Atos
IT-Sicherheitsanforderungen an Partner und Lieferanten

Version: 2.5_März 2022
(internal reference: DEM-SEC-0058_Version: 2.5_May 2021)

Content

1. Einführung

1.1. Zweck

Dieses Dokument ist ein Bestandteil der Sicherheitsrichtlinien und -leitlinien der Atos-Gruppe (abgestimmt auf die Sicherheitsleitlinien der Charta of Trust[1]), die für alle Atos-Partner und -Lieferanten bestimmt sind.

Diese Richtlinie legt fest, wie der Zugriff auf Atos-interne Informationen, Atos-Kundeninformationen und alle damit verbundenen Systeme durch Atos-Partner und -Lieferanten kontrolliert wird.

1.2. Umfang

Diese Richtlinie gilt für alle Partner und Lieferanten weltweit, die mit Atos/oder für Atos arbeiten.

Dies ist eine grundlegende Richtlinie und ersetzt keine anderen Dokumente, bei denen der Zugriff auf Kundeninformationen eine höhere Sicherheitsbeschränkung vorschreibt (z.B. geheime Informationen von offiziellen Stellen).

1.3. EU GDPR Konformitätserklärung

Alle personenbezogenen Daten MÜSSEN auf der Grundlage der Anweisungen des für die Verarbeitung Verantwortlichen (Atos=Controller) in Übereinstimmung mit den GDPR-Kontrollen der EU geschützt werden.

1.4. Bestimmte Zielgruppe

Alle Partner und Lieferanten von Atos sind an diese Richtlinie, die "Allgemeine Richtlinie für alle Partner und Lieferanten von Atos" in Kapitel 2 und an alle oder einen Teil der spezifischen Zielgruppen gebunden, je nach Art der Dienstleistung:

- Partner und Lieferanten mit einem Arbeitsplatz bei Atos - Kapitel 3,
- Partner und Lieferanten, die an eigenen Systemen (z.B. PC, Notebook) arbeiten - Kapitel 4,
- Partner und Lieferanten mit einem Link zu Ressourcen innerhalb des Atos-Intranets (z.B. Online-Zugriff aus ihren eigenen Systemen) - Kapitel 5.

1.5. Verantwortlichkeiten von Partnern und Lieferanten

Atos Partner und Lieferanten MÜSSEN ihre Mitarbeiter anweisen, dieses Dokument einzuhalten und alle notwendigen Kontrollen durchführen, um die Einhaltung dieses Dokuments durch ihre Mitarbeiter zu überprüfen.

Um die Effizienz der Geschäftsprozesse von Atos zu unterstützen, gibt es Fälle, in denen es notwendig ist, Partnern und Lieferanten Zugang zu internen und Atos-Kundeninformationen zu gewähren. Dies reduziert nicht die Anforderung, einen wirksamen Schutz zu gewährleisten, um vor unbefugtem Zugriff zu schützen, Datenverluste zu verhindern (einschließlich, aber nicht beschränkt auf, unbefugtes Kopieren, Löschen, ungünstige Manipulationen) oder die Einführung (bösartiger oder anderer) unbefugter Software und Malware.

Die Einhaltung der Informationssicherheitsrichtlinien von Atos unterliegt der Überwachung. Die Nichteinhaltung kann dazu führen, dass Partnern und Lieferanten der Zugang zu den Atos-Standorten oder zum Zugriff auf die Atos-Systeme untersagt wird und Rechtsfolgen und Schadenersatzansprüche nach sich zieht.

[1] Für weitere Informationen besuchen Sie bitte die Website www.charter-of-trust.com

Es liegt in der Verantwortung der Partner und Lieferanten, die Atos-Sicherheitsanforderungen auch gegenüber ihren Partnern, Lieferanten und Mitarbeitern zu kaskadieren.

Eine Kopie dieser Anforderungen wird Atos-Kunden auf Anfrage zur Verfügung gestellt, damit sie die Sicherheitsanpassung an ihre eigenen Richtlinien sowie Audits gemäß den Vertragsbedingungen gewährleisten können.

1.6. Dokumentenpflege und -verteilung

Dieses Dokument "ATOS-Sicherheitsanforderungen an Partner und Lieferanten" wird im Atos-Intranet veröffentlicht und ist für alle Atos-Mitarbeiter zugänglich. Für Partner und Lieferanten wird das Dokument mit den Vertragsunterlagen übergeben.
Dieses Dokument MUSS mit allen Atos Request For Proposal (RFP) und Atos Request For Information (RFI) bereitgestellt werden, damit Partner und Lieferanten beurteilen können, wie die Atos-Anforderungen für die vorgesehene Dienstleistung/das vorgesehene Unternehmen am besten erfüllt werden können.

Dieses Dokument MUSS den Verträgen von Atos als Verpflichtung gegenüber Partnern und Lieferanten beigefügt werden (in gleichem Maße empfiehlt Atos seinen Partnern und Lieferanten, dieses Dokument den Verträgen seiner eigenen Lieferanten beizufügen).

1.7. Schlüsselwörter

Partner sind Unternehmen, die sich die Markteinführung mit Atos teilen. Insofern kann es sich um einen Lieferanten, einen Unterauftragnehmer oder einen Konsortialpartner handeln. Nicht enthalten sind andere Partner, die unter dem Namen "Handelsvertreter" zusammengefasst sind.

