EOS KSI
Informationssicherheitskonzept

Die Informationsverarbeitung stellt eine Schlüsselrolle für die Aufgabenerfüllung der EOS KSI Inkasso Deutschland GmbH dar. Alle wesentlichen strategischen und operativen Funktionen und Aufgaben werden maßgeblich durch Informationstechnologie unterstützt.

Jede Beeinträchtigung der Informationssicherheit kann die Leistungsfähigkeit der EOS KSI Inkasso Deutschland GmbH mindern oder im Extremfall Geschäftsprozesse ganz zum Erliegen bringen. Dadurch kann der EOS KSI Inkasso Deutschland GmbH oder Dritten (Kunden, säumigen Kunden) erheblicher materieller und immaterieller Schaden zugefügt werden.

Zur langfristigen Sicherung der Informationssicherheit in den Geschäftsprozessen und somit zur Schadensabwehr und Aufrechterhaltung der Leistungsfähigkeit der EOS KSI Inkasso Deutschland GmbH wurde ein ganzheitlicher Informationssicherheitsprozess initiiert, der 2011 in der Zertifizierung nach ISO 27001 (Informationssicherheitsmanagement) als Erweiterung des bestehenden Qualitätsmanagementsystems formal von externer Stelle bestätigt wurde. Der Standard ist in das bereits bestehende QM-System nach DIN EN ISO 9001 integriert. Regelmäßige Kontrollen in Form interner und externer Audits als auch Prüfungsmaßnahmen werden durchgeführt, um die IT-unterstützten Geschäftsprozesse sowie alle Informationen der EOS KSI Inkasso Deutschland GmbH und Dritter vor den beim Einsatz von Informationstechnologie ständig vorhandenen inneren und äußeren Gefährdungen zu schützen. Vertraulichkeit, Integrität und Verfügbarkeit soll hierdurch gewährleistet werden.

Darüber hinaus wird für alle an Geschäftsprozessen Beteiligten oder von diesen Betroffenen die erforderliche Rechtssicherheit geschaffen. Dies kommt den Kunden und säumigen Kunden der EOS KSI Inkasso Deutschland GmbH unmittelbar und mittelbar zugute und fördert das Vertrauen in die Arbeit der EOS KSI Inkasso Deutschland GmbH.

IS ist eine Unternehmensaufgabe. Alle Beschäftigten (Leitungsebene, Führungskräfte und Mitarbeiter) der EOS KSI Inkasso Deutschland GmbH sind daher im Rahmen ihrer Tätigkeiten für die Informationssicherheit verantwortlich und dazu angehalten, sich dieser Herausforderung zu stellen. Schulungen und andere Ausbildungsmaßnahmen unterstützen die Mitarbeiter, den risikogerechten Umgang mit Informationen fortlaufend sicherzustellen. Durch den engen Zusammenhang im Hinblick auf IT-Management, materieller Sicherheit der Gebäude und Betriebsstätten, Erfüllung rechtlicher und behördlicher Auflagen und Kontinuität der Geschäftsabläufe ist es notwendig, dass alle Mitarbeiter sich an die einschlägigen Gesetze (z. B. Strafgesetzbuch, Betriebsverfassungsgesetz, Handelsgesetzbuch, Sozialgesetzbuch, Gesetze und Regelungen zum Datenschutz) halten und vertragliche Regelungen beachten.

Die Hauptverantwortung obliegt dabei der Geschäftsführung der EOS KSI Inkasso Deutschland GmbH, die dadurch auch eine wichtige Vorbildfunktion wahrnimmt. Als unabhängige Instanz ist der/die EOS KSI IS-Manager/-in für die IS-Dokumentation (Leit- und Richtlinien, Standards und Verfahren) verantwortlich und berichtet direkt der Geschäftsleitung.

Informationssicherheit ist ein vitales Interesse und somit ein wichtiges strategisches Ziel für die EOS KSI Inkasso Deutschland GmbH. Die EOS KSI Koordination identifiziert neue Risiken und Compliance-Probleme, treibt IS-Praktiken in den einzelnen Geschäftsbereichen voran, prüft die Eignung von Sicherheitsinitiativen für Geschäftsbereiche und bewertet IS-Aktivitäten vor dem Hintergrund von Geschäftszielen.

EOS KSI
Informationssicherheitskonzept

Schon heute werden folgende die Informationssicherheit betreffenden Maßnahmen bestätigt:

Gebäudesicherheit

- Die komplette Außenhaut aller Gebäude ist mittels Alarmanlage gegen unerlaubten Zutritt gesichert.
- Türen und Tore der Gebäude sind durch Sicherheitsschlösser gesichert.
- Innerhalb der Gebäude gibt es elektronisch gesicherte Bereiche, zu denen nur autorisierte Personen (Vergabe von Zutrittsrechten z. B. für Serverräume, Finanzbereiche) mittels Transponder Zutritt haben.
- Basierend auf Geschäfts- und Sicherheitsanforderungen wurden Regelwerke für die Zugangskontrolle etabliert und dokumentiert. Sie werden regelmäßig kontrolliert.
- Alle Gebäude werden außerhalb der Geschäftszeiten durch einen externen mobilen Wachdienst überwacht.

