Informationssicherheitsleitlinie

Inhalt

Stellenwert der Informationssicherheit und Bedeutung der Informationstechnologie bei der evasys GmbH

Die evasys GmbH bietet ihren Kunden Softwarelösungen und begleitende Dienstleistungen im Bereich der Beratung, Schulung und des Hostings mit Fokus auf den Einsatz bei Befragung, Prüfung und Qualitätsmanagement. Zu unseren Kunden gehören viele öffentliche Institutionen, denen Informationssicherheit neben der unternehmerischen Grundverantwortung aufgrund ihrer öffentlichen Vorbildfunktion ein besonderes Anliegen ist. Neben der unternehmerischen Verantwortung für den Schutz der Informationswerte unserer Kunden, Dienstleister, Lieferanten, Partner und des eigenen Unternehmens ist der evasys GmbH dieses Kundenbedürfnis nicht nur wichtig, sondern wir unterstützen dieses ausdrücklich. Sowohl im Interesse der evasys GmbH als auch seiner interessierten Parteien wird daher die Informationssicherheit als ein vorrangiges Ziel betrachtet. Folglich ist ein entscheidender Faktor für das Geschäftsansehen, die Risikominimierung und die Konformität mit gesetzlichen Vorgaben, die Sicherstellung eines angemessen hohen Sicherheitsniveaus für die schutzbedürftigen Informationen sowie der sie unterstützenden Prozesse und Systeme.

Aufgrund unserer Softwarelösungen gehören zu den zu schützenden Informationswerten insbesondere die Daten unserer Kunden, die in unserer Software erhoben und über die bereitgestellte Infrastruktur gespeichert und verarbeitet werden. Primäre zu schützende Werte sind deshalb der Schutz der von uns entwickelten und bereitgestellten Software und das Hosting der von unseren Kunden genutzten Systeme.

Um ein angemessen hohes Sicherheitsniveau zu erreichen ist ein vorrangiges Ziel eine sichere Informationstechnologie, welche eine hohe Verfügbarkeit und den technologischen Schutz digitaler Systeme und Daten gewährleistet. Dieses Ziel der hohen Verfügbarkeit, sowie der Vertraulichkeit und Integrität der IT-Systeme und Daten spielt eine führende Rolle bei der Umsetzung der bei der evasys GmbH angewandten Sicherheitsstrategie und erfährt deshalb eine spezielle Beachtung und Regelungstiefe.

Weitere Sicherheitsziele der Informationssicherheit erstrecken sich über die Informationstechnologie hinaus und umfassen:

- die personelle sowie physische Sicherheit,
- den Umgang mit Sicherheitsereignissen,
- das Business Continuity Management und
- die Einhaltung von Vorgaben.

Zur Umsetzung der Sicherheitsziele und zur Gewährleistung und Erhaltung des erforderlichen Sicherheitsniveaus betreibt die evasys GmbH ein Informationssicherheits-Managementsystem (ISMS) und entwickelt es kontinuierlich weiter. Dieses ISMS der evasys GmbH orientiert sich an den Grundlagen der internationalen Norm ISO/IEC 27001 und den empfohlenen Maßnahmen der dazugehörigen Normenreihe. Diese spiegelt den hohen Anspruch der evasys GmbH bezüglich der Umsetzung der Informationssicherheitsmaßnahmen wider und wird durch eine jährliche externe Überprüfung garantiert.

Eine effektive Implementierung der Informationssicherheit ist für die evasys GmbH von zentraler Bedeutung und wird durch eine Unternehmenskultur gefördert, in der die Wichtigkeit von Informationssicherheit in sämtlichen Bereichen und auf allen Hierarchieebenen verstanden und umgesetzt wird. Alle Mitarbeitenden werden in dem jeweiligen Verantwortungsbereich aktiv in die Sicherung der Informationen eingebunden. Die Mitarbeitenden werden kontinuierlich sensibilisiert und geschult, um ein Bewusstsein für Sicherheitsrisiken zu schaffen und sie für die Bedeutung sicherer Handhabung von Informationen zu sensibilisieren. Durch dieses Engagement und Bewusstsein können wir die Vertraulichkeit, Verfügbarkeit und Integrität von Informationen langfristig gewährleisten.

