Allgemeine Anforderungen zur Informationssicherheit an Lieferanten der astora GmbH

1. Einleitung

1.1. astora GmbH, im Folgenden astora, ist Betreiber einer kritischen Infrastruktur im Sinne der KRITIS-Verordnung §2 Sektor Energie. Das Unternehmen ist verpflichtet die Sicherheitsanforderungen des IT-Sicherheitskatalogs gemäß §11 (1b) EnWG zu erfüllen und dafür zu sorgen, dass auch seine Lieferanten, die mit Unternehmensinformationen und -Systemen interagieren, diese ebenfalls einhalten.

Das vorliegende Dokument beschreibt grundlegende, auf den Normen ISO/IEC 27001 und 27019 basierende Sicherheitsanforderungen an Lieferanten von astora. Unter Lieferanten werden alle Lieferanten von Waren und Dienstleistung verstanden. Unternehmensinformationen sind primär Daten und Dokumente in schriftlicher oder digitaler Form. Unternehmenssysteme sind jegliche Hardware und Software, die sich im Eigentum oder Besitz des Unternehmens befinden oder im Auftrag von astora von Dritten betrieben werden (z.B. Computer, Server, Netzwerke, Speichermedien etc.).

2. Anforderungen an Informationssicherheit

2.1. Lieferanten setzten die in diesem Dokument festgelegten Anforderungen um. Die Implementierung und Einhaltung dieser Anforderungen sind von Lieferanten regelmäßig zu überprüfen. Alternative Schutzmaßnahmen sind nur zulässig, soweit sie vorab von astora genehmigt sind.

2.2. Mitarbeiter der Lieferanten, die Zugang zu Unternehmensinformationen und -systemen erhalten, müssen die Anforderungen aus diesem Dokument kennen.

2.3. Lieferanten haben sicherzustellen, dass auch die Unterauftragnehmer sämtliche sich aus diesem Dokument ergebenden Anforderungen der astora zur Informationssicherheit im Rahmen ihrer Tätigkeiten mit Bezug zur astora beachten.

3. Anforderungen an Organisation der Informationssicherheit

3.1. Lieferanten benennen bei Bedarf eine kompetente Kontaktperson als Ansprechpartner zum Thema Informationssicherheit.

3.2. Lieferanten gestalten Prozesse und erledigen Aufgaben für astora unter Beachtung der Prinzipien der Funktionstrennung, Kenntniserfordernis (Need-to-Know) und minimaler Rechtevergabe (Least-Privilege), wo es angemessen und erforderlich ist.

4. Anforderungen an Informationssicherheit beim Personaleinsatz

Lieferant stellen sicher, dass

4.1. das für astora eingesetztes Personal zumindest allgemeingültig zur Geheimhaltung verpflichtet ist.

4.2. das für astora eingesetztes Personal, das Zugriff auf Informationen und Systeme von astora nicht mehr benötigt, keine lieferantenseitig gewährten Zugangsmöglichkeiten darauf mehr hat.

4.3. das für astora eingesetzte Personal, die EDV-Geräte und Informationen ordnungsgemäß zurückgibt und existierende Kopien löscht, sofern das Arbeitsverhältnis beendet wird oder keine Tätigkeiten für astora mehr ausgeübt werden.

5. Anforderungen an Verwaltung der Werte[1]

In Bezug auf die Verwaltung von Werten stellen die Lieferant sicher, dass

5.1. Werte von astora nicht ohne vorherige Genehmigung vom Firmengelände der astora entfernt werden.

5.2. Unternehmensinformationen logisch von fremden Informationen getrennt verarbeitet und gespeichert werden.

5.3. nach Abschluss oder Beendigung der Arbeiten für astora alle Kopien der Unternehmensinformationen, einschließlich aller Sicherungs- und Archivierungskopien, in elektronischer oder nicht elektronischer Form bereinigt und sicher vernichtet (oder auf Anfrage an astora zurückgesendet; Ausnahmen sind bei gesetzlichen Anforderungen möglich) werden. Über die sichere Vernichtung ist auf Anfrage von astora Nachweise mit relevanten Angaben vorzulegen (was, wann, wie, wer, ggf. Zeuge).

6. Anforderungen an Zugangssteuerung

Im Rahmen der Zugangssteuerung zu den Unternehmensinformationen stellen die Lieferanten in ihrem Verantwortungsbereich sicher, dass

6.1. das Anschließen von Geräten an die Infrastruktur von astora nur nach einer Genehmigung durch astora erfolgt.

