ATOSS

CODE OF SUPPLIER INFORMATION SECURITY

Sicherheitsinformationen

Öffentliche Fassung v. 04-2024

Als international agierendes Softwareunternehmen hat ATOSS hohe Anforderungen an die Informationssicherheit zu erfüllen.

Dieser Code of Supplier Information Security ist hierbei ein notwendiger Bestandteil unseres Informationssicherheits-managements, um unseren Endkunden die höchstmögliche Informationssicherheit gewährleisten zu können. Nach dem ISO/IEC:27001-Standard sind wir zugleich dazu verpflichtet, unsere geltenden Informationssicherheitsstandards in den Vertragsbeziehungen mit unseren Geschäftspartnern, Leiharbeitern und Lieferanten (kurz: **Lieferanten**) zu adressieren.

Die nachfolgenden Sicherheitsinformationen dienen dazu, Sie über unsere Sicherheitsstandards zu informieren und aufzufordern, diese Standards im Geschäftsverhältnis mit ATOSS zu beachten.

Den aktuellen Code of Supplier Information Security (CoSS) finden Sie jederzeit abrufbar auf der ATOSS Security Webseite.

Wir bitten Sie, diese Informationen zur Kenntnis zu nehmen und zu beachten.

Wir bedanken uns für Ihre Unterstützung!

Ihr ATOSS IT Compliance Team

A. Informationssicherheit

Die nachfolgenden Sicherheitsstandards sind ein Grundpfeiler unseres Lieferantenmanagements auf Basis der ISO/IEC 27001-Zertifizierung.

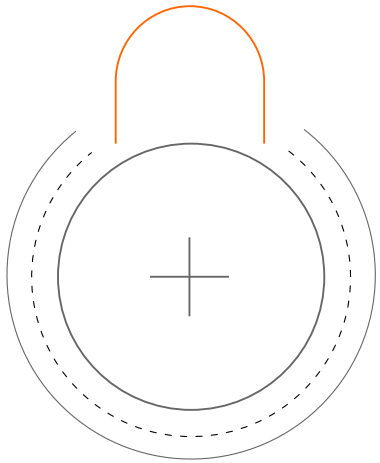
Wir geben einen Überblick über unser Informationssicherheitsverständnis und unsere Grundsätze, die wir von unseren Lieferanten in Bezug auf die Erbringung von Informations- und Kommunikations-Technologie (ICT-) Leistungen erwarten. Das gilt insbesondere, wenn Lieferanten an den ATOSS Standorten oder via Remote-Zugriff bei ATOSS tätig sind oder diese sensible Informationen im Auftrag von ATOSS verarbeiten.

Unser Code of Supplier Information Security ist als ein gemeinsamer Orientierungsrahmen zu verstehen, der hilft, eine angemessene Informationssicherheitsstrategie in Projekten und Lieferanten-beziehungen zu verwirklichen.

Die Verantwortung für die Pflege und Überwachung unserer internen Informationssicherheitsstrukturen obliegt insoweit dem beauftragenden ATOSS Fachbereich als Business Owner.

Zugleich erwarten wir von unseren Lieferanten, mit uns einen engen Kontakt zu pflegen und uns bei den wesentlichen Anforderungen in allen Projektphasen, einschließlich dem laufenden Betrieb und während der gesamten Vertragslaufzeit der Lieferantenbeziehung im gegenseitigen Interesse einer sicheren Leistungsbeziehung zu unterstützen und die Einhaltung der nachfolgenden Sicherheitsinformationen sicherzustellen.

ATOSS hat das Recht, jederzeit ergänzende Sicherheitsanweisungen über Art, Umfang und Verfahren der unternehmerischen Aktivitäten zu erteilen.



Bei der Leistungserbringung sollen unsere Lieferanten den folgenden Sicherheitsgrundsätzen Sorge tragen:

Stand der Technik: Unter Berücksichtigung der konkreten Leistungserbringung sollen unsere Lieferanten angemessene Sicherheitsmaßnahmen nach dem aktuellen Stand der Technik treffen und ihre Effektivität fortlaufend überwachen. Diese Vorgabe dient dazu, ein angemessenes Sicherheitsniveau zugunsten der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der ATOSS Systeme und involvierten sensiblen Informationen zu gewährleisten.

Um diese Anforderung nachvollziehbar zu erfüllen, sollen sich die organisatorischen und technischen Sicherheitsmaßnahmen, an etablierten technischen Richtlinien und Best Practices, wie z.B. die Handreichungen der TeleTrust und dem BSI, nach geltenden ISO-Standards oder nach weiteren einschlägigen gesetzlichen und branchenspezifischen Anforderungen (z.B. Informationssicherheits-anforderungen für kritische Infrastrukturen, etc.) ausrichten.