Ein **Lieferant** ist ein Nicht--Atos-Unternehmen, das Waren und Dienstleistungen liefert, um zur Gestaltung, Umstellung, Erbringung und Verbesserung von Dienstleistungen oder Prozessen beizutragen, ohne direkten Bezug zu einem zwischen Atos und einem Kunden abgeschlossenen Hauptvertrag. Es kann von einem Auftragnehmer oder Subunternehmer unterschieden werden, der üblicherweise spezialisierte Leistungen zu den Ergebnissen hinzufügt. Die Lieferantendefinition beinhaltet gegebenenfalls eigene Subunternehmer.

Ein **Konsortialpartner** ist ein mit Atos verbundenes Unternehmen, das an einer gemeinsamen Aktivität teilnimmt oder seine Ressourcen zur Erreichung eines gemeinsamen Ziels bündelt (spezifische Ausschreibung, etc.).

Sie wird sowohl in der Pre-Sales-Phase des jeweiligen Projekts als auch an der Durchführung des Projekts beteiligt sein.

Die meisten Partner der Gruppe sind Software- und Hardwarelieferanten. Darüber hinaus gibt es Dienstleister, die der Gruppe mit spezifischem Know-how helfen.

Personenbezogene Daten sind alle Informationen über eine identifizierte oder identifizierbare natürliche Person ("betroffene Person"); eine identifizierbare Person ist eine Person, die direkt oder indirekt identifiziert werden kann, insbesondere durch Bezugnahme auf eine Identifikationsnummer oder auf einen oder mehrere Faktoren, die spezifisch für ihre physische, physiologische, mentale, wirtschaftliche, kulturelle oder soziale Identität sind!

Soll, **MUSS**, **darf nicht** oder **darf nicht** sein: strenge Regel, Verpflichtung.

Sollte oder **sollte nicht**: Die Umsetzung dieser Maßnahmen ist zwingend vorgeschrieben, es sei denn, es liegen triftige geschäftliche Gründe dafür vor (z.B. aufgrund technischer Einschränkungen und wenn die Abweichung formell dokumentiert und genehmigt wird).

Kann oder **darf nicht**: optional, zu berücksichtigen.

2. Allgemeine Sicherheitsanforderungen für alle Partner und Lieferanten von Atos

2.1. Einführung in die Charter of Trust

Um die digitale Welt sicherer zu machen, haben sich Atos und große führende globale Unternehmen aus dem privaten und öffentlichen Sektor im Rahmen der globalen Cybersicherheitsinitiative Charter of Trust zusammengeschlossen.

Die Charter of Trust stellt eine beispiellose Initiative dar, die drei Hauptziele festlegt:

- Schutz personenbezogener Daten und Geschäftsdaten einschließlich sensibler Daten
- Um Schäden für Menschen, Unternehmen, Vermögenswerte und Infrastrukturen zu vermeiden.
- Schaffung einer zuverlässigen Grundlage, auf der das Vertrauen in eine vernetzte, digitale Welt Fuß fassen und wachsen kann.

Durch die Mitbegründung der Charter of Trust fördert Atos die Notwendigkeit des Bewusstseins für Cybersicherheit und die Notwendigkeit einer Zusammenarbeit, um das Vertrauen der Verbraucher in die digitale Welt zu stärken. Atos ist davon überzeugt, dass innovative und kollaborative End-to-End-Cybersicherheit ein starkes Asset und Wettbewerbsvorteil für ein Unternehmen ist.
In ihrem Grundsatz 2 (Verantwortung in der gesamten digitalen Lieferkette) hat die Charter of Trust 17 Sicherheitsanforderungen festgelegt, die entlang der Lieferkette kaskadiert werden müssen und die im Folgenden dargestellt werden.
Es ist die Erwartung von Atos, dass die gesamte Lieferkette diese Anforderungen erfüllt. Die Einhaltung dieser Anforderungen wird risikobasiert überwacht.

2.2. Grundlegende Sicherheitsanforderungen der Charter of Trust für die Lieferkette (Prinzip 2)

Für alle Produkte und Dienstleistungen, die an Atos oder einen Kunden von Atos geliefert werden, ist die Einhaltung der folgenden Grundsätze immer dann verbindlich, wenn sie relevant sind (z.B. wenn personenbezogene Daten verarbeitet werden, gilt die erste Anforderung, wenn ein Vorfall entdeckt wird, gilt die siebte Anforderung usw.).
Die Lieferanten sind in der Lage, auf Anfrage von Atos Beweise für den Nachweis der Maßnahmen zur Erreichung der Einhaltung der 17 grundlegenden Sicherheitsanforderungen vorzulegen.

DATA PROTECTION **1**

Products and services shall be designed to provide confidentiality, authenticity, integrity and availability of data

These key principles are not only the foundation of Principle 2 of the Charter of Trust, but are the bedrock of any secure product or service, and should be considered and appropriately implemented early in their design.
a. **Confidentiality**- appropriately protecting data, objects, and resources from unauthorized access, use, or disclosure during processing, storage, and transit
b. **Authenticity**- assurance that data and products come from the source they claim to be from
c. **Integrity**- assurance that unauthorized modification to data or products is prevented
d. **Availability**- assurance that data and products are accessible to authorized parties

DATA PROTECTION **2**

Data shall be protected from unauthorized access throughout the data lifecycle

Data must be protected during all phases of the delivery of a product or service, from creation to destruction, or end of life.

DATA PROTECTION **3**

The design of products and services shall incorporate security as well as privacy where applicable

The confidentiality and sensitivity of data processed by a product or service must be considered during their design, to ensure appropriate protections are included to prevent unauthorized access, use, or disclosure, and to ensure compliance with any applicable regulatory requirements.

