FUNDING SOLUTIONS

Taking
Funding to the
Next Level

1.2.1
Leitlinie zur Informationssicherheit
(Information Security Policy)

Inhaltsverzeichnis

Inhalt

1. Unternehmen und Geschäftszweck

Als Spezialist für IT-Lösungen und Beratung im Bereich der Refinanzierung von Finanzdienstleistenden sind wir sowohl Marktführende in Deutschland und Österreich für Standardsoftwareprodukte im Bereich Pfandbriefmanagement als auch führende Anbieter von Software für Verbriefungstransaktionen auf Basis verschiedener technologischer Produktlinien.

Neben unseren Softwareprodukten betreiben wir eine Verbriefungsplattform für alle Beteiligten einer Verbriefungstransaktion, um effektiv und sicher die relevanten Daten im Zusammenhang mit diesen Verbriefungstransaktionen zu analysieren und prozessieren.

1.1. Geltungs-/ Anwendungsbereich

Der Markt verlangt neben der Produktion und Lieferung qualitativ hochwertiger Software sowie dem Betrieb einer Plattform auch einen Nachweis über die Qualität und Sicherheit interner Prozesse. Die vorliegende Leitlinie zur Informationssicherheit und die damit verbundenen Dokumente

- TXS Information Security Management System (ISMS)
- TXS IT-Sicherheitskonzept
- TXS Business Continuity Management (BCM)

adressieren dieses Erfordernis im Hinblick auf die Sicherheit der Informationsverarbeitung innerhalb unseres Unternehmens. Sie gilt somit für alle Mitarbeitende des Unternehmens. Vertragspartner*innen, die Dienstleistungen für die TXS im Bereich der Informations- und Kommunikationstechnologie erbringen, werden zur Einhaltung der nachfolgend aufgeführten Anforderungen verpflichtet.

1.2. Anforderungen, Risiken und Ziele

Das Vertrauen unserer Kundinnen und 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 Kundinnen und Kunden wahren,
- stabile Softwareprodukte sicher ausliefern,
- einen sicheren und stabilen Betrieb unserer Plattformen gewährleisten sowie
- unsere Projekte und Dienstleistungen in der geplanten bzw. zugesicherten Zeit abwickeln (SLAs).

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 verbleibende Risiken geeignet behandeln.

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

2. Bedeutung der Sicherheit

Das Informationssicherheitsniveau von TXS wird insgesamt als hoch eingestuft. Diese Einstufung erfolgt aufgrund der Tatsache, dass einerseits alle wesentlichen Funktionen und Aufgaben durch Informationstechnik unterstützt werden und ein Ausfall von Informationssystemen die Aufgabenerfüllung nicht beeinträchtigen darf und dass andererseits in einigen Organisationseinheiten personenbeziehbare oder personenbezogene Daten verarbeitet werden (Auftragsdatenverarbeitung).
Vor dem Hintergrund der externen und internen Anforderungen, vor allem aber den Sicherheitsanforderungen unserer Kundinnen und Kunden, muss Informationssicherheit ein integraler Bestandteil unserer Unternehmenskultur sein.

Jeder Mitarbeitende muss sich des hohen Stellenwertes und der Notwendigkeit der Informationssicherheit für die TXS, ihrer Kundinnen und Kunden und Partner*innen bewusst sein, die einschlägigen Regeln und Vorgaben im Unternehmen befolgen und die grundsätzlichen Auswirkungen von Risiken auf den Geschäftserfolg kennen.

2.1. Grundsätzliche Regelungen

Die Geschäftsleitung hat zur Umsetzung der Sicherheitsziele eine Informationssicherheitsbeauftragte (ISB) benannt und ihr die Aufgabe übertragen, einheitliche Vorgaben für die Informationssicherheit zu erstellen, für ausreichende Sensibilisierung aller Mitarbeitenden zu sorgen, sowie die Einhaltung aller Sicherheitsrichtlinien angemessen zu überprüfen bzw. überprüfen zu lassen.

