Allgemeine Anforderungen zur Informationssicherheit an Lieferanten der astora GmbH

ISMS-REQ-15, Ausgabe Februar 2021

1. Informationssicherheit

1.1. Der Lieferant / Auftragnehmer schützt Informationen von astora durch Umsetzung der in diesem Dokument festgelegten Maßnahmen. Die Implementierung und Einhaltung dieser Maßnahmen sind vom Lieferanten / Auftragnehmer regelmäßig zu überprüfen.[1]

1.2. Mitarbeiter des Lieferanten / Auftragnehmers, die Zugang zu Unternehmensnetzen, -systemen oder -daten erhalten sollen, müssen die Kenntnis und Einhaltung der Anforderungen aus diesem Dokument durch eine schriftliche Erklärung bestätigen.

1.3. Der Lieferant hat sicherzustellen, dass auch von ihm eingesetzte Unterauftragnehmer sämtliche sich aus diesem Dokument ergebenden Anforderungen der astora zur Informationssicherheit im Rahmen ihrer Tätigkeiten mit Bezug zur astora beachten.

2. Organisation der Informationssicherheit

2.1. Der Lieferant / Auftragnehmer benennt eine kompetente Kontaktperson als Ansprechpartner zum Thema Informationssicherheit.

2.2. Der Lieferant / Auftragnehmer gestaltet Prozesse und erledigt Aufgaben für astora unter Beachtung der Prinzipien der Funktionstrennung, Kenntniserfordernis (Need-to-Know) und minimaler Rechtevergabe (Least-Privilege), wo es angemessen und erforderlich ist.

3. Informationssicherheit beim Personaleinsatz

Der Lieferant / Auftragnehmer stellt sicher, dass

3.1. Von ihm eingesetztes Personal, das Zugriff auf astora-Informationen hat, sich zum Schutz dieser Informationen durch die Unterzeichnung einer Vertraulichkeitserklärung verpflichtet. Die Vertraulichkeitserklärung ist astora vorzulegen und muss über das Projekt und die Anstellung hinaus gültig sein.[2]

3.2. das von ihm eingesetztes Personal, das Zugriff auf Informationen und Systeme von astora nicht mehr benötigt, keine lieferantenseitig gewährten Zugangsmöglichkeiten zu diesen Informationen und Systemen mehr hat.

3.3. das vom ihm eingesetzte Personal, welches den Lieferanten / Auftragnehmer verlässt oder keinen Bezug mehr zu astora hat, die ihm anvertrauten EDV-Geräte und Informationen ordnungsgemäß zurückgibt.

3.4. das Personal für die jeweiligen Aufgaben qualifiziert und geschult ist (einschließlich Informationssicherheit).

4. Verwaltung der Werte

In Bezug auf die Verwaltung von Vermögenswerten (Assets) stellt der Lieferant / Auftragnehmer sicher, dass

4.1. Informationsvermögenswerte von astora nicht ohne vorherige Genehmigung vom Firmengelände der astora entfernt werden.[3]

4.2. astora-Informationen logisch von fremden Informationen getrennt verarbeitet und gespeichert werden.

4.3. Nach Abschluss oder Beendigung der Arbeiten des Lieferanten / Auftragnehmers für astora alle Kopien der astora-Informationen, einschließlich aller Sicherungs- und Archivierungskopien, in elektronischer oder nicht elektronischer Form bereinigt und sicher vernichtet (oder auf Anfrage an astora zurücksendet; Ausnahmen sind bei gesetzlichen Anforderungen möglich) werden. Über die sichere Vernichtung sind astora auf Anfrage Nachweise mit relevanten Angaben vorzulegen (was, wann, wie, wer, ggf. Zeuge).

5. Zugangssteuerung

Im Rahmen der Zugangssteuerung zu den astora-Informationen stellt der Lieferant / Auftragnehmer in seinem Verantwortungsbereich Folgendes sicher

5.1. Der Zugang zu astora-Informationen folgt stets den Prinzipien von Kenntniserfordernis (Need-to-Know) und minimaler Rechtevergabe (Least-Privilege).

5.2. Es gibt zuverlässige Aufzeichnungen über die Zugriffe auf die Systeme oder Anwendungen von astora. Die Aufzeichnungen stellen die Zurechenbarkeit der Zugriffe sicher.

5.3. Das Anschließen von Geräten an die astora-Infrastruktur erfolgt nur nach einer formalen Genehmigung durch astora.

5.4. An die astora-Infrastruktur angebundene Geräte sind mit einem aktuellen Schadsoftwareschutz ausgestattet und sind in Bezug auf Sicherheits- und Funktionsupdates auf dem neuesten Stand gehalten.

5.5. Vor Einbringen eines externen Datenträgers in die astora Gasspeicher-Infrastruktur (z.B. USB, CD, DVD, externe Festplatte) hat der Lieferant/Auftragnehmer die schriftliche Genehmigung von astora einzuholen und eine vorherige Überprüfung auf Schadsoftware vorzunehmen.