SECURITY POLICIES **4**

Security policies consistent with industry best practices shall be in effect

Mature policies and procedures are critical to provide clear direction to employees on how to operate in a repeatable way, within the confines of an organization's risk tolerance. To that end, organizations should adopt industry best practices that align with standards **such as ISO 27001, ISO 20243, SOC2, IEC 62443**, or similar trusted standards, to ensure appropriate controls are in place to provide confidentiality, authenticity, integrity, and availability.

SECURITY POLICIES **5**

Guidelines on secure configuration, operation and usage of products or services shall be available to customers

Clear and concise directions on how to properly configure, deploy, and operate a product or service are necessary for customers or consumers to fully understand how to secure them.

SECURITY POLICIES **6**

Policies and procedures shall be implemented so as not to consent to include back doors, malware, and malicious code in products and services

Organizations must have Secure Software Development Life Cycle (SSDLC) policies and procedures in place, that can provide reasonable assurances that backdoors, malware, or other malicious code are not included with the product or service, including at the request of a state sponsored actor, criminal organization, or otherwise.

INCIDENT RESPONSE **7**

For confirmed incidents, timely security incident response for products and services shall be provided to customers

Mature incident response policies and procedures are necessary to provide timely response to customers as required by contract, service level agreement, or regulatory requirements.

SITE SECURITY **8**

Measures to prevent unauthorized physical access throughout sites shall be in place

Mature policies, procedures, and controls are required to prevent unauthorized access to controlled areas such as offices, manufacturing facilities, distribution centers, hosting facilities, labs, etc.

ACCESS, INTERVENTION, TRANSFER & SEPARATION **9**

Encryption and key management mechanisms shall be available, when appropriate, to protect data

Based on the confidentiality and sensitivity of data stored or processed by a product or service, encryption and key management should be made available for configuration. For example, where data is classified as public, encryption and key management may not be required. However, where data may be classified as confidential, secret, etc., encryption and key management are critical to protect the confidentiality, authenticity, and integrity of the data at rest, in use, and in transit.

ACCESS, INTERVENTION, TRANSFER & SEPARATION **10**

Appropriate level of identity and access control and monitoring, including third parties, shall be in place and enforced

Role based access controls that follow the principles of least privilege, and segregation of duties, are important to prevent unauthorized access to software, systems, infrastructure, and facilities. Additionally, logging and monitoring the activities of privileged users and third parties with access to sensitive data, systems, areas, or facilities is necessary.

INTEGRITY & AVAILABILITY **11**

Regular security scanning, testing and remediation of products, services, and underlying infrastructure shall be performed

Testing such as code scanning and penetration testing must be performed regularly to ensure that any bugs that may compromise a product, service, or underlying infrastructure are mitigated. If a vulnerability is found, remediation should occur in a timely manner, as appropriate to the risk it presents.

INTEGRITY & AVAILABILITY **12**

Asset Management, Vulnerability Management, and Change Management policies shall be implemented that are capable of mitigating risks to service environments

Policies and procedures in three key areas are necessary to enable and ensure the integrity and availability of products, services, and infrastructure:
a. **Asset Management**- creating inventories and tracking hardware, software, and other assets, both physical and virtual, through the asset's lifecycle, is one of the first steps of any security program.
b. **Vulnerability Management**- the process of regularly identifying vulnerabilities in software, services, and underlying infrastructure, evaluating their risk, installing patches in in timeframes in accordance with that risk, and follow-up scanning to ensure patches are successfully installed
c. **Change Management**- the process of ensuring all changes are documented, evaluated for risk and security impact, tested and authorized prior to deployment, and tracked through delivery.

INTEGRITY & AVAILABILITY **13**

Business continuity and disaster recovery procedures shall be in place and shall incorporate security during disruption, where applicable

Processes shall be in place to ensure essential products and services can be delivered during, and after, a significant disruption to business operations such as a natural disaster, supply-chain failure, cyber-attack, pandemic, etc., and where applicable, security continuity shall be maintained.

INTEGRITY & AVAILABILITY **14**

A process shall be in place to ensure that products and services are authentic and identifiable

Processes that allow a customer or consumer of a product or service to know that they are receiving exactly what they purchased, not a clone or copy. For example, code signing is a process of digitally signing executables and scripts to guarantee the software has been provided by the author, and not altered or corrupted.

SUPPORT **15**

The timeframe of support, specifying the intended supported lifetime of the products, services or solutions shall be defined and made available

Customers or consumers of a product or service must be able to clearly understand the level of support that will be provided, and the intended life cycle of that product or service.

SUPPORT **16**

Based on risk, and during the timeframe of support, processes shall be in place for: (1) Contacting Support, (2) Security Advisories, (3) Vulnerability Management, and (4) Cybersecurity related Patch Delivery and Support

Based on the confidentiality and sensitivity of data stored or processed by a product or service, processes shall be maintained during the supported lifetime:
a. **Contacting Support**- there must be a way for a customer or consumer of the product or service to contact support
b. **Security Advisories**- a method for clearly communicating security advisories to your customers or consumers
c. **Vulnerability Management**- identifying any vulnerabilities in your products or services, evaluating their risk, and developing patches to remediate them in accordance with the risk they present
d. **Cybersecurity related Patch Delivery and Support**- a method of delivering patches to your customers or consumers within a reasonable timeframe in accordance to the risk the vulnerability presents, and providing support related to the installation of these patches.

TRAINING **17**

A minimum level of security education and training for employees shall be regularly deployed (e.g., by training, certifications, awareness)

Employees should regularly receive security training appropriate to their job role, to ensure they are aware of formal processes and procedures as they evolve, best practices, changing threat landscapes, and updates to technology.

For more information...

