# *Informationssicherheits-leitlinie*

# *Inhalt*

Die Leitung verabschiedet hiermit folgende Leitlinie zur Informationssicherheit als Bestandteil ihrer Strategie:

# 1 Anlass und Stellenwert der Informationsverarbeitung

Die IT-Strategie von queo ventures GmbH orientiert sich an der Geschäfts- und Risikostrategie des Unternehmens, sodass die Wirkung der IT auf die Geschäftstätigkeit von queo ventures GmbH und nicht das Kostensenkungspotenzial der IT im Vordergrund steht.

Durch die Festlegung der IT-Strategie sowie durch daraus abgeleitete Maßnahmen zur Erreichung der Strategieziele, die unternehmensintern zu veröffentlichen sind, wird auch Klarheit über die Bedeutung der IT für die sichere Durchführung des Tagesgeschäftes geschaffen, die für das IT-Risikobewusstsein notwendig ist.

Informationsverarbeitung spielt eine Schlüsselrolle für unsere Aufgabenerfüllung. Alle wesentlichen strategischen und operativen Funktionen und Aufgaben werden durch Informationstechnik (IT) maßgeblich unterstützt. Ein Ausfall von IT-Systemen muss insgesamt kurzfristig kompensiert werden können. Auch in Teilbereichen darf unser Geschäft nicht zusammenbrechen. Da unsere Kernkompetenz in der Beratung von Marken liegt, ist der Schutz dieser Informationen vor unberechtigtem Zugriff und vor unerlaubter Änderung von existenzieller Bedeutung.

# 2 Übergreifende Ziele

Mit der IT-Strategie soll unter Berücksichtigung der Schutzziele, besonders der Integrität, Verfügbarkeit und Vertraulichkeit das Optimum aus den getätigten Investitionen in die IT herausgeholt werden.

Unsere Daten und unsere IT-Systeme in allen technikabhängigen und kaufmännischen Bereichen werden in ihrer Verfügbarkeit so gesichert, dass die zu erwartenden Stillstandszeiten toleriert werden können. Fehlfunktionen und Unregelmäßigkeiten in Daten und IT-Systemen sind nur in geringem Umfang und nur in Ausnahmefällen akzeptabel (Integrität). Die Anforderungen an Vertraulichkeit haben ein hohes Niveau und erfüllen mindestens Gesetzeskonformität.

Die Standard-Sicherheitsmaßnahmen müssen in einem wirtschaftlich vertretbaren Verhältnis zum Wert der schützenswerten Informationen und IT-Systeme stehen. Schadensfälle mit hohen reputativen Auswirkungen müssen verhindert werden.

Alle Mitarbeitenden des Unternehmens halten die einschlägigen Gesetze (z. B. Strafgesetzbuch, Handelsgesetzbuch, Sozialgesetzbuch, Gesetze und Regelungen zum Datenschutz) und vertraglichen Regelungen ein. Negative finanzielle und immaterielle Folgen für das Unternehmen sowie für die Mitarbeitenden durch Gesetzesverstöße sind zu vermeiden.

Alle Mitarbeitenden sowie die Unternehmensführung sind sich ihrer Verantwortung beim Umgang mit IT bewusst und unterstützen die IT-Strategie nach besten Kräften.

# 3 Interessierte Parteien

Informationssicherheit und deren Management ist eine Unternehmensanforderung, welche von den Interessen verschiedener Gruppen beeinflusst wird.

Mitarbeitende möchten zum einen, dass Ihre persönlichen Informationen durch das Unternehmen angemessen behandelt werden, und zum anderen, dass Sie durch Anweisungen und angemessen konfigurierte Geräte und Dienste in die Lage versetzt werden, sich "sicher" zu verhalten.

Im Sinne von Geschäftsführung und Gesellschaftenden liegt die Betrachtung der Informationssicherheit als Mittel zur Erfüllung von vertraglichen und rechtlichen Anforderungen und zur Aufrechterhaltung und Verbesserung der wirtschaftlichen Lage des Unternehmens.

Im Rahmen unserer Dienstleistungen kommen wir auch mit sensiblen Informationen unserer Kundschaft in Kontakt. Folglich liegt die Sicherheit der uns anvertrauten Informationen in deren größten Interesse.

Behörden und Gesetzgeber stellen Anforderungen an bestimmte Aspekte der Informationssicherheit im Unternehmen, bspw. durch die Anforderung des Nachweises angemessener technischer und organisatorischer Maßnahmen nach Stand der Technik durch die DSGVO, bei der Beachtung von Lizenz- und Patentrecht, den Anforderungen an ordentliche Buchführung und Datenhaltung oder auch die Verwendung und den Export von Kryptografie.

# *4 Detailziele*

Verspätete oder fehlerhafte Managemententscheidungen können weitreichende Folgen nach sich ziehen. Daher ist für das Management bei wichtigen Entscheidungen der Zugriff auf aktuelle Steuerungsdaten wichtig. Für diese Informationen ist ein hohes Sicherheitsniveau in Bezug auf Vertraulichkeit und Integrität sicher zu stellen.