[1] Alternative Schutzmaßnahmen sind nur zulässig, soweit sie vorab von astora genehmigt wurden.

[2] Die Vertraulichkeitserklärung kann allgemeingültig sein

[3] Informationsvermögenswerte sind Daten, Anwendungen, Hardware, Komponenten der Prozessleittechnik, und andere Vermögenswerte, die diese unterstützen.

5.6. Der Fernzugriff auf die astora-Infrastruktur darf ausschließlich über von astora vorab genehmigte Kommunikationskanäle und -technologien (VPN, Standleitung, Zwei-Faktor-Authentifizierung) erfolgen.

5.7. Systeme, auf welchen astora-Informationen verarbeitet, gespeichert oder übertragen werden, verfügen über ein angemessenes Zugriffs- und Identitätsmanagement. Dies beinhaltet mindestes folgende Sicherheitsmaßnahmen:

a) Verwendung eindeutiger Benutzer-IDs;
b) Autorisierung und Verwaltung von Zugriffsrechten;
c) Zeitnahe Löschung von obsoleten Zugriffsrechten;
d) Regelmäßige Überprüfung der Zugriffsrechte hinsichtlich der Geschäfts- und Sicherheitsanforderungen;
e) Revisionssichere Protokollierung der Zugriffsaktivitäten in Bezug auf astora-Informationen;
f) Kennwortanforderungen von astora oder strengere Anforderungen werden angewandt und durchgesetzt.

6. Kryptographie

6.1. Kryptografische Maßnahmen müssen in Übereinstimmung mit allen relevanten Vereinbarungen, Gesetzen und Vorschriften angewendet werden.

7. Physische und umgebungsbezogene Sicherheit

7.1. Besucherausweise sind auf dem Gelände und in den Büroräumen / -bereichen der astora stets an gut sichtbarer Stelle zu tragen.

8. Betriebssicherheit

Im Rahmen von Dienstleistungen zu oder an astora-Informationssystemen, sind von Lieferanten folgende Maßnahmen anzuwenden:

8.1. astora ist über bestehende oder potenzielle Verfügbarkeitseinschränkungen der astora-Informationssysteme, die sich in der Verwaltung des Lieferanten / Auftragnehmers befinden, falls nicht anders geregelt, zu informieren.

8.2. Systeme, die permanent mit der astora-Infrastruktur verbunden sind, müssen folgende Sicherheitsanforderungen erfüllen:

a) Privilegierte Benutzeraktionen werden protokolliert.
b) Die Protokolle werden revisionssicher geführt. Es sind mindestens sicherheitsrelevante Ereignisse aufzuzeichnen.[4]
c) Die Protokolle müssen mindestens 90 Tage lang aufbewahrt und innerhalb dieser Zeit astora auf Anfrage zur Verfügung gestellt werden.
d) Backups müssen so durchgeführt und gepflegt werden, dass sie ihre vereinbarte Zielsetzung erfüllen können.
e) Der Schadsoftwareschutz ist, wo technisch machbar, aktiv und wird auf dem neuesten Stand gehalten.
f) Ein angemessener Schwachstellen- und Patch-Management-Prozess wird angewandt, so dass die Systeme des Lieferanten zeitnah aktualisiert werden.

9. Kommunikationssicherheit

9.1. astora-Informationen in Ruhe oder Übertragung sind durch angemessene Sicherheitsmaßnahmen zu schützen (z.B. Verschlüsselung, Firewalls, Intrusion Detection/ Prevention etc.)

9.2. Drahtlose Netzwerkverbindungen von Lieferanten / Auftragnehmern, die astora-Informationen übertragen, müssen mindestens den WPA2-Sicherheitsstandard aufweisen.

10. Handhabung von Informationssicherheitsvorfällen

10.1. Der Lieferant/Auftragnehmer hat über Prozesse zu verfügen, die im Kontext der Organisation des Lieferanten / Auftragnehmers, eine angemessene Behandlung von Sicherheitsvorfällen ermöglichen.

10.2. Sicherheitsvorfälle oder –Schwachstellen beim Lieferanten/Auftragnehmer, bei welchen Auswirkungen auf astora nicht sicher ausgeschlossen werden können, sind unverzüglich dem Ansprechpartner bei astora oder dem Information Security Officer[5] der astora zu melden.

11. Business Continuity Management

11.1. Der Lieferant / Auftragnehmer unterstützt die astora-Sicherheitsorganisation beim jährlichen ISMS-Risikomanagementprozess auf Anforderung durch astora.

12. Compliance

12.1. Der Lieferant / Auftragnehmer muss auf Anfrage von astora die Einhaltung der in diesem Dokument beschriebenen Sicherheitsanforderungen durch eine angemessene Prüfung durch astora oder ihre Beauftragten oder auf eine andere geeignete Art und Weise nachweisen.

[4] Die sicherheitsrelevanten Ereignisse sind Ereignisse, die Vertraulichkeit, Integrität oder Verfügbarkeit von Informationssystemen beeinträchtigen können.

[5] Tel. 0561 99858 7038 oder it-security@astora.de