For more information about Charter of Trust Requirements, visit www.charter-of-trust.com

CoT Kategorie	CoT Prinzipien	
Datenschutz-bestimmungen	**1**	Produkte oder Dienstleistungen müssen so konzipiert sein, dass sie Vertraulichkeit, Authentizität, Integrität und Verfügbarkeit von Daten gewährleisten.
	2	Die Daten müssen während des gesamten Datenlebenszyklus vor unbefugtem Zugriff geschützt sein.
	3	Bei der Gestaltung von Produkten und Dienstleistungen sind wo zutreffend Sicherheit und Datenschutz zu berücksichtigen.
Sicherheitsrichtlinien	**4**	Sicherheitsrichtlinien in Übereinstimmung mit branchenüblichen bewährten Verfahren und Standards wie ISO 27001, ISO 20243, SOC2, IEC 62443 sind umzusetzen (einschließlich Zugangskontrolle, Sicherheitsausbildung, Überprüfung von Mitarbeitern, Verschlüsselung, Netzwerkisolierung/-segmentierung, Betriebssicherheit, physische Sicherheit, Lieferantenmanagement).
	5	Den Kunden müssen Richtlinien für die sichere Konfiguration, den Betrieb und die Nutzung von Produkten oder Dienstleistungen zur Verfügung stehen.
	6	Richtlinien und Verfahren werden so umgesetzt, dass keine Hintertüren (Back Doors), Schadsoftware und bösartigen Code in Produkte und Dienstleistungen ermöglicht werden.
Störfallreaktion	**7**	Bei bestätigten Vorfällen ist dem Kunden eine rechtzeitige Reaktion auf Sicherheitsvorfälle für Produkte und Dienstleistungen zu gewähren.
Standortsicherheit	**8**	Es müssen Maßnahmen zur Verhinderung eines unbefugten physischen Zutritts an allen Standorten getroffen werden.
Zugang, Intervention, Transfer & Trennung	**9**	Wenn notwendig oder sinnvoll müssen zum Schutz der Daten Verschlüsselungs- und Schlüsselverwaltungsmechanismen zur Verfügung stehen.
	10	Es muss ein angemessenes Maß an Identität-, Zugangskontrolle und -überwachung, einschließlich Dritter, vorhanden sein und sichergestellt werden.
Integrität und Verfügbarkeit	**11**	Regelmäßige Sicherheitsüberprüfungen, Tests und Behebung von Sicherheitsrisiken in Produkten, Dienstleistungen und der Infrastruktur sind durchzuführen.
	12	Es werden Richtlinien für Asset Management, Schwachstellenmanagement und Change-Management implementiert, die geeignet sind, Risiken für Service-Umgebungen zu minimieren.
	13	Wenn notwendig, müssen Verfahren für die Aufrechterhaltung des Systembetriebs und Systemwiederherstellung im Notfall vorhanden sein, welche die Sicherheit auch bei Störungen gewährleisten.
	14	Es muss ein Verfahren im Einsatz sein, um sicherzustellen, dass Produkte und Dienstleistungen authentisch und identifizierbar sind.
Unterstützungsleistung	**15**	Unterstützungsleistungen für die beabsichtigte Lebensdauer der Produkte, Dienstleistungen oder Lösungen wird definiert und zur Verfügung gestellt.
	16	Basierend auf dem Risiko und während des Zeitraums der Unterstützungsleistung müssen Prozesse für: (1) Kontaktaufnahme mit dem Support, (2) Sicherheitsmeldungen, (3) Schwachstellenmanagement und (4) Auslieferung Cybersicherheitsbezogener Patches und Support implementiert sein.
Training	**17**	Ein Mindestmaß an Sicherheitsausbildung und -schulung für Mitarbeiter ist regelmäßig anzuwenden (z.B. durch Schulungen, Zertifizierungen, Sensibilisierung).

2.3. Umgang mit Informationen

1. Unabhängig von der Art der Informationen und dem verwendeten Medium MÜSSEN alle Informationen (die Atos oder den Kunden von Atos gehören) von Partnern und Lieferanten gemäß ihrer Klassifizierungsstufe und den GDPR-Anforderungen geschützt werden.
2. Alle Informationen, die personenbezogene Daten enthalten, MÜSSEN in Übereinstimmung mit den GDPR-Kontrollen der EU geschützt werden.
3. Im Falle der Verarbeitung personenbezogener Daten stellen Partner und Lieferanten sicher, dass sie die geltenden Datenschutzgesetze einhalten. Partner und Lieferanten verpflichten sich, (i) angemessene technische und organisatorische Maßnahmen zu ergreifen, um den Schutz der personenbezogenen Daten zu gewährleisten und eine unbefugte oder rechtswidrige Verarbeitung der personenbezogenen Daten von Atos oder seinen Kunden, sowie einen unbeabsichtigten Verlust oder eine unbeabsichtigte Zerstörung oder Beschädigung der personenbezogenen Daten von Atos oder seinen Kunden zu verhindern, und (ii) keine personenbezogenen Daten von Atos und seinen Kunden und/oder die Durchführung der Verarbeitung personenbezogener Daten von Atos und seinen Kunden ohne vorherige formelle Zustimmung von Atos an Dritte zu übermitteln, auch wenn diese Übertragung zur Erfüllung der in dieser Vereinbarung beschriebenen Dienstleistung erfolgt.
   Sobald Partner und Lieferanten personenbezogene Daten in Übereinstimmung mit der EU GDPR verarbeiten und es noch keine entsprechende Datenschutz- und Verarbeitungsvereinbarung gibt, ist der Partner oder Lieferant verpflichtet, unverzüglich ihren Atos-Kontakt zu benachrichtigen und MÜSSEN eine entsprechende Vereinbarung mit Atos abschließen.
4. Für Atos-Informationen, die nicht öffentlich zugänglich sind, gibt es drei Schutzklassen

- "Für den internen Gebrauch" oder „Atos für internen Gebrauch (mit autorisierter Weitergabe an Dritte)“,
- " Vertraulich",
- " Geheim",

   die in Anhang 1 "Klassifizierung der ATOS-Informationen" beschrieben sind.

