Corporate Policy:

CP1-010

Informationssicherheit / Information Security

Anforderungen begegnen

Wir, die Bausch+Ströbel SE + Co. KG, nachfolgend „Bausch+Ströbel“) sind uns unserer ganzheitlichen Verantwortung für die Daten und Informationen von unseren Kunden, Geschäftspartnern und Beschäftigten bewusst.
Wir haben Regelungen zur Umsetzung von Informationssicherheit getroffen und dokumentiert. Die Abteilungen im Bereich IT sowie definierte Verantwort-liche für die eingesetzten IT-Systeme führen mit Unter-stützung der jeweils zuständigen Führungskräfte konti-nuierlich einen Soll-Ist-Vergleich durch und veranlassen die notwendigen Ver-besserungen. Die Angemessenheit der umgesetzten Maßnahmen und Verbesserungen wird im Rahmen der geplanten internen Audits sowie weiteren Über-prüfungen, teilweise unter Beauftragung externer Firmen, kontrolliert.
Für Themen im Bereich Datenschutz unterstützt ein externes Unternehmen.
Aus dieser unternehmerischen Verpflichtung heraus legen wir folgende Politik für den Schutz von Informationen und Geschäftsprozessen fest:

Leitbild

Die Kernkompetenz von Bausch+Ströbel umfasst die Entwicklung, die Herstellung, den Vertrieb und den After-Sales-Service von Verpackungs- und Produktionssystemen für die pharmazeutische, kosmetische und artverwandte Industrie einschließlich der damit verbundenen Dienstleistungen. Es ist unerlässlich, mit unseren Kunden und Interessenten in einem stark regulierten Umfeld hochtechnologische Prozesse in unseren Maschinen und Anlagen umzusetzen. Die Vertraulichkeit, Integrität und Verfügbarkeit aller verarbeiteten Informationen hat dabei höchste Priorität.
Das uns entgegengebrachte Vertrauen und letztlich unser Geschäftserfolg beruht darauf, dass wir in Bezug auf die Informationssicherheit insbesondere:

+ gesetzliche, regulatorische sowie vertragliche Anforderungen einhalten.
+ die Vertraulichkeit, Integrität und Verfügbarkeit der durch Bausch+Ströbel verarbeiteten Informationen und Daten (insbesondere Daten von interessierten Parteien, geistiges Eigentum sowie Betriebsgeheimnisse) sicherstellen.
+ Datenverlust vermeiden.

Meeting Requirements

We, Bausch+Ströbel SE + Co. KG (hereinafter: Bausch+Ströbel) are aware of our holistic responsibility for the data and information of our customers, business partners and employees.

We have established and documented regulations concerning the implementation of information security. The IT area as well as defined responsibles for the IT systems used - supported by the responsible executives - periodically perform target-actual comparisons and initiate required improvements where necessary. The appropriateness of the implemented measures and improvements is checked as part of the planned internal audits and other reviews, some of which are carried out by external companies.
An external company provides support and advice on data protection issues.
Based on this corporate obligation, we establish the following policy for the protection of information and business processes:

Mission Statement

The core competence of Bausch+Ströbel includes the development, manufacture, distribution and after-sales service of packaging and production systems for the pharmaceutical, cosmetic and related industries, including related services. It is essential that we implement high-tech processes in our machines and systems with our customers and prospective customers in a highly regulated environment. The confidentiality, integrity and availability of all the information processed is of the utmost priority.

The trust placed in us and ultimately our business success is based on the fact that, with regard to information security in particular, we:

+ comply with legal, regulatory and contractual requirements.
+ ensure the confidentiality, integrity and availability of the information and data processed by Bausch+Ströbel (in particular data from interested parties, intellectual property and trade secrets)
+ avoid data loss.

+ Risiken und Gefahren angemessen behandeln, die z.B. durch die Technik (Strom-/ Internetausfall bzw. Ausfall der IT-Infrastruktur), durch elementare Gefahren der Umwelt (z.B. Überschwemmung, Feuer) sowie durch kriminelle Handlungen (Industriespionage, IT-Sabotage, Cyberangriffe, Datendiebstahl oder Einbruchdiebstahl/ Raub) bedingt sind.

Das Einhalten aller für uns bindenden Verpflichtungen, wie gesetzliche, Kunden- und eigene Anforderungen, bildet hierbei eine vertrauensvolle Basis für eine langfristige Zusammenarbeit mit allen interessierten Parteien.

Informationssicherheit ist daher eines der grundlegenden Ziele zur ständigen Verbesserung der Prozesse unseres
Unternehmens. Alle Führungskräfte und die Beschäftigten sind verpflichtet, die gesetzlichen Vorschriften und die betrieblichen Vorgaben hinsichtlich Informationssicherheit jederzeit einzuhalten.

Ressourceneinsatz

Wir sehen den bewussten Umgang mit Informationen in allen Bereichen unseres Unternehmens als wesentlichen Erfolgsfaktor an.

