WIR BEWEGEN IT.

Leitlinie zur Informationssicherheit

SHD System-Haus-Dresden GmbH

Vertraulichkeit:	öffentlich - C0
Status:	Freigegeben
Version:	2.0
Datum:	31.01.2025

Grundsätze

Die SHD System-Haus-Dresden GmbH (SHD) ist als IT-Dienstleistungsunternehmen in den Bereichen Beratung, Realisierung und Betreuung vom komplexen IT-Systemlösungen an mehreren Standorten in Deutschland tätig.
Die SHD betreut dabei mittlere bis große Kunden aus den Bereichen Industrie, Gesundheit, Forschung und öffentliche Einrichtungen und agiert als strategischer Partner zahlreicher am Weltmarkt führender Hersteller und in deutschlandweiter Kooperation mit weiteren IT-Partnerunternehmen.
Die Kernprozesse der SHD bestehen in der Projekt- und Servicetätigkeit mit den Kunden und der damit verbundenen Auftrags- und Vertragsbearbeitung. Alle wesentlichen strategischen und operativen Funktionen und Aufgaben und die Verarbeitung von Daten werden durch Informationstechnik (IT) maßgeblich unterstützt.

Die Unternehmensleitung der SHD verpflichtet sich zur Sicherstellung der Kontinuität der Kernprozesse und zum Schutz der eigenen und der von SHD betreuten Daten und Werte von Kunden und Partnerunternehmen, eine IT-Sicherheitsorganisation zu etablieren und mit angemessenen Ressourcen und regelmäßiger Kontrolle die Einhaltung der Informationssicherheitsziele zu unterstützen. Durch eine Zertifizierung nach ISO/IEC Norm 27001 sollen diesbezügliche Anstrengungen auch den Kunden und Partnern transparent belegt werden können.

Sicherheitsorganisation

Die Gesamtverantwortung für die Informationssicherheit trägt die Geschäftsführung. Sie beruft und beauftragt für den gesamten Anwendungsbereich einen Datenschutzbeauftragten (DSB), einen Notfallbeauftragten und einen Informationssicherheitsbeauftragten (ISB). Der ISB steuert den Aufbau und den Betrieb des Informationssicherheitsmanagementsystems (ISMS). Dabei arbeitet er eng mit dem Datenschutzbeauftragten und dem Notfallbeauftragten zusammen. Der ISB ist als Stabsstelle der SHD direkt der Geschäftsführung unterstellt und erhält von dieser die erforderlichen Ressourcen und notwendigen Befugnisse. Er ist für die Umsetzung der festgelegten Richtlinien, die Durchführung definierter Kontrollen und für die Behandlung von erkannten Abweichungen oder Sicherheitsvorfällen zuständig und berichtet direkt der Geschäftsführung.
Der ISB ist frühzeitig in alle Projekte einzubinden, um schon in der Planungsphase sicherheitsrelevante Aspekte zu berücksichtigen. Sofern personenbezogene Daten betroffen sind, gilt Gleiches für den DSB.

Zur umfassenden Beurteilung wesentlicher Geschäftsinteressen der SHD werden die Grundsätze zur Informationssicherheit in einem ISMS-Team abgestimmt. Der ISB organisiert und koordiniert die Arbeit dieses ISMS-Teams und ist für die Aufzeichnungen aller wesentlichen Aktivitäten und Beschlüsse des ISMS-Teams zuständig.

Bei gravierenden Abweichungen bzw. Sicherheitsvorfällen wird entsprechend dem Notfallplan der SHD ein Krisenstab zur Steuerung notwendiger Abwehr- bzw. Beweissicherungsmaßnahmen gebildet.

Informationssicherheitsziele

Sicherstellung des kontinuierlichen Betriebes

Die Kontinuität der Geschäftsprozesse ist eine wichtige Grundlage für den wirtschaftlichen Erfolg der SHD. Die Einhaltung der vertraglichen Vereinbarungen über Dienstleistungen gegenüber den Kunden und im Warenhandel hat eine große wirtschaftliche Bedeutung. Der ausfallsichere Betrieb der IT-Systeme sowie die störungsfreie Kommunikation in den Geschäfts- und Leitungsprozessen ist ein grundlegendes Ziel der Informationssicherheit. Dazu zählen Maßnahmen zur schnellen und systematischen Reaktion auf Sicherheitsvorfälle ebenso, wie eine Notfallplanung zur Reaktion auf schwerwiegende Ereignisse mit gravierenden Folgen auf den Betrieb der IT-Umgebung.

Schutz der Daten

Im alltäglichen Geschäftsbetrieb der SHD ist die Verarbeitung von Daten ein essentieller Bestandteil der Prozesse. Ohne den Zugriff auf Auftrags-, Vertrags- oder kundenrelevante Daten ist ein Geschäftsbetrieb nicht möglich. Andererseits beinhalten die Daten Geschäftsgeheimnisse der SHD, deren Offenlegung einen beträchtlichen wirtschaftlichen Schaden verursachen kann.
Der Schutz von Daten von der Entstehung bis zur Entsorgung ist ein wichtiges Ziel der Informationssicherheit. Entsprechend dem Schutzbedarf (Klassifizierung) werden Maßnahmen umgesetzt, um Daten bei der Verarbeitung, dem Transport und der Speicherung in angemessenem Maße hinsichtlich der Vertraulichkeit, Verfügbarkeit und Integrität zu schützen.

Vermeidung von Risiken

Basierend auf der Bewertung von Risiken die beim Betrieb der Informationstechnologien und der Verarbeitung von Daten entstehen, werden Maßnahmen zur Vermeidung bzw. zur Reduktion[1] von Risiken umgesetzt. Zur Identifizierung von Informationssicherheitsrisiken wird eine Risikoanalyse durchgeführt, und entsprechend den Kriterien zur Risikoakzeptanz behandelt.

Sicherheitsbewusstsein der Mitarbeiter schulen

Die Unternehmensleitung unterstützt die Einhaltung und strebt eine systematische Verbesserung des Sicherheitsniveaus des gesamten Unternehmens an. Die Mitarbeiterinnen und Mitarbeiter der SHD unterstützen die Ziele zur Informationssicherheit und werden aufgefordert, den ISB bei diesbezüglich erkannten Schwachstellen unverzüglich zu informieren und bei Optimierungsanregungen den ISB

[1] Reduktion von Risiken: Absenkung auf ein tolerierbares Maß

oder ihre direkten Vorgesetzten zu kontaktieren. Um das Bewusstsein der Mitarbeiter für die Belange der Informationssicherheit zu verbessern, werden Mitarbeiterschulungen bzw. Sensibilisierungsworkshops zu aktuellen Themen der Informationssicherheit durchgeführt.

Kontinuierliche Verbesserung der Informationssicherheit

Durch eine kontinuierliche Revision der Richtlinien und Maßnahmen und deren konsequente Einhaltung und Umsetzung wird das angestrebte Sicherheits- und Datenschutzniveau gewährleistet. Abweichungen werden unmittelbar mit dem Ziel analysiert, die Sicherheitssituation zu verbessern und ständig auf dem aktuellen Stand der Technik zu halten.