5. In Absprache und gemeinsam mit dem Atos-Kontakt und wenn nicht ausdrücklich festgelegt, MÜSSEN Partner und Lieferanten die Vertraulichkeitsstufe für die ihnen anvertrauten oder von ihnen erstellten Informationen festlegen.
6. Partner und Lieferanten MÜSSEN die Atos-/Kunden Informationen schützen. Informationen, die nicht öffentlich zugänglich sind, dürfen nicht an Unbefugte weitergegeben, weitergegeben oder übermittelt werden.
7. Für Informationen, die Eigentum von Atos Dritten (d.h. Kunden, andere Partner oder Lieferanten von Atos) sind, müssen die Informationen nach den mit dem Dritten definierten und vereinbarten Regeln geschützt werden.
8. Partner und Lieferanten MÜSSEN die ihnen im Rahmen ihrer Aktivitäten oder vertraglichen Vereinbarungen mit Atos bekannt gewordenen relevanten Maßnahmen berücksichtigen.
9. Der Export oder sonstige Umschlag von Atos-/Drittpartei-Informationen kann der Notwendigkeit einer Ausfuhrgenehmigung gemäß den US-amerikanischen, EU- oder nationalen Ausfuhrbestimmungen im Zusammenhang mit militärischen oder Dual-Use-Bedingungen unterliegen. Falls erforderlich, klären Sie dies mit dem zuständigen Atos-Büro und holen Sie rechtzeitig die entsprechende Lizenz ein. Beachten Sie, dass die Exportbestimmungen auch dann gelten, wenn die Informationen elektronisch oder über Kommunikationsnetze (z.B. per E-Mail oder Dateiübertragung) ins Ausland übertragen oder vom Ausland auf einem Server verfügbar sind.
10. Auf Anfrage des zuständigen Atos-Ansprechpartners müssen die Mitarbeiter von Partnern und Lieferanten an der obligatorischen jährlichen Atos-Sicherheitsübung (ca. eine Stunde) teilnehmen. Dies gilt insbesondere für Mitarbeiter, die sich regelmäßig in Atos- oder Atos Kundenräumen aufhalten oder dort arbeiten.
11. Der Zugang zu Informationen kann in einigen Verträgen erfordern, dass die Mitarbeiter von Partnern und Lieferanten eine Geheimhaltungsvereinbarung (NDA) unterzeichnen. Auf Anfrage

des zuständigen Atos-Ansprechpartners MÜSSEN die von dieser Anforderung betroffenen Mitarbeiter von Partnern und Lieferanten das jeweils von Atos vorgegebene NDA unterzeichnen. Jede Weigerung, zu unterschreiben, kann den Partner oder den Mitarbeiter des Lieferanten von der Arbeit an dem Vertrag ausschließen.

2.4. Systemzugriffs- und Zugangsberechtigungen

Sollten Partnern und Lieferanten Systemzugriffs- und Autorisierungscodes zur Verfügung gestellt werden, um den Zugriff auf Atos-interne Informationen, Atos-Kundeninformationen und alle zugehörigen Systeme zu erleichtern, geschieht dies unter der Bedingung, dass eine solche Nutzung unter Verwendung der von Atos bereitgestellten Geräte erfolgt, es sei denn, eine Verbindung von einem kundeneigenen Gerät oder System wurde von Atos Group Security genehmigt und ist auf den vereinbarten Rahmen von Aufgaben oder Aktivitäten beschränkt. Wo technisch umsetzbar, MUSS die Zwei-Faktor-Authentifizierung die Mindestanforderung an die Authentifizierung sein. Benutzer-IDs (und die dazugehörige Authentifizierung) dürfen nicht von oder zwischen Partnern und Mitarbeitern von Lieferanten geteilt werden.

2.5. Beendigung der Tätigkeit

Partner und Lieferanten MÜSSEN das Folgende nach Abschluss der vereinbarten Aktivitäten an das zuständige Atos-Büro zurücksenden (sofern nicht anders vereinbart):

- Die Dokumente und Ressourcen, die an Partner und Lieferanten weitergegeben werden;
- Alle von Partnern und Lieferanten erstellten oder verwendeten Informations- und Datenträger, einschließlich Kopien und Entwürfe;
- Partner und Lieferanten MÜSSEN sicherstellen, dass die Systemzugangsberechtigungen, die ihren Mitarbeitern zur Durchführung der vereinbarten Tätigkeiten erteilt werden, widerrufen werden, sobald sie nicht mehr benötigt werden.

Partner und Lieferanten (incl. Sublieferanten) MÜSSEN unter Berücksichtigung der gesetzlichen Aufbewahrungspflichten alle auf ihrer eigenen Infrastruktur (einschließlich des Backup-Speichers) gespeicherten Informationen oder Daten löschen und MÜSSEN eine Erklärung abgeben, in der eine solche Löschung nachgewiesen wird.