Korrekter Umgang mit sensiblen Daten: Von ATOSS vorgelegte Schutzklassenkonzepte zum korrekten Umgang und eine Klassifizierung von digitalen und physischen Daten sind zu berücksichtigten. Insbesondere ist die Verarbeitung von sensiblen Dokumenten nur mit Zustimmung des internen ATOSS Ansprechpartners sowie im Rahmen der getroffenen Geheimhaltungsvereinbarung erlaubt.

Korrekte Nutzung von IT-Systemen: Nur von ATOSS IT freigegebene Hardware, Netzwerke und Anwendungen sind an das IT-Firmennetzwerk anzuschließen. Dazu zählen auch von ATOSS IT genehmigte VPN-Verbindungen oder die Nutzung des Gäste-WLAN. Der Lieferant trägt im Zweifel die Beweislast für die erteilte Freigabe.

An den ATOSS Standorten sind in der Regel Bild-, Video- und Tonaufzeichnungen (z.B. durch Nutzung von Smartphones, Videokameras) nicht erlaubt. Ausnahmen bedürfen einer dokumentierten Erlaubnis. Via Remote-Zugriff ist das Anfertigen von Screenshots oder Mitschnitten der Sessions nicht gestattet.

Datenverarbeitungen: Werden ATOSS Daten von Lieferanten oder genehmigten Sub-Lieferanten gehostet, müssen die ATOSS Daten von den Daten anderer Kunden getrennt gespeichert, verarbeitet und übermittelt werden. Beauftragt ein Lieferant einen Sub-Lieferanten mit der Durchführung bestimmter Verarbeitungstätigkeiten, so muss diese Beauftragung im Wege eines Vertrags erfolgen, der dem Sub-Lieferanten im Wesentlichen dieselben Datenschutz- und Informationssicherheitspflichten auferlegt wie diejenigen, die für den Lieferanten gelten.

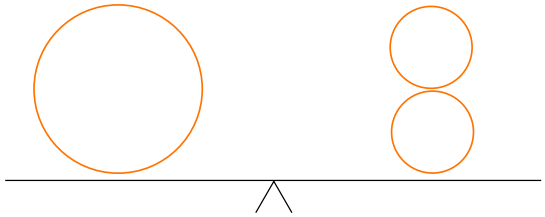
Meldung von Sicherheitsvorfällen: Essentieller Bestandteil unseres Informationssicherheitsmanagements ist die rechtzeitige Information über Sicherheitsvorfälle, damit ATOSS geeignete Maßnahmen ergreifen kann. Somit ist es für ATOSS ausschlaggebend, dass Sicherheitsvorfälle unverzüglich unter Angabe des Sachverhalts an ATOSS gemeldet werden. Das Online-Kontaktformular finden Sie hier.

B. Personelle Sicherheitsanforderungen

Beim Einsatz von Personal sollen unsere Lieferanten für die folgenden Sicherheitsgrundsätze Sorge tragen:

Kontaktstelle für Informationssicherheit: Es ist eine für die Informationssicherheit verantwortliche Kontaktstelle zu benennen, an die Informationssicherheitsbelange über allgemein zugängliche Quellen (z.B. Kontakt ID auf Website) übermittelt werden können. Ist ein Kontakt nicht über allgemein zugängliche Quellen möglich, soll der Lieferant andere Kontaktmöglichkeiten mitteilen und diese aktuell halten.

Qualifikation: Es soll ausschließlich zuverlässiges und fachkundiges Personal für die Erfüllung des Auftrags bei ATOSS sowie damit in Zusammenhang stehender Leistungen (z.B. Administration von IT-Systemen, interne Wartungsarbeiten) tätig werden. Über personelle Änderungen ist zu informieren.



Schulungen: Der Lieferant soll durch regelmäßige Schulungen zur Informationssicherheit und Datenschutz sicherstellen, dass die für ihn tätigen Personen bei Aufträgen von ATOSS auf ihre Verantwortung und Verpflichtungen in Bezug auf die Informationssicherheit hingewiesen wurden und mit den einschlägigen Bestimmungen zur Informationssicherheit, zum Datengeheimnis und Datenschutz vertraut sind.

