1. Zweck und Geltungsbereich

Der Schutz von Informationen ist eine wesentliche Voraussetzung für die Geschäftstätigkeit der Advanced UniByte GmbH. Diese Informationssicherheitspolitik beschreibt die strategische Ausrichtung, die übergeordneten Ziele und die Verpflichtungen der Advanced UniByte GmbH zur Informationssicherheit.

Die Informationssicherheitspolitik gilt innerhalb des festgelegten Anwendungsbereichs des Informationssicherheitsmanagementsystems für sämtliche Organisationseinheiten, Beschäftigte, Prozesse, Informationen, Informationssysteme, Anwendungen und Standorte der Advanced UniByte GmbH.

Anforderungen an relevante externe Parteien, insbesondere Lieferanten, Partner und Dienstleister, werden abhängig von der Art der Zusammenarbeit und den damit verbundenen Informationssicherheitsrisiken festgelegt und, soweit erforderlich, vertraglich vereinbart.

2. Stellenwert der Informationssicherheit

Die Advanced UniByte GmbH ist seit Jahrzehnten im hochsensiblen Umfeld kritischer Enterprise-IT-Projekte tätig. Informationssicherheit ist daher fest in den Strukturen, Abläufen und der Unternehmensstrategie der Advanced UniByte GmbH verankert.

Angesichts einer sich stetig verändernden Bedrohungslage stärkt die Advanced UniByte GmbH die Widerstandsfähigkeit ihrer Organisation durch die risikobasierte Umsetzung und fortlaufende Verbesserung angemessener technischer und organisatorischer Maßnahmen. Diese werden durch das Informationssicherheitsmanagementsystem gesteuert.

Die Geschäftsführung trägt die Gesamtverantwortung für die Informationssicherheit, unterstützt das Informationssicherheitsmanagementsystem und stellt die für dessen Aufrechterhaltung und Weiterentwicklung erforderlichen Ressourcen bereit. Der Schutz von Informationen erstreckt sich auf den gesamten festgelegten Anwendungsbereich des Informationssicherheitsmanagementsystems.

3. Informationssicherheitsziele

Die Informationssicherheit der Advanced UniByte GmbH orientiert sich insbesondere an den Schutzzielen Vertraulichkeit, Integrität und Verfügbarkeit. Auf dieser Grundlage legt die Advanced UniByte GmbH messbare Informationssicherheitsziele fest und überprüft deren Erreichung regelmäßig. Die Ziele berücksichtigen die strategische Ausrichtung, die relevanten Anforderungen sowie die Informationssicherheitsrisiken der Organisation.

Vertraulichkeit: Schutz sensibler und personenbezogener Informationen vor unberechtigtem Zugriff.

Integrität: Gewährleistung der Unversehrtheit von Informationen und der korrekten Funktion von Systemen.

Verfügbarkeit: Sicherstellung, dass Informationen und Systeme zum benötigten Zeitpunkt zugänglich und nutzbar sind.

Die Informationssicherheitsziele werden risikobasiert, unter Berücksichtigung des Stands der Technik sowie der zutreffenden gesetzlichen, behördlichen, regulatorischen, vertraglichen und internen Anforderungen verfolgt. Die Advanced UniByte GmbH richtet ihr Handeln dabei an den folgenden Leitsätzen aus:

- Der Schutz von Leben und Gesundheit hat oberste Priorität.
- Cyber Resilience im Fokus: Widerstandsfähigkeit der Organisation stärken
- Beschäftigte, Kunden und Geschäftspartner können auf die Sicherheit der Advanced UniByte GmbH vertrauen.
- Die Advanced UniByte GmbH nutzt bevorzugt eigene Kompetenzen zur Stärkung ihrer Cyber Resilience.

