Zur Bewertung der Wirksamkeit des Informationssicherheitsmanagements sind geeignete Kennzahlen (Key Performance Indicators – KPI) festzulegen, regelmäßig auszuwerten und im Rahmen des Management-Reviews zu berücksichtigen.

Art. 187 Managementbewertung

Die Geschäftsleitung überprüft das Informationssicherheitsmanagement regelmäßig hinsichtlich Zielerreichung, Wirksamkeit, Ressourceneinsatz und strategischer Weiterentwicklung.

Die Ergebnisse sind zu dokumentieren.

Art. 188 Anpassung des Reglements

Dieses Reglement ist regelmäßig auf Aktualität, Zweckmäßigkeit und Vereinbarkeit mit gesetzlichen, normativen und organisatorischen Anforderungen zu überprüfen.

Erforderliche Anpassungen sind nach den geltenden Governance-Prozessen zu beschließen.

Art. 189 Wissensmanagement

Erfahrungen, Erkenntnisse und bewährte Verfahren aus dem Informationssicherheitsmanagement sind systematisch zu dokumentieren und für Schulungen sowie zukünftige Verbesserungen nutzbar zu machen.

Art. 190 Nachhaltige Weiterentwicklung

Die kontinuierliche Verbesserung verfolgt das Ziel, die Informationssicherheit langfristig an neue wissenschaftliche, technische, organisatorische und internationale Entwicklungen anzupassen und dauerhaft ein hohes Sicherheitsniveau sicherzustellen.

Kapitel 20 – Strategische Informationssicherheit und Governance

Art. 191 Strategische Bedeutung der Informationssicherheit

Die Informationssicherheit ist ein integraler Bestandteil der Unternehmens- und Universitätsstrategie der Yushin-Ryu AG. Sie dient dem nachhaltigen Schutz von Menschen, Wissen, Forschung, Infrastruktur, Vermögenswerten sowie der langfristigen Erfüllung des institutionellen Auftrags.

Art. 192 Integration in die Governance

Das Informationssicherheitsmanagement ist dauerhaft in die Governance-, Compliance-, Qualitätsmanagement-, Risiko- und Sicherheitsstrukturen der Yushin-Ryu AG integriert.

Alle strategischen Entscheidungen sind unter Berücksichtigung der Anforderungen der Informationssicherheit zu treffen.

Art. 193 Strategische Zielsetzung

Die strategische Informationssicherheit verfolgt insbesondere folgende Ziele:

- Schutz von Menschen, Informationen und kritischen Infrastrukturen;
- Sicherstellung der Verfügbarkeit geschäftskritischer Prozesse;
- Erhaltung wissenschaftlicher Integrität;
- Schutz geistigen Eigentums;
- Förderung des Vertrauens von Studierenden, Mitarbeitenden, Forschungspartnern und Behörden;
- Unterstützung einer nachhaltigen internationalen Entwicklung der Organisation.

Art. 194 Internationale Ausrichtung

Die Informationssicherheitsstrategie orientiert sich an anerkannten internationalen Standards sowie bewährten wissenschaftlichen und technischen Verfahren.

Internationale Kooperationen sind nach einheitlichen Governance-Grundsätzen zu gestalten und kontinuierlich weiterzuentwickeln.

Art. 195 Sicherheitskultur

Informationssicherheit ist Bestandteil der Organisationskultur.

Alle Mitarbeitenden, Führungskräfte, Lehrpersonen, Forschenden sowie externe Partner tragen Verantwortung für die Einhaltung und Förderung einer nachhaltigen Sicherheitskultur.

Art. 196 Ressourcen

Die Geschäftsleitung stellt sicher, dass für das Informationssicherheitsmanagement ausreichend personelle, organisatorische, technische und finanzielle Ressourcen zur Verfügung stehen.

Art. 197 Zusammenarbeit der Governance-Bereiche

Informationssicherheit arbeitet eng mit den Bereichen Qualitätsmanagement, Compliance, Datenschutz, Risikomanagement, Arbeitssicherheit, Forschungssicherheit, Ethik sowie den weiteren Governance- und Kontrollorganen zusammen.

Die Zusammenarbeit erfolgt koordiniert, transparent und unter Beachtung klar definierter Zuständigkeiten.

Art. 198 Strategische Weiterentwicklung

Die Informationssicherheitsstrategie wird regelmäßig überprüft und an neue wissenschaftliche Erkenntnisse, technologische Entwicklungen, internationale Anforderungen sowie organisatorische Veränderungen angepasst.

Art. 199 Verantwortung der obersten Leitung

Die oberste Leitung trägt die Gesamtverantwortung für die strategische Ausrichtung und Wirksamkeit des Informationssicherheitsmanagements.

Sie fördert eine Kultur der Verantwortung, Transparenz, Integrität und kontinuierlichen Verbesserung.

Art. 200 Langfristige Sicherung des Informationsschutzes

Die Yushin-Ryu AG verpflichtet sich, Informationssicherheit als dauerhaftes strategisches Führungsprinzip zu verankern.

Das Informationssicherheitsmanagement dient der langfristigen Sicherung von Forschung, Lehre, Innovation, Infrastruktur und institutioneller Stabilität sowie dem Schutz aller Personen und Organisationseinheiten.

Schlussbestimmungen

Art. 201 Inkrafttreten

Dieses Informationssicherheitsreglement tritt mit Beschluss des Verwaltungsrates der Yushin-Ryu AG am festgelegten Datum in Kraft.

Art. 202 Änderungen

Änderungen dieses Reglements bedürfen der Genehmigung durch die zuständigen Governance-Organe der Yushin-Ryu AG.

Alle Änderungen sind nachvollziehbar zu dokumentieren und zu versionieren.

Art. 203 Verbindlichkeit

Dieses Reglement ist für sämtliche Organe, Mitarbeitenden, Lehrpersonen, Forschenden, Studierenden, Tochtergesellschaften sowie beauftragte Dritte verbindlich, soweit sie Tätigkeiten im Auftrag oder im Verantwortungsbereich der Yushin-Ryu AG ausführen.

Art. 204 Übergangsbestimmungen

Bestehende organisatorische Regelungen sind innerhalb der festgelegten Übergangsfristen an die Anforderungen dieses Reglements anzupassen.

Art. 205 Vorrang

Soweit andere interne Regelwerke Regelungen zur Informationssicherheit enthalten, gehen bei Widersprüchen die Bestimmungen dieses Informationssicherheitsreglements vor, sofern keine spezialgesetzlichen oder spezielleren internen Regelungen Anwendung finden.