Diese Leitlinie bildet das Fundament für sämtliche Aktivitäten und Maßnahmen im Bereich der Informationssicherheit bei der evasys GmbH. Sie verpflichtet alle Beschäftigten, einschließlich Führungskräfte und Mitarbeitende, und ist somit verbindlich für das gesamte Unternehmen. Zur Erreichung der Informationssicherheitsziele wurde eine Sicherheitsorganisation eingeführt und ein Informationssicherheitsbeauftragter benannt.

Im Rahmen des Auftrags dieser Informationssicherheitsleitlinie hat die Sicherheitsorganisation der evasys GmbH, Prozesse zur Steuerung, Überwachung und Verbesserungen der Informationssicherheit etabliert, sowie hieraus resultierend, risikoorientierte Sicherheitsanweisungen erlassen. Die Sicherheitsorganisation überwacht und verbessert deren Umsetzung und Effektivität kontinuierlich. Der Informationssicherheitsbeauftragte berichtet in seiner Funktion direkt an die Leitungsebene. Die Durchsetzung wird von der Leitungsebene periodisch überprüft und Verstöße werden verfolgt und sanktioniert.

Geltungsbereich

Die Informationssicherheitsleitlinie gilt für die evasys GmbH und die evasys labs Kft.

Ziele und Prinzipien der Informationssicherheit bei der evasys GmbH

Im Folgenden werden die Ziele und Grundsätze als Rahmen für die weitere Ausgestaltung des Regelwerks bei der evasys GmbH festgelegt. Der Fokus liegt dabei auf der Sicherstellung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen. Zusätzlich werden die grundlegenden Prinzipien im Kontext der Informationssicherheit definiert, darunter die Einhaltung von Vorschriften, Funktionstrennung, Eigentümerschaft, Minimierung von Rechten und Diensten, Nachvollziehbarkeit, Reaktionsfähigkeit sowie angemessene Dokumentation.

Ziele der Informationssicherheit

Informationssicherheit bezeichnet den Schutz von Informationen mit dem Ziel, den Geschäftsbetrieb aufrechtzuerhalten und Geschäftsrisiken zu minimieren. Wie zu Anfang beschrieben, gilt die Etablierung und Aufrechterhaltung unseres ISMS zur Wahrung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen. Daher definieren wir folgende

Ziele für das Informationssicherheitsmanagementsystem:

Vertraulichkeit: Die Vertraulichkeit von Informationen der evasys GmbH ist zu wahren, indem sichergestellt wird, dass sensible Daten vor dem Zugriff oder der Offenlegung durch unbefugte Personen geschützt sind.

Integrität: Die Integrität der Informationen der evasys GmbH ist sicherzustellen, sodass diese stets korrekt und vollständig sind und somit den Anforderungen und Erwartungen der Mitarbeitenden, Kunden und Kooperationspartner entsprechen.

Verfügbarkeit: Die Informationen der evasys GmbH sollen jederzeit und zuverlässig für berechtigte Personen zugänglich und nutzbar sein, um die Geschäftsprozesse reibungslos und effizient durchzuführen.

Weitere Eigenschaften wie Authentizität, Zurechenbarkeit, Nicht-Abstreitbarkeit und Verlässlichkeit, die in der ISO/IEC 27001 erwähnt werden könnten, sind größtenteils durch die Wahrung von Vertraulichkeit, Integrität und Verfügbarkeit abgedeckt und werden daher in dieser Leitlinie nicht gesondert definiert.

Prinzipien im Kontext der Informationssicherheit

Folgende Prinzipien sind unter Berücksichtigung von technischen, wirtschaftlichen oder administrativen Rahmenbedingungen angemessen einzuhalten.

Einhaltung von gesetzlichen, externen, vertraglichen und internen Regularien: Regularien für die Informationssicherheit sind zu identifizieren und durch angemessene Maßnahmen umzusetzen.

Funktionstrennung: Für kritische Funktionen in Geschäftsprozessen, die nicht von ein und derselben Person oder Organisationseinheit ausgeführt werden dürfen, ist eine Funktionstrennung durchzuführen. Dies geschieht, indem Funktionen und Verantwortlichkeiten organisatorisch getrennt werden und diese Trennung soweit möglich und sinnvoll technisch unterstützt wird.

Eigentümerschaft: Informationen, Werte und IT-Systeme sowie -Anwendungen sind Eigentümern zugeordnet. Diese haben für ihre organisationseigenen Werte die Verantwortung für die Kontrolle der Erstellung, Entwicklung, Verwendung, Wartung und Sicherheit.