4. Verpflichtungen zur Informationssicherheit

Die Advanced UniByte GmbH ist sich ihrer Verantwortung für die Informationssicherheit bewusst. Die Geschäftsführung verpflichtet sich und alle Beschäftigten zur Einhaltung der für ihre Tätigkeiten geltenden gesetzlichen, behördlichen, regulatorischen, vertraglichen und internen Anforderungen sowie der geltenden Richtlinien, Prozesse und sonstigen Vorgaben zur Informationssicherheit. Die hierfür erforderlichen Kenntnisse und Kompetenzen werden durch regelmäßige Informationen, Schulungen und Awarenessmaßnahmen vermittelt und gefördert.

Die Advanced UniByte GmbH verpflichtet sich zur fortlaufenden Verbesserung der Eignung, Angemessenheit und Wirksamkeit ihres Informationssicherheitsmanagementsystems.

Anforderungen an Lieferanten, Partner und Dienstleister werden abhängig von der Art der Zusammenarbeit, den betroffenen Informationen und Systemen sowie den damit verbundenen Informationssicherheitsrisiken festgelegt und, soweit erforderlich, vertraglich vereinbart.

Die Geschäftsführung stellt angemessene personelle, organisatorische, technische und finanzielle Ressourcen für die Aufrechterhaltung und fortlaufende Verbesserung des Informationssicherheitsmanagementsystems bereit. Zur organisatorischen Unterstützung ist ein Informationssicherheitsbeauftragter benannt. Dieser koordiniert und überwacht die Umsetzung der Informationssicherheitspolitik im Rahmen der ihm übertragenen Aufgaben und Befugnisse.

Die Advanced UniByte GmbH verpflichtet sich insbesondere zu folgenden Grundsätzen:

- Informationssicherheitsrisiken werden systematisch identifiziert, analysiert, bewertet und angemessen behandelt.
- Informationssicherheitsereignisse, Schwachstellen und Sicherheitsvorfälle können über einfach zugängliche und bekannte Meldewege gemeldet werden. Meldungen werden systematisch erfasst, dokumentiert, bewertet und abhängig von ihrer Kritikalität behandelt.
- Regelmäßige Schulungen und Awarenessmaßnahmen stärken die erforderlichen Kompetenzen und fördern eine nachhaltige Sicherheitskultur.
- Verantwortlichkeiten und Befugnisse für die Informationssicherheit werden festgelegt und innerhalb der Organisation kommuniziert.
- Informationssicherheit wird bei relevanten Geschäftsprozessen, Projekten, Veränderungen sowie Lieferantenbeziehungen angemessen berücksichtigt.

5. Überprüfung und Verbesserung der Informationssicherheit

Die Advanced UniByte GmbH überprüft regelmäßig die Eignung, Angemessenheit und Wirksamkeit ihres Informationssicherheitsmanagementsystems. Die Ergebnisse der Überprüfungen werden bewertet und zur fortlaufenden Verbesserung des Informationssicherheitsmanagementsystems verwendet.

Hierzu werden insbesondere folgende Maßnahmen durchgeführt:

- regelmäßige Bewertung der Informationssicherheitsziele und der zugehörigen Kennzahlen
- regelmäßige Bewertung der Informationssicherheitsrisiken
- Auswertung von Informationssicherheitsereignissen, Schwachstellen und Sicherheitsvorfällen
- interne Audits entsprechend dem festgelegten Auditprogramm
- externe Audits im Rahmen der Zertifizierung des Informationssicherheitsmanagementsystems
- Managementbewertungen des Informationssicherheitsmanagementsystems
- Nachverfolgung von Korrektur- und Verbesserungsmaßnahmen
- risikobasierte Überprüfung informationssicherheitsrelevanter Lieferanten und Lieferantenbeziehungen
- Unterstützung vereinbarter Audits durch Kunden und andere berechtigte Geschäftspartner

Die Informationssicherheitspolitik wird in geplanten Abständen sowie bei wesentlichen Veränderungen überprüft und bei Bedarf angepasst. Änderungen an der Informationssicherheitspolitik werden durch die Geschäftsführung freigegeben.

6. Kontakt

Fragen, Hinweise sowie Meldungen zur Informationssicherheit können per E-Mail an *informationssicherheit(at)au.de* gerichtet werden.