Die Datenschutzgesetze und die Interessen unserer Mitarbeitenden sowie Subunternehmenden verlangen eine Sicherstellung der Vertraulichkeit der Daten der Mitarbeitenden. Die Daten und die IT-Anwendungen der Personalabteilung werden daher einem hohen Vertraulichkeitsschutz unterzogen. Gleiches gilt für die Daten unserer Kundschaft und Geschäftspartner*innen.

In den IT-Richtlinien werden der gesamten Organisation die folgenden Ziele vorgegeben:

- Maximierung der Effizienz und Transparenz durch kontinuierliche Verbesserung
- Minimierung von IT-Gefahrenpotenzialen durch Umsetzung adäquater IT-Standards
- Unternehmensweite Optimierung des IT-Verbundes mittels Plan-Do-Check-Act
- Gestaltung moderner und ergonomischer Arbeitsplätze
- Einhaltung gesetzlicher und aufsichtsrechtlicher Vorschriften und Richtlinien
- Erhöhung der Skalierbarkeit und Verfügbarkeit durch Einsatz ausgelagerter Kompetenzen
- Konsequente Nutzung von Synergien in den IT-Prozessen und IT-Services
- Aufbau von Automatisierung für regelmäßige Prozesse zur Verbesserung von Qualität und Geschwindigkeit (und zur Schonung personeller Ressourcen und Vereinfachung von Prozessen)

Für die Kreation, ebenso wie für den Kundenservice ist die Aufrechterhaltung der Kommunikation nach außen zu der Kundschaft und Geschäftspartner*innen und der Zugriff auf die Kundendatenbank elementar. Die Geschäftsabwicklung darf nicht verzögert oder gar gefährdet werden. Wenn vertraglich festgelegte Fristen nicht eingehalten werden können, kann dies weitreichende negative Folgen haben. Insbesondere eine mangelhafte Verfügbarkeit der IT-Systeme und der Daten, aber auch Fehlfunktionen können zu Erlösminderungen führen. Die Aufrechterhaltung der Kommunikation und der ständige Zugriff auf korrekte Daten für die Mitarbeitenden hat einen hohen Schutzbedarf.

Durch technische Maßnahmen und die hohe Aufmerksamkeit der Mitarbeitenden wird die Vertraulichkeit geschützt und Manipulationen vorgebeugt.

Die Nutzung des Internets zur Informationsbeschaffung und zur Kommunikation ist für uns selbstverständlich. E-Mail dient als Ersatz oder als Ergänzung von anderen Bürokommunikationswegen. Durch entsprechende Maßnahmen wird sichergestellt, dass die Risiken der Internetnutzung möglichst gering bleiben.

# 5 Informationssicherheitsmanagement

Zur generischen Einbindung von Sicherheitsmechanismen in alle Bereiche der Informationsverarbeitung im Informationsverbund der Organisation betreiben wir ein Informations-Sicherheits-Managementsystem – kurz ISMS. Hier werden die definierten Sicherheitsziele mit Maßnahmen versehen und diese wiederum auf Wirksamkeit überprüft.

Zur Erreichung der Informationssicherheitsziele wurde eine Sicherheitsorganisation eingerichtet. Es ist ein Datenschutz- und Informationssicherheitsteam (DIST, siehe Anlage 1) benannt worden, das sich aus einem Datenschutzteam und einem Informationssicherheitsteam zusammensetzt. Das DIST berichtet in dessen Funktion direkt an die IT-Verantwortlichen, die Mitglieder der Geschäftsführung sind.

Dem DIST und den Administrierenden werden von der Leitung ausreichende finanzielle und zeitliche Ressourcen zur Verfügung gestellt, um sich regelmäßig weiterzubilden und zu informieren und die vom Management festgelegten Informationssicherheitsziele zu erreichen.

Die Administrierenden und das DIST sind durch die IT-Benutzenden ausreichend in ihrer Arbeit zu unterstützen.

Das DIST ist frühzeitig in alle Projekte einzubinden, um schon in der Planungsphase sicherheitsrelevante Aspekte zu berücksichtigen.

Die IT-Benutzenden haben sich in sicherheitsrelevanten Fragestellungen an die Anweisungen des DIST zu halten.

Die Mitglieder des Datenschutzteams werden in der Anlage 2 benannt. Für das Datenschutzteam wird ein ausreichend bemessenes Zeitbudget für die Erfüllung der Pflichten zu Verfügung gestellt. Die Organisation vom Datenschutz wird in der Datenschutzleitlinie festgeschrieben.

# 6 Sicherheitsmaßnahmen

Für alle Verfahren, Informationen, IT-Anwendungen und IT-Systeme wird eine verantwortliche Person benannt, die den jeweiligen Schutzbedarf bestimmt und Zugriffsberechtigungen vergibt.