6.2. an die Infrastruktur von astora angebundene Geräte mit einem aktuellen Schadsoftwareschutz ausgestattet sind und in Bezug auf Sicherheits- und Funktionsupdates auf dem neuesten Stand gehalten werden.

6.3. vor Einbringen eines externen Datenträgers in die Infrastruktur von astora (z.B. USB, CD, DVD, externe Festplatte) eine vorherige Überprüfung auf Schadsoftware vorgenommen wird.

6.4. der Fernzugriff auf die Infrastruktur von astora ausschließlich über von astora vorab genehmigte Kommunikationskanäle und -technologien (z.B. VPN, Standleitung, Zwei-Faktor-Authentifizierung) erfolgt.

6.5. elektronische Systeme, auf welchen Unternehmensinformationen verarbeitet, gespeichert oder

[1] Werte sind Daten, Anwendungen, Hardware, Komponenten der Prozessleittechnik, und andere Werte, die diese unterstützen.

übertragen werden, über ein angemessenes Zugriffs- und Identitätsmanagement entsprechend dem Stand der Technik verfügen.

7. Anforderungen an physische und umgebungsbezogene Sicherheit

7.1. Die Lieferanten stellen sicher, dass die seitens von astora festgelegten Regeln zum Betreten der Räumlichkeiten des Unternehmens streng befolgt werden.

8. Anforderungen an Betriebssicherheit

8.1. Informationssysteme der Lieferanten, die mit der Infrastruktur von astora permanent verbunden sind müssen folgendes sicherstellen:

a) Revisionssichere Protokollierung von sicherheitsrelevanten Benutzeraktionen mit einer Aufbewahrungszeit von mindestens 90 Tagen;
b) Aktueller Schadsoftwareschutz;
c) Schwachstellen- und Patch-Management.

8.2. astora ist über bestehende oder potenzielle Verfügbarkeitseinschränkungen der Informationssysteme, die sich in der Verwaltung der Lieferanten befinden, falls nicht anders geregelt, zu informieren.

9. Anforderungen an Kommunikationssicherheit

9.1. die auf Systemen oder Datenträgern gespeicherten bzw. verarbeiteten oder zu übertragenen Unternehmensinformationen sind nach dem Stand der Technik zu schützen (z.B. Verschlüsslung, Einsatz von Firewalls etc.)

9.2. Regeln in Bezug auf Klassifizierung und Handhabung von Informationen müssen streng beachtet werden. Vorgaben hinsichtlich des richtigen Umgangs mit klassifizierten Informationen sind dem Anhang A zu entnehmen.

10. Anforderungen an Handhabung von Informationssicherheitsvorfällen

10.1. Die Lieferanten haben über Prozesse zu verfügen, die im Kontext ihrer Organisation eine angemessene Behandlung von Sicherheitsvorfällen ermöglichen.

10.2. Sicherheitsvorfälle oder –Schwachstellen bei den Lieferanten, bei welchen Auswirkungen auf astora nicht sicher ausgeschlossen werden können, sind unverzüglich dem Ansprechpartner bei astora oder an it-security@astora.de zu melden.

11. Anforderungen an Compliance

11.1. Die Lieferanten müssen 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.

Anhang A: Klassifizierung von Informationen

Folgende Regeln sind für die Klassifizierung und Handhabung von Dokumenten in elektronischer, gedruckter oder anderer Form festgelegt:

Klassifizierung / Aktion	INTERNAL	CONFIDENTIAL	STRICTLY CONFIDENTIAL
Definition	Informationen zu internen Prozessen von astora, die einer Gruppe von Mitarbeitern oder Auftragnehmern gemäß dem „Need-to-know"-Prinzip zugänglich und nicht öffentlich sind.	Informationen zum Unternehmen, die für eine Gruppe von Mitarbeitern oder Auftragnehmern gemäß dem „Need-to-know"-Prinzip zugänglich sind. Die vertraulichen Informationen können die personenbezogenen Daten von Mitarbeitern, Informationen über rechtliche Vorgänge, Geschäfts- und Produktionspläne sowie Jahresabschlüsse und andere Geschäftsinformationen im Zusammenhang mit dieser von den Informationseigentümern festgelegten Vertraulichkeitsklasse umfassen.	Informationen, die für eine beschränkte Anzahl von Mitarbeitern gemäß dem „Need-to-know"-Prinzip zugänglich sind. Sie können alle Arten von Informationen (industrielle, finanzielle, kommerzielle Informationen etc.) umfassen, die aufgrund der Vertraulichkeit dieser Informationen gegenüber Dritten einen tatsächlichen oder potentiellen Wert haben.
Kennzeichnung	Implizit. Nichtgekennzeichnete Information sind immer als INTERNAL zu behandeln.	Immer zu kennzeichnen als CONFIDENTIAL. Fettgedruckte Großbuchstaben auf jeder Seite in der Kopfzeile. Seitenzahl und Gesamtzahl der Seiten in der Fußzeile.	Wie CONFIDENTIAL und zusätzlich Nennung sämtlicher Empfänger des Dokuments auf der ersten Seite.
Vervielfältigung mittels Kopiergerät oder Drucker	Originale so bald wie möglich aus dem Kopiergerät oder Drucker nehmen. Kopien, Ausdrucke und Scans sollen nicht mittels öffentlich zugänglicher Geräte angefertigt werden.	Der Prozess des Kopierens, Druckens bzw. Scannens muss überwacht werden. Kopien, Ausdrucke und Scans dürfen nicht mittels öffentlich zugänglicher Geräte angefertigt werden.	Wie CONFIDENTIAL. Kopieren oder Drucken ausschließlich mit Genehmigung des Informationseigentümers von astora..
Weiterleitung an Dritte	Ausschließlich mit Genehmigung des Informationseigentümers von astora.	**Verboten**. Anderweitige Regelungen können einzelvertraglich mit astora getroffen werden.	
Übermittlung per E-Mail	Sicherstellen, dass die E-Mail Adresse des Empfängers richtig ist.	Sicherstellen, dass die Adresse des Empfängers dienstlich und richtig ist. Der Empfänger muss zum Empfang dieser Informationen berechtigt sein. Text und Anhänge der E-Mail müssen verschlüsselt werden.	
Postsendung	Die Informationen können in einem normalen Umschlag senden.	Die Informationen in einem manipulationssicheren Umschlag senden und eine Empfangsbestätigung einholen (Verwendung eines versiegelten Umschlags mit Beschriftung CONFIDENTIAL in einem zweiten, äußeren Umschlag ohne Kennzeichnung).	Wie CONFIDENTIAL und zusätzlich per Einschreiben mit Übergabe an den Empfänger oder per Kurier senden.
Übermittlung per Fax	Sicherstellen, dass die Nummer des Empfängers richtig ist. Deckblatt verwenden, auf dem die Gesamtzahl der Seiten angegeben ist.	**Verboten.**	
Vernichtung von auf Papier niedergelegten Informationen	Dokumente mittels Schredder der Sicherheitsstufe P5 sicher vernichten.		

Klassifizierung / Aktion	INTERNAL	CONFIDENTIAL	STRICTLY CONFIDENTIAL
Mündliche Verbreitung	Nur zulässig, wenn keine Unbefugten mithören können. Verifizierung der Identität der Person, mit der gesprochen wird.		
Speichern von Informationen in IT-Anwendungen	Sicherstellen des need-to-know Prinzips. Maßnahmen zum Schutz vor unbefugtem Zugriff etablieren.		
Speichern von Informationen auf Dateiservern und mobilen Geräten	Informationen unter Berücksichtigung der Zugriffsrechte gemäß ihrer Klassifikation auf verfügbaren Laufwerken bzw. in Ordnern speichern; falls erforderlich Zugriffsrechte ausdrücklich zuweisen.	ZUSÄTZLICH sind die Informationen in verschlüsselten Ordnern zu speichern. Verschlüsselung darf mindestens die Standards AES-128 oder höher, RSA-2048 oder höher verwenden.	
Speichern von Informationen auf tragbaren Speichermedien.	Daten müssen verschlüsselt werden.		
Löschen elektronischer Informationen von tragbaren Speichermedien	Mehrfaches Überschreiben der verwendeten Speicherbereiche ermöglicht.		
Entsorgung tragbarer Speichermedien	physische Zerstörung der Speichermedien.		
Speicherung von Informationen in Cloud-Diensten	Grundsätzlich verboten. Anderweitige Regelungen können einzelvertraglich mit astora getroffen werden.		