Zur Unterstützung der Informationssicherheitsbeauftragten wurde ein Informationssicherheit- und Datenschutz Team (IDT) etabliert. Neben dem Datenschutzbeauftragten (DSB) wirken alle Organisationseinheiten jeweils durch einen Vertretenden mit, indem die wesentlichen Richtlinien und Arbeiten rund um die Informationssicherheit koordiniert werden. Insbesondere wurde im Sicherheitsgremium ein Managementsystem der Informationssicherheit erarbeitet und der Geschäftsleitung zur Genehmigung vorgelegt bzw. laufend aktualisiert.

Nach Maßgabe dieser Leitlinie ist jede Organisationseinheit unseres Unternehmens für die Sicherheit und den Schutz der eigenen Daten und deren Verarbeitung verantwortlich ("Informationseigner*in").

Im Rahmen dieser Verantwortung hat jede Organisationseinheit eine Aufstellung ihrer Assets (Daten, Systeme und Prozesse) angefertigt, eine Risikoanalyse und -bewertung der Ergebnisse nach vorgegebenem einheitlichen Muster durchgeführt und aktualisiert diese in regelmäßigen Abständen sowie nach gravierenden Änderungen.

Dort wo eine Klassifizierung von Informationen und verarbeitender Systeme erforderlich ist, wurde der Umgang mit solchen Informationen und Systemen in einer separaten Richtlinie geregelt.

Zur Wahrung der Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität (soweit anwendbar) von Daten und Systemen werden auf der Basis der Risikoeinschätzungen geeignete Maßnahmen in einem Sicherheitskonzept dargestellt und umgesetzt. Die Informationssicherheitsbeauftragte ist frühzeitig in alle Projekte einzubinden, um schon in der Planungsphase sicherheitsrelevante Aspekte zu berücksichtigen. Sofern personenbeziehbare oder personenbezogene Daten betroffen sind, gilt gleiches für den Datenschutzbeauftragten.

Durch geeignete technische, organisatorische und infrastrukturelle Maßnahmen ist der Zugang zu sensiblen Systemen, zu Sicherheitszonen und kritischen Infrastruktureinrichtungen 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 oder entzogen. Dabei sind die Informationseigner*innen einzubinden.

Die Mitarbeitenden unseres Unternehmens erhalten bei Bedarf für den jeweiligen Arbeitsplatz spezielle Sicherheitsregeln, die insbesondere eine Meldepflicht bei Sicherheitsvorkommnissen beinhalten. Alle Mitarbeitenden haben regelmäßig an den angebotenen Sicherheitsschulungen teilzunehmen.

Vor dem Hintergrund der oben genannten Sicherheitsziele sind angemessene Nachweise über die Einhaltung aller Sicherheitsmaßnahmen zu erbringen und zu archivieren. Die die Informationssicherheit betreffenden Unterlagen, Berichte etc. sind einem geordneten Dokumentenmanagement zu unterwerfen, in dem die Erstellung, Freigabe, Verteilung, Archivierung der Unterlagen und Dokumente geregelt sind.

Der Informationssicherheitsbeauftragten wird aufgegeben, der Geschäftsleitung regelmäßig Berichte über die Sicherheitslage des Unternehmens zuzuleiten.

2.2. Verbesserung der Sicherheit

Das Managementsystem der Informationssicherheit wird regelmäßig auf seine Aktualität und Wirksamkeit hin 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 Geschäftsleitung unterstützt die ständige Verbesserung des Managementsystems der Informationssicherheit und somit 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.

3. Verpflichtungen

Die Geschäftsleitung unterstützt die Sicherheitsorganisation und den Sicherheitsprozess aktiv und uneingeschränkt.

Unser Unternehmen orientiert sich an dem VDA-ISA TISAX-Modell für Informationssicherheit, welches auf dem Standard ISO 27001 basiert, und hat ein Managementsystem der Informationssicherheit (ISMS) etabliert und lässt dieses regelmäßig auditieren und zertifizieren.

Jeder Mitarbeitende ist verpflichtet, die allgemeinen sowie die für den jeweiligen Arbeitsplatz geltenden Sicherheitsrichtlinien zu beachten und einzuhalten.

Diese Sicherheitsleitlinie trat am 20. April 2020 in Kraft und wurde zu diesem Zeitpunkt in der Version 2.0 das erste Mal veröffentlicht.