Dies ist ein Beispiel für eine IT-Sicherheitsleitlinie, und zwar für die Fa. Qualsoft GmbH aus dem Lehrgangsteil 4 des Seminars „Der IT-Sicherheitsbeauftragte“.
Daten zu dieser Firma finden sich in den Seminarunterlagen.
Bitte die Leitlinie nicht verwechseln mit einem Sicherheitskonzept oder einer Sicherheitsrichtlinie!

Informationssicherheitsleitlinie

der Qualsoft GmbH

Unternehmen und Geschäftszweck

Unser Unternehmen ist ein innovativer Dienstleister bei der Entwicklung kundenspezifischer Software.

Unser Unternehmen ist gegliedert in Verwaltung, Marketing/Vertrieb und Software-Entwicklung. Letztere ist auch für den Betrieb unserer IT verantwortlich.

Zurzeit ist Wiesbaden unser zentraler und einziger Standort.

Geltungs-/Anwendungsbereich

Der Wettbewerb verlangt neben der Produktion und Lieferung qualitativ hochwertiger Software auch den Nachweis der Qualität und Sicherheit interner Prozesse. Die vorliegende Informationssicherheitsleitlinie adressiert dieses Erfordernis im Hinblick auf die Sicherheit der Informationsverarbeitung innerhalb unseres Unternehmens. Sie gilt somit für das gesamte Unternehmen.

Anforderungen, Risiken und Ziele

Das Vertrauen unserer Kunden und letztlich unser Geschäftserfolg beruhen darauf, dass wir insbesondere

- die gesetzlichen Vorgaben und hier nicht zuletzt die Datenschutzgesetze einhalten (Compliance),
- unsere Betriebsgeheimnisse schützen,
- die Vertraulichkeit der Daten unserer Kunden wahren,

- unsere Projekte und Dienstleistungen in der geplanten bzw. zugesicherten Zeit abwickeln,
- integere Produkte (Software) sicher ausliefern und archivieren.

Vor diesem Hintergrund ist der Geschäftserfolg unseres Unternehmens davon abhängig, dass wir bestehende Risiken für die genannten Ziele erkennen, durch geeignete Maßnahmen vermeiden bzw. mindern und Restrisiken geeignet behandeln.

Zu den Risiken zählen die unvollständige bzw. nicht korrekte Einhaltung von gesetzlichen Vorgaben, die unbefugte und ggf. unbemerkte Weitergabe von Betriebsgeheimnissen, die Verletzung von Vorgaben unserer Kunden aufgrund von Systemausfall, Datenverlust, unbefugter Preisgabe von Informationen.

Bedeutung der Sicherheit

Vor dem Hintergrund der externen und internen Anforderungen, vor allem aber den Sicherheitsanforderungen unserer Kunden muss Informationssicherheit ein integraler Bestandteil unserer Unternehmenskultur sein.

Jeder Mitarbeiter / jede Mitarbeiterin muss sich der Notwendigkeit der Informationssicherheit bewusst sein und die grundsätzlichen Auswirkungen von Risiken auf den Geschäftserfolg kennen.

Grundsätzliche Regelungen

1. Die Leitung hat zur Umsetzung der Sicherheitsziele eine Stabsfunktion "Informationssicherheit" eingerichtet und dieser die Aufgaben übertragen, einheitliche Vorgaben für den Sicherheitsprozess zu erstellen, für ausreichende Sensibilisierung aller Mitarbeiter/innen zu sorgen, sowie die Einhaltung der Sicherheitsrichtlinien angemessen zu überprüfen bzw. überprüfen zu lassen.

2. Alle Organisationseinheiten wirken jeweils durch einen Vertreter / eine Vertreterin im Sicherheitsforum mit, in dem die wesentlichen Richtlinien und Arbeiten koordiniert werden. Die Leitung dieses Sicherheitsforums obliegt der Stabsfunktion "Informationssicherheit". Insbesondere wird im Sicherheitsforum ein Gesamtsicherheitskonzept erarbeitet und der Leitung zur Genehmigung vorgelegt.

