Leitlinie zur Gewährleistung der Informationssicherheit für Lieferanten der Bolta Werke GmbH

Version 1.0 Stand 19.05.2017

Inhalt

Präambel

Für die Bolta Werke GmbH ist eine zuverlässig funktionierende Informations- und Kommunikations-technik (IT) zur Erfüllung der Aufgaben unerlässlich. Auch von den Lieferanten wird dies erwartet.

Die automatisierte Verarbeitung von Daten und Informationen spielt hierbei eine Schlüsselrolle. Alle wesentlichen Prozesse werden durch Informations- und Kommunikationstechnik maßgeblich unterstützt.

Durch die verstärkte Abhängigkeit von moderner IT-Technik hat sich das Risiko der Beeinträchtigung von Informationsinfrastrukturen und deren Komponenten durch vorsätzliche Angriffe von innen und außen, durch fahrlässiges Handeln, Unkenntnis oder potenzielles Versagen der Technik deutlich erhöht.

Mangelnde Informationssicherheit kann zu Störungen bei der Aufgabenerfüllung führen, die die Leistungsfähigkeit des Unternehmens mindern und im Extremfall deren Geschäftsprozesse zum Erliegen bringen.

Vor diesem Hintergrund ist ein angemessenes Niveau der Informationssicherheit in den Geschäftsprozessen der Lieferanten der Bolta Werke GmbH zu organisieren.

Die Verantwortung für die ordnungsgemäße und sichere Aufgabenerledigung und damit für die Informationssicherheit trägt der Lieferant.

Dieser ist insbesondere verantwortlich für

- die Schaffung organisatorischer Rahmenbedingungen zur nachhaltigen Gewährleistung von Informationssicherheit,
- die Definition und Festlegung der erforderlichen Verantwortlichkeiten und Befugnisse,
- die Einrichtung eines Informationssicherheits-Managements,
- die Umsetzung der vereinbarten Sicherheitsmaßnahmen einschließlich der Bereitstellung der erforderlichen Mittel,
- eine hinreichende und geeignete Dokumentation der IT-Infrastruktur sowie aller Sicherheitsvorkehrungen und Sicherheitsmaßnahmen.

Die vorliegende Leitlinie beschreibt die allgemeinen Anforderungen an den Lieferanten, welche für die Initiierung und Etablierung eines ganzheitlichen Informationssicherheitsprozesses erforderlich sind.

Geltungsbereich

Diese Leitlinie gilt für Lieferanten der Bolta Werke GmbH.
Die Leitlinie und die daraus resultierenden Vorschriften und Maßnahmen sind von allen Lieferanten der Bolta Werke GmbH zu beachten und einzuhalten.

1. Grundsätze der Informationssicherheit

1.1. Begriffseinführung

Informationssicherheit bezeichnet einen Zustand, in dem die Risiken für die Sicherheitsziele Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Informationstechnik durch angemessene Maßnahmen auf ein akzeptierbares Maß reduziert sind. Die Informationssicherheit umfasst neben der Sicherheit der IT-Systeme und der darin gespeicherten Daten auch die Sicherheit von nicht elektronisch verarbeiteten und gespeicherten Daten und Informationen.
Dabei bedeuten:

- **Vertraulichkeit**
  Die Vertraulich wird durch Rechtsnormen geschützt. Vertrauliche Daten, Informationen (z.B. Verbindungsdaten) und Programme sind vor unberechtigten Zugriffen und unbefugter Preisgabe zu schützen. Sie sind nur für einen beschränkten Empfängerkreis vorgesehen.

- **Integrität**
  Unter Integrität versteht man die Korrektheit, also die Unversehrtheit von Daten und der Korrektheit von Systemen. Arten der Integrität sind der korrekte Inhalt, ein unmodifizierter Zustand, die Erkennung von Modifikationen und die temporale Korrektheit von Daten.

- **Verfügbarkeit:**
  Die Funktionen der Hard- und Software im System- und Netzbereich sowie notwendige Informationen stehen dem Anwender zum richtigen Zeitpunkt am richtigen Ort zur Verfügung.

1.2. Bedeutung der Informationssicherheit beim Einsatz

Der Lieferant stellt sicher, dass alle Einrichtungen, die der Erstellung, Speicherung und Übertragung von Daten dienen, so ausgewählt, integriert und konfiguriert sind, dass für die auf ihnen verarbeiteten Daten zu jeder Zeit und unter allen Umständen das angemessene Maß an Vertraulichkeit, Integrität und Verfügbarkeit sichergestellt ist. Dies gilt auch für die Orte zur Aufbewahrung der Medien zur Datensicherung.
Die Einhaltung dieser Anforderungen ist unabdingbarer Bestandteil jedes Einsatzes von IT-Technik und ist mit technischen und organisatorischen Maßnahmen verbindlich sicherzustellen.