Daten- und Dokumentensicherheit

- Alle Dokumente und Aufzeichnungen werden gemäß den zertifizierten QM-Prozessen „Lenkung von Dokumenten“ und „Lenkung von Aufzeichnungen“ gelenkt. Sie werden also vor der Herausgabe geprüft, genehmigt und aktualisiert und je nach Inhalt nur autorisierten Personen zur Verfügung gestellt.
- Nach Möglichkeit werden ausschließlich elektronische Dokumente und Aufzeichnungen verwendet, da deren Lenkung sicherer ist.
- Die Aufbewahrung physikalischer Dokumente erfolgt ebenfalls in eigens dafür vorgesehenen, verschließbaren Lagerräumen oder Schränken.
- Unbefugte Dritte haben zu den Räumlichkeiten keinen Zutritt (dokumentierte Zutrittskontrolle).
- Der Austausch elektronischer Daten mit Dritten erfolgt ausschließlich über gesicherte, verschlüsselte Datenleitungen.
- Alle Änderungen an elektronischen Daten werden systemtechnisch nachgehalten und können somit jederzeit nachvollzogen werden.
- Versorgerleitungen für Strom und Telekommunikation, die Informationssysteme versorgen oder die Daten transportieren, sind vor Abhören und Beschädigung geschützt.
- Bei allen Geräten, die Speichermedien enthalten, wird vor der Entsorgung überprüft, ob alle sensiblen Daten und die lizenzierte Software entfernt oder sicher überschrieben wurden.
- Es sind Maßnahmen zur Erkennung und zur Verhinderung vor Schadsoftware umgesetzt. Es gibt Maßnahmen zur Wiederherstellung, und den Benutzern wurde ein angemessenes Bewusstsein vermittelt.
- Um den Informationsaustausch für alle Arten von Kommunikationseinrichtungen zu schützen, wurden geeignete formale Regelungen, Verfahren und Maßnahmen festgelegt.

EDV-Anlagen

- Die EDV-Anlagen befinden sich in speziellen Serverräumen (fensterlose Innenräume), die den modernsten Anforderungen an derartige Räume entsprechen.
- Zu den Räumen haben nur ausgewählte Personen Zutritt. Die Zugangsberechtigung ist schriftlich geregelt.
- Backup-Kopien von Informationen und von Software werden regelmäßig und im Einklang mit der akzeptierten Backup-Methode erstellt und getestet.
- Die Server sind durch USV-/Notstromanlagen geschützt.
- Das Netzwerk wird angemessen verwaltet und kontrolliert, um es vor Bedrohungen zu schützen, um die Sicherheit von Systemen und Anwendungen im Netzwerk zu erhalten sowie um die übertragenen Informationen zu sichern.
- Der Zugriff auf das System ist mit Benutzerkennungen und abgestuften Kennwörtern geschützt. Alle Clients sind durch Kennwörter geschützt.
- Die Kennwörter müssen in regelmäßigen Abständen geändert werden.
- Auf allen Computersystemen sind Virenscanner installiert, die täglich aktualisiert werden.
- Das Netzwerk der EOS KSI ist durch ein mehrstufiges Firewallsystem vor unerlaubten Zugriffen geschützt.
- Die Festplatten aller Laptops sind verschlüsselt und können nur mit Kennwort in Betrieb genommen werden.
- Generell werden zu vernichtende physikalische Dokumente und sonstiger Datenmüll von einem gewerblichen Aktenvernichter entsorgt. Das Unternehmen stattet die EOS KSI Inkasso Deutschland GmbH mit abschließbaren Vernichtungscontainern aus, die regelmäßig abgeholt und gegen leere Container ausgetauscht werden. Dieses Verfahren wird genauestens protokolliert.
- Der Zugang zu den Clients wird durch autorisiertes Personal kontrolliert.
- Es bestehen Zugangsmöglichkeiten nur zu den unmittelbar benötigten Anwendungen und Daten (Access-Rules).
- Der Einsatz von betriebsfremder Medien und Software usw. ist strengstens untersagt; die Computer werden regelmäßig darauf überprüft.
- Ausschließlich Systemadministratoren dürfen nach erfolgter Genehmigung Software installieren.
- Alle organisationseigenen Geräte (Assets) sind eindeutig gekennzeichnet und werden in einem Inventar aller wichtigen organisationseigenen Geräte (Assets) gepflegt.
- Die Zugangsrechte aller Angestellten, Auftragnehmer und Drittbenutzer zu Informationen und informationsverarbeitenden Einrichtungen werden bei Veränderungen angepasst beziehungsweise aufgehoben, wenn ihre Anstellung, Vertrag oder Vereinbarung endet.

Datenschutz und personelle Sicherheit

- Alle Mitarbeiter sind nach dem Bundesdatenschutzgesetz (BDSG) belehrt und haben eine entsprechende Erklärung unterschrieben. Die Erklärung ist Bestandteil des Arbeitsvertrages.
- Alle Abläufe entsprechen den Bestimmungen des BDSG.
- Sicherheitsaufgaben und -verantwortung sind im Einklang mit den Informationssicherheitsgrundsätzen der EOS KSI Inkasso Deutschland GmbH definiert und dokumentiert.

Regelungen für die Mitarbeiter

- Es gelten spezielle Regelungen zum Datenschutz im Telefonverkehr und beim Versenden von Telefaxnachrichten an externe Empfänger.
- Der PC ist beim Verlassen des Arbeitsplatzes zu sperren.
- Kennwörter dürfen nicht weitergegeben werden. Wird ein Kennwort einem Dritten bekannt, muss unverzüglich ein neues Kennwort vergeben werden.
- Der zulässige Gebrauch von Informationen und organisationseigenen Geräten (Assets) in Verbindung mit informationsverarbeitenden Einrichtungen sind für jeden Mitarbeiter geregelt.
- Es gilt der Grundsatz des aufgeräumten Schreibtisches für Papiere und Wechselmedien sowie des leeren Bildschirmes für informationsverarbeitende Einrichtungen.