3. Nach Maßgabe dieser Leitlinie ist zunächst jede Organisationseinheit unseres Unternehmens für die Sicherheit der eigenen Daten und deren Verarbeitung verantwortlich ("Informationseigner"). Im Rahmen dieser Verantwortung wird jede Organisationseinheit eine Aufstellung ihrer Assets (Daten, Systeme und Prozesse) anfertigen, eine Risikoanalyse

und -bewertung nach einheitlichem Muster durchführen und in regelmäßigen Abständen sowie nach gravierenden Änderungen aktualisieren.

4. Dort, wo eine Klassifizierung von Informationen und verarbeitender Systeme erforderlich ist, wird in ergänzenden Richtlinien der Umgang mit solchen Informationen und Systemen separat geregelt.

5. Zur Wahrung der Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität (soweit anwendbar) von Daten und Systemen sind auf der Basis der Risikoeinschätzungen geeignete Maßnahmen in einem Sicherheitskonzept darzustellen und geeignet umzusetzen.

6. Durch geeignete technische, organisatorische und infrastrukturelle Maßnahmen ist der Zugang zu sensiblen Systemen, zu Sicherheitszonen und kritischen Infrastruktur-einrichtungen sowie der Zugriff zu kritischen Informationen und Anwendungen zu kontrollieren und nur für Befugte zu ermöglichen. Zutritts- und Zugriffsberechtigungen werden nur nach formalisierten Antragsverfahren bei Bedarf vergeben und entzogen. Dabei sind die Informationseigner einzubinden.

7. Die Mitarbeiter/innen unseres Unternehmens erhalten bei Bedarf für den jeweiligen Arbeitsplatz spezielle Sicherheitsregeln, die insbesondere eine Meldepflicht bei Sicherheitsvorkommnissen beinhalten.

8. Vor dem Hintergrund der oben genannten Sicherheitsziele sind angemessene Nachweise über die Einhaltung aller Sicherheitsmaßnahmen zu erbringen und zu archivieren.

9. Die die Informationssicherheit betreffenden Unterlagen, Berichte, etc. sind einem geordneten Dokumentmanagement zu unterwerfen, in dem die Erstellung, Freigabe, Verteilung, Archivierung geregelt sind.

10. Der Stabsfunktion "Informationssicherheit" wird aufgegeben, der Leitung quartalsweise Berichte über die Sicherheitslage des Unternehmens zuzuleiten.

Verpflichtungen

Die Leitung wird die Sicherheitsorganisation und den Sicherheitsprozess aktiv unterstützen. Unser Unternehmen wird sich an dem Standard ISO 27001 orientieren und die Management-Elemente dieses Standards realisieren. Diese umfassen die Durchführung von regelmäßigen

internen Audits, eine geeignete Dokumentenlenkung, die Managementbewertung und die Anwendung des Modells der kontinuierlichen Verbesserung (PDCA).

Jeder Mitarbeiter / jede Mitarbeiterin ist verpflichtet, die allgemeinen sowie die für den jeweiligen Arbeitsplatz geltenden Sicherheitsrichtlinien zu beachten und einzuhalten.

Die vorliegende Sicherheitsleitlinie ist grundsätzlich nur unternehmensintern zu halten. Bei Bedarf wird die Leitung darüber befinden, ob sie an Dritte (z. B. Kunden, Vertragspartner, Lieferanten) weitergegeben werden kann.

Diese Sicherheitsleitlinie tritt am <Datum> in Kraft.

<Ort, Datum, Unterschrift der Leitung>

Glossar

Sicherheit	Schutz von Informationen, Daten und ggf. Anwendungen vor Verlust von Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität.
Vertraulichkeit	Informationen werden nach Maßgabe des Eigentümers nur an Befugte weitergegeben.
Integrität	Gespeicherte bzw. übertragene Daten sind so geschützt, dass unbefugte bzw. störungsbedingte Änderungen verhindert werden oder zumindest entdeckbar sind. Systeme und Anwendungen sind gegen unbefugte / störungsbedingte Veränderungen geschützt.
Verfügbarkeit	Daten und Anwendungen sind ohne unzumutbare Verzögerung für vorgesehene Verarbeitungen verfügbar.
Authentizität	Der Urheber einer Datei, einer Email etc. kann eindeutig festgestellt werden.