2.6. Mängel und IT-Sicherheitsvorfälle

1. Alle Mängel, anormales Verhalten eines Systems und Vorfälle mit Auswirkungen auf die Informationssicherheit (z.B. Datenverlust oder Offenlegung) MÜSSEN von Partnern und Lieferanten unverzüglich an die zuständigen Ansprechpartner bei Atos gemeldet werden.

2. Jeder Verlust von Informationsgeräten, die Atos-Informationen enthalten (oder Kundeninformationen im Zusammenhang mit dem Vertrag), MUSS von Partnern und Lieferanten unverzüglich an den Atos-Kontakt gemeldet werden.

3. Zusätzliche Regeln für Partner und Lieferanten mit Arbeitsplatz bei Atos

1. Partner und Lieferanten MÜSSEN die ihnen im Rahmen ihrer Tätigkeiten oder vertraglichen Vereinbarungen bekannt gewordenen relevanten Informationssicherheitsmaßnahmen berücksichtigen.
2. Es MUSS eine Clean Desktop Policy gelten: Dokumente, die als vertraulich oder geheim eingestuft sind, MÜSSEN auch beim kurzfristigen Verlassen des Schreibtisches immer geschützt und in eine verschlossene Schublade oder einen Schrank gelegt werden. Alle Dokumente, unabhängig von der Klassifizierung, MÜSSEN am Ende eines jeden Tages sicher aufbewahrt werden.

3. Das Verlassen des Firmengeländes von an Partner und Lieferanten übergebenen Dokumenten, Arbeitsergebnissen, Datenträgern oder IT-Systemen ist nur mit entsprechender Genehmigung und/oder Anweisung von Atos zulässig.
4. Die Nutzung der Informationssysteme (z.B. PCs, Workstations) durch Partner und Lieferanten erfolgt nur für die zugewiesenen Aufgaben. Insbesondere ist die Nutzung der von Atos zugänglich gemachten IT-Umgebungen für private Zwecke untersagt.
5. Partner und Lieferanten MÜSSEN sicherstellen, dass Systeme und der Zugriff auf Systeme gemäß den in diesem Dokument kommunizierten Sicherheitsregeln oder durch eine andere ausdrückliche Anweisung von Atos geschützt sind.
6. Partner und Lieferanten MÜSSEN die Schutzmechanismen mit der gebotenen Sorgfalt behandeln. Ressourcen wie Passwörter und Smartcards (PKI-Karten) dürfen nicht an Dritte weitergegeben oder veröffentlicht werden. Sie sind streng persönlich (außer bei der Verwendung von gemeinsamen generischen IDs, wo sie dem internen Genehmigungsprozess von Atos folgen müssen).
7. Die Definition und Änderung von Passwörtern und PIN-Codes MUSS Regeln unterworfen werden, die nicht umgangen werden können. Partner und Lieferanten MÜSSEN sicherstellen, dass Passwörter und PIN-Codes den Best Practices entsprechen (die jedes Mal durchgesetzt werden, wenn dies auf Atos-Systemen möglich ist).
8. Wenn die Mitarbeiter von Partnern und Lieferanten einen Arbeitsplatz allein verlassen, MÜSSEN sie, wenn auch nur kurzzeitig, alle offenen Zugangspunkte sichern, z.B. durch den Einsatz eines Bildschirmschoners oder das Entfernen der Smartcard aus dem Kartenleser.
9. Wo die Nutzung des Internets möglich ist, MÜSSEN die lokalen Vorschriften und die bei Atos geltenden Richtlinien eingehalten werden.
10. Sicherheitseinstellungen, Systemfunktionen oder Vorsichtsmaßnahmen gegen Computerviren oder andere auf den Systemen installierte bösartige Software dürfen nicht deaktiviert, modifiziert oder umgangen werden.
11. Bei Verdacht auf eine Infektion durch Computerviren, die nicht automatisch erkannt oder beseitigt werden, oder bei Problemen mit der Ausführung von Virenschutzprogrammen MÜSSEN die lokalen Atos-Kontakte unverzüglich informiert werden.
12. Partner und Lieferanten verwenden Atos E-Mail nur für geschäftliche Zwecke.
13. Die Verwendung von E-Mail-Verschlüsselung ist nur mit den Tools von Atos möglich, wenn eine entsprechende schriftliche Vereinbarung vorliegt und die entsprechenden Vorschriften eingehalten werden.
14. Die automatische Weiterleitung eingehender E-Mails an externe Postfächer, z.B. private E-Mail-Adresse, externe E-Mail-Anbieter, ist NICHT zulässig.
15. Für die Datenarchivierung und -sicherung MÜSSEN Partner und Lieferanten Atos-Dateiserver und Atos-Backup-Infrastrukturen innerhalb des Atos-Netzwerks verwenden.
16. USB-Sticks (oder jede andere Form von Wechselmedien) dürfen nicht ohne die ausdrückliche Genehmigung von Atos und dann nur in voller Übereinstimmung mit der Atos-Richtlinie für Wechselmedien verwendet werden.

4. Zusätzliche Regeln für Partner und Lieferanten, die an ihren eigenen Systemen arbeiten.

1. Partner und Lieferanten MÜSSEN ihre Systeme vor dem Verlust der Vertraulichkeit, Integrität und Verfügbarkeit aller Daten oder Informationen schützen, die für Atos erstellt, verarbeitet oder gespeichert wurden oder die für Atos wichtig sind.
2. Für den Zweck des an Atos (oder an die Kunden von Atos) gelieferten Dienstes ist es strengstens verboten, eigene Geräte mitzubringen.