1.3. Informationssicherheit als Leistungsmerkmal von IT-Verfahren

Die Informationssicherheit ist ein zu bewertendes und herbeizuführendes Leistungsmerkmal von IT-Verfahren. Bleiben im Einzelfall trotz der Sicherheitsvorkehrungen Risiken untragbar, ist auf den IT-Einsatz zu verzichten. Belange der Informationssicherheit sind zu berücksichtigen bei

- der Entwicklung und Einführung von IT-Verfahren,
- dem Betrieb und der Pflege von IT-Verfahren,
- der Beschaffung und Beseitigung / Entsorgung von IT-Produkten,
- der Nutzung von Diensten Dritter.

1.4. Informationssicherheit als Leistungsmerkmal der Organisation

Technische und organisatorische Sicherheitsmaßnahmen sind so zu gestalten, dass diese stets integraler Bestandteil aller Verwaltungsprozesse sind und nicht Erweiterungen, die über das vermeintlich Notwendige hinausgehen. Belange der Informationssicherheit sind zu berücksichtigen bei

- der Gestaltung der Organisation,
- der Schaffung und Besetzung von Funktionen und Rollen,
- der Führung von Mitarbeitern,
- der Aus- und Weiterbildung,
- der Gestaltung von Arbeitsabläufen und Prozessen
- der Zusammenarbeit mit anderen Behörden und Externen,
- der Auswahl und dem Einsatz von Hilfsmitteln.

1.5. Wirtschaftlichkeit

Die Sicherheitsmaßnahmen müssen in einem wirtschaftlich vertretbaren Verhältnis zum Schaden stehen, der durch Sicherheitsvorfälle verursacht werden kann. Dieser wird durch den Wert der zu schützenden Informationen und der IT-Systeme definiert. Zu bewerten sind dabei in der Regel die Auswirkungen auf die körperliche und seelische Unversehrtheit von Menschen, das Recht auf informationelle Selbstbestimmung, finanzielle Schäden, Beeinträchtigungen des Ansehens der Verwaltung und die Folgen von Gesetzesverstößen.

1.6. Regelungskompetenz

Sicherheitsanforderungen von übergeordnetem Interesse, für deren Umsetzung eine vertragliche oder gesetzliche Verpflichtung besteht, sind zu erfüllen. Entsprechende Vorschriften und Maßnahmen stellen den Mindeststandard bei der Formulierung interner Vorschriften und Maßnahmen dar.
Die Wahl der Mittel und die Formulierung von Arbeitsanweisungen, mit denen die Sicherheitsziele erreicht werden sollen, obliegt den Bereichen und Abteilungen selbst. Sie können eigenständig angemessene Sicherheitsmaßnahmen planen und umsetzen.

1.7. Sicherheit vor Verfügbarkeit

Wenn Angriffe auf die Sicherheit der IT-Infrastruktur der Bolta Werke GmbH drohen oder bekannt werden oder sonstige Sicherheitsrisiken auftreten, kann die Verfügbarkeit von IT-Technik, IT-Anwendungen, Daten und Netzwerken entsprechend dem Bedrohungs- und Schadensrisiko vorübergehend eingeschränkt werden. Im Interesse der Funktionsfähigkeit des gesamten Unternehmens ist der Schutz vor Schäden vorrangig.

1.8. Prinzip des informierten Mitarbeiters

Die Mitarbeiter sind im erforderlichen Umfang bezüglich der Informationssicherheit zu sensibilisieren und zu qualifizieren.

2. Informationssicherheitsziele

2.1. Verfügbarkeit

Verfügbarkeit - die Gewährleistung, dass Informationen, Anwendungen und IT-Systeme für Berechtigte im vorgesehenen Umfang und in angemessener Zeit nutzbar sind. Betriebsunterbrechungen sind weitgehend zu vermeiden. Wartungsarbeiten sind nach Zahl und Dauer zu begrenzen, bzw. so zu legen das Betriebsstörungen so gering wie möglich gehalten werden.

2.2. Vertraulichkeit

Vertraulichkeit - die Gewährleistung, dass Informationen ausschließlich Berechtigten zugänglich sind.
Zu diesem Zweck ist für alle Daten der Personenkreis, dem der Zugriff gestattet werden soll, zu bestimmen. Jeder Mitarbeiter erhält eine Zugriffsberechtigung nur auf die Daten, die er zur Erfüllung seiner dienstlichen Aufgaben benötigt. Der Zugriff auf IT-Systeme, IT-Anwendungen und Daten sowie Informationen ist auf den unbedingt erforderlichen Personenkreis zu beschränken.