Minimale Rechte: Der Zugang und Zugriff auf Informationen, Systeme und Anwendungen wird auf den notwendigen Personenkreis beschränkt. Berechtigungen sind risikobasiert zu entwickeln. Jede Benutzerin und jeder Benutzer erhält nur für diejenigen Informationen eine Zugriffsberechtigung, die zur Erfüllung der ihr oder ihm zugewiesenen Aufgaben erforderlich ist.

Minimale Dienste: Den Nutzenden (Personen, technischen Usern oder anderen IT-Systemen) von Ressourcen werden nur die Dienste zur Verfügung gestellt, die sie tatsächlich benötigen. Bei der Nutzung von Informationstechnologie bedeutet dies, dass nur die Funktionalität

verfügbar ist, die auch erforderlich ist.

Nachvollziehbarkeit und Nachweisbarkeit: Alle informationssicherheitsrelevanten Aktivitäten und Ereignisse sollen im erforderlichen Umfang nachvollziehbar sein. Aufzeichnungen über informationssicherheitsrelevante Ereignisse dürfen nicht unnachvollziehbar veränderbar sein.

Reaktion: Beim Auftreten von Informationssicherheitsereignissen, ist nach Meldung an das Risikomanagementboard durch das selbige zu reagieren. Durch rechtzeitiges Erkennen sowie adäquate Reaktionen auf Gefährdungen ist eine negative Beeinträchtigung der Informationssicherheit in den Geschäftsprozessen somit zu verhindern bzw. unter Beachtung von Risikoaspekten auf ein akzeptables Niveau zu reduzieren.

Angemessene Dokumentation: Dokumentationen sind in Bezug auf die Detaillierungstiefe stets so zu gestalten, dass ein sachverständiger, aber unternehmensfremder Dritter innerhalb eines angemessenen Zeitraums die vorgesehenen Tätigkeiten nachvollziehen kann.

Organisation des ISMS

Verantwortung für die Informationssicherheit

Die Geschäftsführung ist insgesamt für die angemessene Umsetzung der Informationssicherheit im Unternehmen verantwortlich und unterstützt dabei die geplante Zuweisung der erforderlichen technischen, finanziellen und personellen Ressourcen für die Informationssicherheit. Die Sicherheit von Informationen ist fest in die Strukturen, Hierarchien und Arbeitsabläufe der evasys GmbH integriert. Es ist ein Informationssicherheitsbeauftragter benannt worden. Der Informationssicherheitsbeauftragte berichtet in seiner Funktion direkt an die Geschäftsführung.

Dem Informationssicherheitsbeauftragten und den IT-Administratoren werden von der Leitung ausreichende finanzielle und zeitliche Ressourcen zur Verfügung gestellt, um sich regelmäßig weiterzubilden, zu informieren und die festgelegten Informationssicherheitsziele zu erreichen.

Eigentümer von Informationen, Verfahren und IT-Systemen / -Anwendungen

Im Rahmen von Risikobeurteilungen wird der Schutzbedarf für wesentliche Informationswerte in den Geschäftsprozessen ermittelt. Der Eigentümer trifft Entscheidungen über Zugriffsrechte auf seine Informationen unter Berücksichtigung technischer Restriktionen und administrativer Aspekte sowie der Entwicklung und Umsetzung wirtschaftlicher Lösungen.

Umsetzung des ISMS

Um einem möglichen Risikoeintritt und den dadurch verursachten Schaden vorzubeugen, werden rechtliche, vertragliche, organisatorische, technische, personelle und infrastrukturelle

Risiken zur Informationssicherheit auf Grundlage einer nachvollziehbaren Risikoeinschätzung identifiziert.

Informationssicherheit wird durch die Umsetzung geeigneter Maßnahmen erreicht. Maßnahmen können dabei sein: dokumentierte Entscheidungen in Form von Leitlinien, Richtlinien und Anweisungen oder Prozesse, Verfahren, Organisationsstrukturen sowie technische Software - und Hardwarefunktionen.

Die Maßnahmen müssen angemessen und risikoorientiert eingeführt, umgesetzt, überwacht, auf ihre Wirksamkeit hin überprüft sowie falls nötig verbessert werden. Dadurch soll sichergestellt werden, dass die spezifischen Sicherheitsziele der evasys GmbH erfüllt werden. Die Umsetzungen und Wirksamkeitsprüfungen sind angemessen zu dokumentieren.