3. Partner und Lieferanten führen ihre eigenen geeigneten Maßnahmen auf der Grundlage von Sicherheitsrisikobewertungen durch, wobei sie mindestens Folgendes berücksichtigen:
   - Datensicherung (nur auf gesicherten Medien);
   - Virenschutz;
   - Persönliche Firewall-Nutzung;
   - Vollständige Festplattenverschlüsselung;
   - System- und Datenzugriffsschutz.
4. Die Datenübergabe an Atos erfolgt ausschließlich nach den vereinbarten Verfahren und nach einer vollständigen Virenprüfung mit aktualisierten Signaturen.
5. Nach Abschluss der vereinbarten Tätigkeiten werden die Partner und Lieferanten alle im Rahmen der Zusammenarbeit anfallenden Daten, Dokumente und Datenträger sowie die dazugehörigen Kopien oder Datensicherungen sicher entsorgen. Auf Verlangen von Atos löschen Partner und Lieferanten alle Informationen oder Daten, die auf ihrer eigenen Infrastruktur (einschließlich des Backup-Speichers) gespeichert sind, und MÜSSEN eine Erklärung abgeben, in der diese Löschung nachgewiesen wird.
6. Wenn Partner und Lieferanten keine eigenen geeigneten Möglichkeiten haben, um die sichere Entsorgung von Informationen, Dokumenten und Datenträgern zu gewährleisten, MÜSSEN sie ihren Atos-Ansprechpartner bitten, ihnen beim Zugang zu den relevanten internen Einrichtungen von Atos zu helfen. Datenvernichtungszertifikate MÜSSEN vorgelegt werden.
7. Partner und Lieferanten dürfen sich ohne Genehmigung der Atos Group Security nicht direkt mit dem internen Netzwerk von Atos (Atos Intranet) von einem nicht-Atos-eigenen Gerät aus verbinden.
8. Der Zugang zum Internet wird für Geräte, die nicht im Besitz von Atos sind, über das Atos-Gastnetzwerk bereitgestellt, sofern verfügbar.
9. Verbindungen zu externen Netzwerken sind an Atos-Standorten verboten. Die Freigabe MUSS an allen Standorten beim Atos Verantwortlichen eingeholt werden, bevor eine Verbindung hergestellt wird.
10. USB-Sticks (oder jede andere Form von Wechselmedien) dürfen nicht ohne die ausdrückliche Genehmigung von Atos und dann nur in voller Übereinstimmung mit der Atos-Richtlinie für Wechselmedien verwendet werden.

5. Zusätzliche Regeln für Partner und Lieferanten mit Anbindung an Ressourcen im Atos-Intranet

1. Partner und Lieferanten dürfen Informationen nur auf der Grundlage der von Atos erteilten Anweisungen und der von Atos erteilten Genehmigungen verarbeiten.
2. Partner und Lieferanten MÜSSEN sich nur über die technische Konfiguration und die mit Atos vereinbarte Netzwerkarchitektur und auf den für den vereinbarten Zweck bereitgestellten Systemen mit einem Atos-Netzwerk, -Gerät oder -Dienst verbinden.
3. Partner und Lieferanten dürfen ohne ausdrückliche und schriftliche Zustimmung der Atos IT-Abteilung kein Remote-VPN (z.B. IPSEC oder SSL) aufbauen, um ihre Atos Workstations mit einem Nicht--Atos-Netzwerk zu verbinden.
4. Alle Informationen über Netzwerke und Zugangsmöglichkeiten (z.B. Einwahlnummern, Netzwerkadressen) und Sicherheitsvorkehrungen in Bezug auf Atos interne Systeme und Netzwerke MÜSSEN von Partnern und Lieferanten als "Atos Vertraulich" behandelt werden.

ANHANG 1 "ATOS INFORMATION CLASSIFICATION".

Dieser Anhang beschreibt die Klassifizierung, die Atos Information beigefügt ist, und wie sie während ihrer gesamten Lebensdauer von der Erstellung bis zur Entsorgung behandelt werden muss.

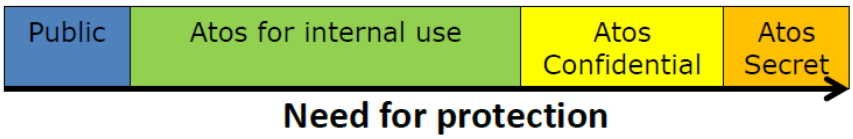
Klassifizierungen von Kunden müssen gemäß dem Klassifizierungsstandard des Kunden behandelt werden.

1. ATOS Schema zur Klassifikation von Informationen

Alle Informationen müssen vom Eigentümer oder Autor als solche eingestuft werden:

1. Öffentlich;
2. Atos für den internen Gebrauch oder Atos für internen Gebrauch (mit autorisierter Weitergabe an Dritte);
3. Atos Vertraulich;
4. Atos Geheim.

Standardmäßig wird davon ausgegangen, dass alle Informationen, deren Klassifizierung nicht explizit definiert ist, zur Klassifizierung "Atos for internal use" gehören.



1.1. Öffentlich

Informationen sind als öffentlich definiert, wenn die Informationen über autorisierte Unternehmenskanäle in der Konzern- oder Abteilung für lokale Kommunikation zur öffentlichen Verbreitung bereitgestellt wurden.

Öffentliche Informationen sind weder im Kontext noch im Inhalt sensibel und bedürfen keinem besonderen Schutz.

Beispiele:

- Der Jahresbericht von Atos (nach der Veröffentlichung);
- Atos Verhaltenskodex für Ethik
- Atos Binding Corporate Rules (BCR);
- Informationen, die für den öffentlichen Verbrauch erzeugt werden, wie z.B. Bulletins für den öffentlichen Dienst, Marketing, etc.
  Broschüren und Anzeigen.