Vertraulichkeit: Jede für den Lieferanten tätige Person, der sensible Informationen von ATOSS im Rahmen der Auftragserledigung offengelegt werden müssen, ist zur Vertraulichkeit durch den Lieferanten zu verpflichten. Diese Geheimhaltungsverpflichtung besteht auch nach Ende der Vertragsverhältnisse fort und kann auf Anfrage jederzeit nachgewiesen werden.

Kundgabe: Der Lieferant gibt diese Sicherheitsinformationen sowie die einschlägigen Anforderungen zum Datenschutz und zur Informationssicherheit aus der Kundenvereinbarung mit ATOSS an das eingesetzte Personal weiter. Das Gleiche gilt, wenn ATOSS ergänzende Sicherheitsanweisungen über Art, Umfang und Verfahren der unternehmerischen Aktivitäten erteilt.

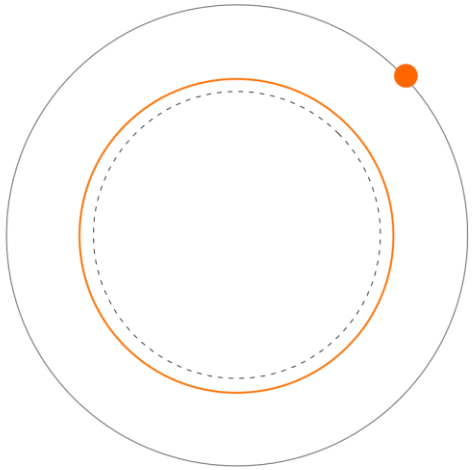
C. Sicherheit von IT-Systemen und Netzwerken

Sichere Betriebsumgebungen: Sofern IT-Systeme oder Netzwerke von Lieferanten für die Generierung, Übertragung oder Speicherung von ATOSS Daten zum Einsatz kommen, sollen unsere Lieferanten geeignete angemessene Sicherheitsmaßnahmen für ihre IT-Systeme und Netzwerk nach dem aktuellen Stand der Technik treffen und diese fortlaufend überwachen.

Folgende Mindestmaßnahmen sollen unsere Lieferanten in Bezug auf Daten von ATOSS im Einsatz haben:

- Patch-, Kapazitäts- und Schwachstellenmanagement
- Datensicherungen
- Zugriffs- und Berechtigungsmanagement
- Rechte- und Rollenkonzepte
- Sicheres Passwortmanagement
- Kommunikationssicherheit
- Einsatz von Kryptographie
- Malwareschutz
- Aktive Protokollierungen und Monitoring
- Vorkehrungen zur physischen Sicherheit (z.B. Schutz gegen Hitze, Feuer und Wasser von relevanten informationsverarbeitenden IT-Systemen)
- Notfallmanagement

Sicherheitsüberprüfungen: Unsere Lieferanten können die Einhaltung dieser Mindestmaßnahmen gegenüber ATOSS jederzeit nachweisen. Ein Nachweis in aller Regel durch Vorlage eines Prüftestats, ein Auditbericht unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzauditor, Pentestbericht) oder eine Zertifizierung - z.B. nach ISO/IEC:27001 oder BSI-Grundschutz - möglich. Auf Wunsch und in begründeten Fällen bleiben ATOSS eigenständige Sicherheitsprüfungen vorbehalten.



D. Sichere Softwareentwicklung

Lieferanten, die Leistungen in Zusammenhang mit unserer Softwareentwicklung erbringen oder an ATOSS Software-programme lizenzieren, sollen für die folgenden Software-entwicklungsgrundsätze Sorge tragen:

Sichere Softwarentwicklungsumgebung: Programmentwicklungen sollen in einer sicheren Entwicklungsumgebung (z.B. Zugriffskonzept auf Source Code, Versionskontrolle) erfolgen. Es sollen sichere Repositories eingesetzt werden.

Richtlinien zur sicheren Softwareentwicklung: Die Entwickler unserer Lieferanten sollen Sicherheitsrichtlinien und Best Practices zur sicheren Softwareentwicklung (z.B. Security und Privacy by Design, Principle of Least Privilege, Segregation of Duties) berücksichtigen.

Code Reviews: Auf Basis einer definierten Softwareentwicklungsmethodik sollen unsere Lieferanten regelmäßige Überprüfungen (z.B. Code Reviews) der von ihnen lizenzierten Softwareprogramme sicherstellen und erkannte Schwachstellen behandeln.

Softwarepflege: Softwarepflege und -support darf ausschließlich über von ATOSS IT freigegebene Remote-Zugriffe erfolgen. Alle Ferngriffe müssen protokolliert werden.

Dokumentationspflichten: Relevante Dokumentations-anforderungen sollen vertraglich berücksichtigt werden.

ATOSS.COM