Verstöße gegen Regelungen zur Informationssicherheit sind den jeweiligen Vorgesetzten oder dem Risikomanagementboard zu melden. Verhalten, das die Sicherheit von Informationen oder IT-Systemen sowie -Anwendungen gefährdet, kann disziplinarisch oder arbeitsrechtlich geahndet werden.

Um Schäden zu begrenzen bzw. vorzubeugen, muss auf Sicherheitsvorfälle zügig und konsequent reagiert werden. Ziel ist es, kritische Geschäftsprozesse aufrecht zu erhalten und die Verfügbarkeit der Informationen und ausgefallenen Systeme innerhalb einer definierten, tolerierbaren Zeitspanne wiederherzustellen. Maßnahmen für den Notfall werden im Rahmen der Regelungen des Notfall- und Krisenmanagements
zusammengestellt.

Schulungs-, Weiterbildungs- und Sensibilisierungsmaßnahmen für den Umgang mit den Informationen und der verarbeitenden Informationstechnologie sind für die Erreichung der Ziele der Informationssicherheit und die präventive Sicherstellung des Geschäftsbetriebs unabdingbar. Alle Mitarbeitenden sind bezüglich der Gefährdungen im Umgang mit Informationen und der verarbeitenden Informationstechnologie regelmäßig auf geeignete Weise zu sensibilisieren. Die evasys GmbH stellt hierfür adressatengerechte Schulungsprogramme zur Verfügung. Das ISMS Team der evasys GmbH ermöglicht die Teilnahme an Schulungsmaßnahmen und stellt dies sicher.

Wirksamkeitsprüfung des ISMS

Das ISMS wird regelmäßig - jedoch mindestens jährlich - auf Angemessenheit, Aktualität und Wirksamkeit geprüft und durch die Geschäftsführung bewertet. Die Führungsebenen unterstützen die ständige Aufrechterhaltung des Sicherheitsniveaus. Beschäftigte sind angehalten, mögliche Verbesserungen oder Schwachstellen an den jeweiligen Vorgesetzten oder das Risikomanagementboard zu melden.

Durch eine kontinuierliche Aktualitäts- und Angemessenheitsprüfung der ISMS Regelungen und deren Einhaltung wird das erforderliche und angestrebte Sicherheitsniveau gewährleistet. Abweichungen werden mit dem Ziel analysiert, die Sicherheitssituation zu verbessern und ständig auf dem aktuellen Stand der

Sicherheitstechnik zu halten.

Mitwirkungspflichten

Führungskräfte und Mitarbeitende

Alle Führungskräfte und Mitarbeitende der evasys GmbH gewährleisten die Informationssicherheit durch ihr verantwortliches Handeln und halten die für die Informationssicherheit relevanten Gesetze, Vorschriften, Leitlinien, Regelungen, Anweisungen und vertraglichen Verpflichtungen ein.

Jede Führungskraft ist dafür verantwortlich, dass die in ihrem Verantwortungsbereich Beschäftigten die Informationssicherheit entsprechend der geltenden Regelungen umsetzen.

Die Beschäftigten sind verpflichtet, die Maßnahmen zur Informationssicherheit in ihrem Aufgabenbereich umzusetzen und Regeln einzuhalten. Hierbei werden sie durch wiederkehrende sensibilisierende Schulungen und Trainings unterstützt.

Die Geschäftsführung unterstützt die kontinuierliche Verbesserungen im Sicherheitsniveau und ermutigt alle Mitarbeitenden sowie Nutzende der IT-Infrastruktur dazu, potenzielle Verbesserungsmöglichkeiten oder Schwachstellen an die entsprechenden Stellen zu melden.

Lieferanten und Dienstleister

Die evasys GmbH hat für Lieferanten oder Dienstleister, die für die evasys GmbH Leistungen erbringen, risikoorientiert Sicherheitsanforderungen festzulegen.

Umsetzung der Leitlinie

Die evasys GmbH setzt die Anforderungen an die Informationssicherheit aufgrund dieser Leitlinie um. Des Weiteren wird die Leitlinie regelmäßig auf Angemessenheit überprüft und ggf. angepasst.

Inkrafttreten

Die Geschäftsführung hat diese Informationssicherheitsleitlinie als Bestandteil der Unternehmenspolitik in Kraft gesetzt und veröffentlicht.