Durch eine gelebte Informationssicherheitspolitik und die kontinuierliche Weiterentwicklung unseres Informationssicherheitsmanagementsystems (ISMS) werden eingesetzte Ressourcen auf den Schutz von Informationen und Geschäftsprozessen ausgerichtet. Mit der risikobasierten Umsetzung von Sicherheitsmaßnahmen sichern wir unsere Position auf dem Markt und bauen diese weiter aus. Alle Ressourcen und Dienstleistungen, welche Einfluss auf von uns genutzte Informationen und Geschäftsprozesse haben, werden unter Berücksichtigung von Vertraulichkeit, Integrität und Verfügbarkeit ausgewählt, beurteilt, kontrolliert und überwacht.

+ Treat risks and dangers appropriately caused by technology (power failure / internet failure or failure of the IT infrastructure), by elementary dangers of the environment (e.g. flood, fire) as well as risks/hazards caused by criminal acts (industrial espionage, IT sabotage, cyber attacks, data theft or burglary / robbery).

Compliance with all obligations that are binding for us, such as legal, customer and our own requirements, forms a trusting basis for long-term cooperation with all interested parties.

Information security is therefore a fundamental goal for the continuous improvement of our company. Executives and employees are obliged to permanently follow the legal regulations and the company guidelines covering information security.

Use of Resources

We regard the confidential handling of information in all areas of our company as an essential success factor.

Through a practiced information security policy and the continuous development of our information security management system (ISMS), resources are directed towards the protection of information and business processes. With our risk-based approach to safety measures, we secure our position in the market and continue to expand it. All resources and services that have an influence on the information and business processes we use are selected, assessed, controlled and monitored with regard to confidentiality, integrity and availability.

Betriebsstörungen und Notfälle

Verbleibende Restrisiken können bspw. durch Störungen oder Ausfälle der verschiedenen Systeme und durch Verstöße gegen die Informationssicherheitsvorgaben auftreten.

Treten Betriebsstörungen oder Notfälle erstmalig auf, werden die Szenarien mit der gebotenen Dringlichkeit analysiert, um den Soll-Zustand durch festzulegende Maßnahmen unmittelbar wiederherstellen zu können.

Mitarbeiterorientierung

Unsere Beschäftigten bilden den Grundstein für unseren Erfolg. Mittels unserem Informationssicherheitsmanagement und den darauf ausgerichteten Prozessen stellen wir sicher, dass ein vertrauensvoller Umgang mit Informationen durch unsere Mitarbeiter und Dienstleister erfolgt. Jeder unserer Mitarbeiter und Dienstleister ist dazu verpflichtet, Gefahren zu minimieren bzw. diese umgehend zu melden. Ein hohes Maß an Informationssicherheit ist Grundvoraussetzung für ein zukunftsorientiertes Unternehmen. Die Minimierung von Risiken und die Beseitigung von Gefahren sind für Bausch+Ströbel ein Grundstein des Erfolges. In wesentlichen Fragen werden unsere Mitarbeiter konsultiert und eingebunden. Damit ist sichergestellt, dass auch deren Erfahrungen in die Verbesserung unseres Unternehmens einfließen.

Alle Beschäftigten sind demnach aufgefordert / verpflichtet

+ alle im jeweiligen Umfeld relevanten Gesetze, Vorschriften und Regelungen zu kennen und einzuhalten.
+ regelmäßig an den angebotenen Trainingsmaßnahmen teilzunehmen.
+ sich anforderungsgerecht zu verhalten und mit Informationen und Daten mit der gebotenen Sicherheit und Vertraulichkeit umzugehen.
+ Virenmeldungen, mögliche Sicherheitsvorfälle bzw. Sicherheitsereignisse umgehend gem. der definierten und bekannten Meldewege an die verantwortlichen Stellen zu melden.
+ ihr spezifisches Wissen einzubringen, um die Informationssicherheit ständig weiter zu entwickeln.

Operational interruptions and emergencies

Remaining residual risks can arise, for example, from malfunctions or failures of the various systems and breaches of information security demands.

If operational disruptions or emergencies occur for the first time, the scenarios are analysed with the necessary urgency in order to be able to immediately restore the target state by means of measures to be defined.

Employee orientation

Our employees are the cornerstone of our success. By means of our information security management and the processes geared to it, we ensure that our employees and service providers handle information in a trustworthy manner. Each of our employees and service providers is obliged to minimize dangers or to report them immediately. A high level of information security is a basic requirement for a future-oriented company.
The minimization of risks and the elimination of hazards are a cornerstone of success for Bausch+Ströbel. Our employees are consulted and involved in essential questions. This ensures that their experience also flows into the improvement of our company.

All employees are instructed / committed

+ to comply with all relevant laws, rules and regulations in the respective environment.
+ to regularly participate in trainings offered.
+ to act as required and to handle information and data with the necessary security and confidentiality.
+ report viruses, possible security incidents or security events immediately to the responsible authorities in accordance with the defined and known reporting channels.
+ to contribute with their specific knowledge to continuously further develop the information security aspect.