Für alle verantwortlichen Funktionen sind, wenn möglich, Vertretungen einzurichten. Es muss durch Unterweisungen und ausreichende Dokumentationen sichergestellt werden, dass Vertretende ihre Aufgaben erfüllen können.

Gebäude und Räumlichkeiten werden durch ausreichende Zutrittskontrollen geschützt. Der Zugang zu IT-Systemen wird durch angemessene Zugangskontrollen und der Zugriff auf die Daten durch ein restriktives Berechtigungskonzept geschützt.

Computer-Viren-Schutzprogramme werden auf allen IT-Systemen eingesetzt. Alle Internetzugänge werden durch eine geeignete Firewall gesichert. Alle Schutzprogramme werden so konfiguriert und administriert, dass sie einen effektiven Schutz darstellen und Manipulationen verhindert werden. Des Weiteren unterstützen die IT-Benutzenden durch eine sicherheitsbewusste Arbeitsweise diese Sicherheitsmaßnahmen und informieren bei Auffälligkeiten die entsprechend festgelegten Stellen.

Datenverluste können nie vollkommen ausgeschlossen werden. Durch eine umfassende Datensicherung wird daher gewährleistet, dass der IT-Betrieb kurzfristig wiederaufgenommen werden kann, wenn Teile des operativen Datenbestandes verloren gehen oder offensichtlich fehlerhaft sind. Informationen werden einheitlich gekennzeichnet und so aufbewahrt, dass sie schnell auffindbar sind.

Um größere Schäden in Folge von Notfällen zu begrenzen bzw. diesen vorzubeugen, muss auf Sicherheitsvorfälle zügig und konsequent reagiert werden. Maßnahmen für den Notfall werden in einem separaten Notfallvorsorgekonzept zusammengestellt und im Notfallhandbuch angeleitet. Unser wichtigstes Ziel im Störfall ist die Wahrung der Integrität und Vertraulichkeit der Daten. Ziel ist es ferner, auch bei einem Systemausfall kritische Geschäftsprozesse schnellstmöglich wieder anlaufen zu lassen und die Verfügbarkeit der ausgefallenen Systeme innerhalb einer tolerierbaren Zeitspanne wiederherzustellen.

Sofern IT-Dienstleistungen an externe Stellen ausgelagert werden, werden von uns konkrete Sicherheitsanforderungen in den Service Level Agreements vorgegeben. Das Recht auf Kontrolle wird festgelegt. Für umfangreiche oder komplexe Outsourcing-Vorhaben erstellen wir ein detailliertes Sicherheitskonzept mit konkreten Maßnahmenvorgaben.

IT-Benutzende nehmen regelmäßig an Schulungen zur korrekten Nutzung der IT-Dienste und den hiermit verbundenen Sicherheitsmaßnahmen teil. Die Unternehmensleitung unterstützt dabei die bedarfsgerechte Fort- und Weiterbildung.

# 7 Verbesserung der Sicherheit

Das Managementsystem der Informationssicherheit wird regelmäßig auf seine Aktualität und Wirksamkeit geprüft. Daneben werden auch die Maßnahmen regelmäßig daraufhin untersucht, ob sie den betroffenen Mitarbeitenden bekannt sind, ob sie umsetzbar und in den Betriebsablauf integrierbar sind.

Die Leitung unterstützt die ständige Verbesserung des Sicherheitsniveaus. Mitarbeitende sind angehalten, mögliche Verbesserungen oder Schwachstellen an die entsprechenden Stellen weiterzugeben.

Durch eine kontinuierliche Revision der Regelungen und deren Einhaltung wird das angestrebte Sicherheits- und Datenschutzniveau sichergestellt. Abweichungen werden mit dem Ziel analysiert, die Sicherheitssituation zu verbessern und ständig auf dem aktuellen Stand der IT-Sicherheitstechnik zu halten.

# 8 Ressourcen

Die personellen, finanziellen und technischen Kapazitäten werden nach Notwendigkeit, technischer Verfügbarkeit und wirtschaftlicher Machbarkeit schnellstmöglich bereitgestellt und laufend flexibel an den Bedarf angepasst.

Dabei sind alle Abteilungen der Organisation für die durch sie betriebenen oder unterstützten Prozesse und Services einzubinden.

Am Aufbau eines ISMS und dem anschließenden Betrieb werden primär folgende Abteilungen und Rollen beteiligt:

- Geschäftsführung
- IT Abteilung
- Informationssicherheitsteam

Ferner einzubinden sind:
- HR

- Business Administration
- Finance
- EK Compliance und Recht
- Datenschutzteam

# 9 Zuständigkeiten

Verantwortlich für die Sicherheit in der Organisation bleibt immer die Leitung. Es können jedoch im Rahmen der Tätigkeit Teilverantwortlichkeiten delegiert werden. Dies setzt die Erteilung entsprechender Privilegien und Weisungsrechte voraus und erfordert entsprechende Weiterbildungsangebote. Alle Zuständigkeiten sind schriftlich zu regeln.