2.3. Integrität

Informationen sind gegen unbeabsichtigte Veränderung und vorsätzliche Verfälschung zu schützen. Dokumentation (Protokolle) machen dies überprüfbar damit alle IT-Verfahren stets aktuelle und vollständige Informationen liefern.

3. Verantwortlichkeiten

3.1. Verantwortung der Mitarbeiter

Alle Mitarbeiter gewährleisten die Informationssicherheit durch verantwortungsbewusstes Handeln und halten die für die Informationssicherheit relevanten Gesetze, Vorschriften, Richtlinien, Anweisungen und vertraglichen Verpflichtungen ein. Sie gehen korrekt und verantwortungsvoll mit den von ihnen genutzten IT-Systemen, Daten und Informationen um. Verhalten, das die Sicherheit von Daten, Informationen, IT-Systemen oder der Netze gefährdet, kann disziplinar- oder arbeitsrechtlich geahndet werden. Unter Umständen kann das Verhalten als Ordnungswidrigkeit oder Straftat verfolgt werden.
Mitarbeiter, die die Sicherheit von Daten, Informationen, IT-Systemen oder des Netzes gefährden und einen Schaden für die Bolta Werke GmbH oder einen Dritten verursachen, können darüber hinaus nach den gesetzlichen Regelungen zum Schadenersatz herangezogen werden oder einem Rückgriffsanspruch ausgesetzt sein.
Verstöße gegen die Informationssicherheit sind unverzüglich dem zuständigen Beauftragten für Informationssicherheit (s. Pkt. 4.1) zu melden.

3.2. Verantwortung externer Leistungserbringer

Personen, Behörden und Unternehmen, die nicht zur Bolta Werke GmbH gehören, für diese aber Leistungen erbringen (Auftragnehmer), haben die Vorgaben des Auftraggebers zur Einhaltung der Informationssicherheitsziele gemäß dieser Leitlinie einzuhalten.
Der Auftraggeber informiert den Auftragnehmer über diese Regeln und verpflichtet ihn in geeigneter Weise zur Einhaltung. Dazu gehört auch, dass der Auftragnehmer bei erkennbaren Mängeln und Risiken eingesetzter Sicherheitsmaßnahmen den Auftraggeber zu informieren hat.

4. Informationssicherheitsorganisation

4.1. Beauftragter für Informationssicherheit

Als zentrale Sicherheitsinstanz der Bolta Werke GmbH ernennt die Geschäftsleitung einen Beauftragten für Informationssicherheit (BfIS), der für alle operativen Belange und Fragen der Informationssicherheit zuständig ist.
Im jeweiligen Zuständigkeitsbereich hat der BfIS folgende Aufgaben:

- Mitwirkung bei allen zusammenhängenden Aufgaben des Informationssicherheitsprozesses,
- Überprüfung der Umsetzung der Vorgaben zur Informationssicherheit,
- Vorschlag von neuen Sicherheitsmaßnahmen und –strategien,
- Ansprechpartner für die Mitarbeiter in den Fragen der Informationssicherheit,
- Koordination von Sensibilisierungs- und Schulungsmaßnahmen,
- Meldung von besonders sicherheitsrelevanten Zwischenfällen im Rahmen seiner Berichtswege.

4.2. Informationssicherheitsmanagement-Teams

Zur Unterstützung des BfIS bei der Erfüllung seiner Aufgaben können temporär Informationssicherheitsmanagement-Teams gebildet werden, um bei strategischen Entscheidungen oder Einzelmaßnahmen(z. B. bei Projekten entsprechender Größenordnung) die Belange der Informationssicherheit der Bolta Werke GmbH sicherzustellen.

5. Umsetzung

Diese Leitlinie bildet die Grundlage für die Erstellung weiterer, auch fachspezifischer Richtlinien, Informationssicherheitskonzepte und detaillierter Regelungen und Anweisungen zur Informationssicherheit.

6. Sicherung und Verbesserung der Informationssicherheit

Der Informationssicherheitsprozess ist regelmäßig auf seine Aktualität und Wirksamkeit zu überprüfen. Insbesondere sind die Maßnahmen regelmäßig daraufhin zu untersuchen, ob sie den betroffenen Mitarbeitern bekannt, umsetzbar und in den Betriebsablauf integrierbar sind.
Die Leitungsebenen unterstützen die ständige Verbesserung des Sicherheitsniveaus.
Die Mitarbeiter 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.