1.2. Atos für den internen Gebrauch

Die Sicherung dieser Informationen ist notwendig, um die Interessen von Atos zu schützen.

Interne Nutzungsinformationen sind so definiert, dass eine Offenlegung außerhalb des Unternehmens dem Interesse von Atos zuwiderläuft und daher auf die Verwendung innerhalb von Atos beschränkt werden muss. Unter besonderen Umständen, die durch spezifische Geschäftsanforderungen gerechtfertigt sind, kann es erforderlich sein, Dokumente aus dieser

Klassifizierung mit externen Dritten wie Auditoren, Kunden, Lieferanten oder potenziellen Kunden zu teilen.

Beispiele:

- operative Geschäftsinformationen / Berichte;
- Unternehmensrichtlinien, -verfahren, -richtlinien und -standards;
- interne Firmenmitteilungen;
- detaillierte und technische Dokumentation der Dienstleistungen.

1.3. Atos Vertraulich

Die Sicherheit dieser Informationen steht im Vordergrund.

Die Sicherheit dieser Informationen steht im Vordergrund.

Vertrauliche Informationen sind definiert als Informationen, die so beschaffen sind, dass die versehentliche oder unrechtmäßige Zerstörung, der Verlust, die Veränderung, die unberechtigte Offenlegung oder der unberechtigte Zugriff darauf Atos Schaden zufügen kann durch

- Verletzung der Privatsphäre der Atos-Mitarbeiter,
- Einflussnahme auf den Aktienkurs von Atos,
- negative Auswirkungen auf die Bereitstellung der Dienstleistungen durch Atos.

Beispiele:

- personenbezogene Daten
- Businesspläne, Marketingpläne
- Finanzinformationen
- Informationen von Dritten, die einer Geheimhaltungsvereinbarung unterliegen
- interne Auditberichte / Ergebnisse von Penetrationstests

Beispiele:

- personenbezogene Daten;
- Businesspläne, Marketingpläne;
- Finanzinformationen;
- Informationen von Dritten, die einer Geheimhaltungsvereinbarung unterliegen;
- Interne Auditberichte / Ergebnisse von Intrusionstests.

1.4. Atos Geheim

Die Sicherheit dieser Informationen ist für Atos von entscheidender Bedeutung.

Geheime Informationen sind definiert als Informationen, die so schädlich sind, dass eine unbefugte Weitergabe extreme finanzielle Schäden für Atos verursachen oder den Preis von
den Marktanteil und kann zur Inhaftierung des Managements oder der Mitarbeiter von Atos führen.

Beispiele:

- Finanzergebnisse vor dem Veröffentlichungsdatum;
- Atos Unternehmensstrategie (z.B. Fusionen und Übernahmen);
- Insiderinformationen.

2. Verteilung von klassifizierten Informationen

Für die Verteilung von klassifizierten Informationen MÜSSEN die folgenden Regeln gelten:

2.1. Atos Public

Kann ohne Einschränkung geteilt werden.

2.2. Atos für den internen Gebrauch

Kann geteilt werden:

- ohne jegliche Einschränkung nur innerhalb von Atos;
- mit Dritten unter den folgenden Richtlinien.
  Wenn die Informationen an einen Dritten weitergegeben werden sollen, so ist folgendes zu beachten: Wenn
  - mit Atos eine vertragliche Vereinbarung getroffen wurde, die eine "Atos For Internal Use"-Behandlungsanleitung enthält, müssen die Vertragspartner an ihre vertraglichen Verpflichtungen erinnert werden;
  - keine vertragliche Vereinbarung mit Atos besteht, können sie nicht weitergegeben werden, solange sie nicht mit Handlungsanweisungen versehen wurden und eine Geheimhaltungsvereinbarung von dem Dritten unterzeichnet wurde.
  - keine vertragliche Vereinbarung mit Atos besteht, aber durch schriftliche Nachweise eine Erlaubnis gegeben wurde, dass er Informationen als "vertraulich" behandelt und keinen Zugang zu diesen Informationen oder deren Weitergabe an Dritte erlaubt.

2.3. Atos Vertraulich

Kann geteilt werden:

- Nur an die vom Informationseigentümer angegebenen Empfänger (Atos-Gruppe von Empfängern);
- Mit Ausnahme von Projekten, in denen die Teammitglieder aufgeführt sind, kann der Empfänger vertraulicher Informationen von einer Gruppe oder einer lokalen Verteilerliste benannt oder spezifiziert werden; die Verteilerliste kann allgemeiner Natur sein, als "Personalabteilung" oder "Kunde {X}". (für Informationen, die zwischen Atos-Teams und einem Kunden ausgetauscht werden) oder eine soziale geschlossene Community über interne Tools (z.B. SharePoint);
- Die angegebenen Empfänger dürfen einigen vertrauenswürdigen Atos-Mitarbeitern eine Kopie vertraulicher Informationen übermitteln, ohne dem Informationseigentümer zu melden:
  - Dies ist aus betrieblichen oder geschäftlichen Gründen gerechtfertigt;
  - Jeder Empfänger erklärt sich damit einverstanden, dass er die Informationen nicht an eine andere Person weitergeben darf.
  - Dies steht im Einklang mit allen anderen Verfahren, die zur Anwendung kommen können.

2.4. Atos Geheim

Eine Übermittlung ist nur an die vom Informationseigentümer angegebenen Empfänger möglich. Die Empfänger MÜSSEN entweder benannt werden, einer lokalen Verteilerliste oder der Kalkulationstabelle der Projektmitglieder angehören.