Prozessorientierung und Kennzahlen

Sowohl unsere Organisation als auch unsere Prozesse unterliegen der kontinuierlichen Verbesserung, um die Ver-traulichkeit, Integrität und Verfügbarkeit stetig zu verbessern. Ziele zur Informationssicherheit sind ebenfalls Bestandteil unserer Unternehmensziele und werden gleich-bedeutend mit Qualitäts-, Arbeits-, Umwelt-, Energie-Management- und wirtschaftlichen Zielen gewichtet. In regelmäßig festgelegten Abständen überprüfen wir unsere Vorgaben und stellen so den kontinuierlichen
Verbesserungsprozess sicher. Alle Informationen und Ressourcen, welche für die Zielerreichung erforderlich sind, werden zur Verfügung gestellt.

Process orientation and key figures

Both our organization and our processes are subject to continuous improvement in order to constantly improve their confidentiality, integrity and availability. Information security goals are also part of our corporate objectives and are weighted equally with quality, labor, environmental, energy management and economic goals. We review our targets at regular intervals to ensure a continuous improvement process. All information and resources required to achieve the objectives are made available.

Verstöße

Verstöße gegen die Informationssicherheit können das Ansehen von Bausch+Ströbel bei Kunden, Geschäftspartnern und Beschäftigten nachhaltig schädigen. Sie werden daher nicht toleriert und angemessen sanktioniert.
Verstöße werden den definierten Stellen gemeldet und durch diese weiterverfolgt.

Violations

Violations of information security can cause lasting damage to the reputation of Bausch+Ströbel in the eyes of customers, business partners and employees. They will therefore not be tolerated and will be sanctioned appropriately.
Violations will be reported to the defined authorities and followed up by them.

Ilshofen, 2026-04-22

Markus Ströbel | Thorsten Bullinger | Frank Preißner

Verteiler:

VS	QQ/QM	QQ//QP	QQ/QU	QQ//MD	QQ//QC	QQ/ESM	QQ/QSC	DSB	
VVS	MKT	PMS	SALES	SENG	CSV	CCP	SPSC	FSV	TSV
VTS	PM	PPM	FPT	TRQ	RD	RD/PMD	DPS	DDA	RTP
	DST	DDT	PAL	PAL1	PAL2	EED	PCL	PCL1	PCL2
	PCL3	BSN							
VPL	SFK	BFA	BFB	LSB	BFS	vEFK	SGG		
	INE	SCMP	SCM	PPRM	PP	WPC	SD	FE	FSG
	LOG	LOG/OLS							
VRC	RT	MC							
VFA	BPM	CTM	COR	HR	HR//AM	HR//AE	HR//AS	PT	GFM
	IT	IT-BPS	IT-SIA						
Betriebsarzt		Betriebsrat		ASEDO			Reinigungs-unternehmen		

Änderungsverzeichnis:

Vers.	Änderungsgrund	Version wirksam ab:	Seite
01	Erste freigegebene Ausgabe *Ersteller dieser Version: D. Stankowski, QQ/SM* *Empfohlene Schulungsstufe: 3 (Schulungsbestätigung erforderlich)*	**2024-07-14**	gesamt
01.1	2023-10-10, xpf: Dokument zweisprachig gestaltet		
02	Dokument an neues Layout angepasst Textpassagen und Abschnitte aus ehemaligen MH-Kapitel MH1-151 in Abschnitte „Anforderungen begegnen“, „Leitbild“ und „Mitarbeiterorientierung“ übernommen. Abschnitt „Betriebsstörungen und Notfälle“ integriert *Ersteller dieser Version: H. Leipersberger, QQ/QM* *Empfohlene Schulungsstufe:*1 *(Verteilung des Dokuments nur zur Info)*	**2024-08-19**	gesamt
03	Dokument in Bezug auf die Umsetzung eines zertifizierungsfähigen ISMS konkretisiert und erweitert. Änderungen sind nicht gekennzeichnet. *Ersteller dieser Version: L. Roth, HVS + R. Rösch, QQ/QM* *Empfohlene Schulungsstufe: I (Verteilung des Dokuments nur zur Info)*	**2025-04-22**	gesamt
04	Dokument an neues Layout angepasst Schreibweise „Bausch + Ströbel“ zu „Bausch+Ströbel“ angepasst Unterschriftenfelder der Vorstände angepasst: Dr. H. Gehringer, A. Gakhar, B. Frisch entfernt und F. Preißner hinzugefügt Änderungen sind nicht gekennzeichnet *Ersteller dieser Version: Marvin Charrier (cham), HR-AHP* *Empfohlene Schulungsstufe:* I (*Verteilung* des Dokuments nur zur Info)	**JJJJ-MM-TT**	gesamt

2026-05-20	thb- T. Bruchdorfer	2026-05-27	rro-
Datum:	Inhaltlich freigegeben: IT	Datum:	Formal freigegeben: QQ/QM