FORTSCHRITT DURCH LEICHTIGKEIT.

POLITYKA BEZPIECZEŃSTWA INFORMACJI

LEIBER GROUP GMBH & CO. KG
LEIBER POLAND GMBH Sp. z o.o. Oddział w Polsce

Spis treści

Historia zmian

Wersja	Data	Autor	Zmiany / uwagi
0.9	04.04.2025	Hartmut Grande	Projekt na podstawie ISO 27001:2022 / VDA-ISA 6.x
1.0	31.07.2025	Udo Faulhaber	Dostosowanie LEIBER Group
2.0	11.12.2025	Udo Faulhaber	Wytyczne dotyczące komunikacji, odpowiedzialność przy nowych projektach

Zarząd LEIBER Poland GmbH w 78576 Emmingen-Liptingen, zwany dalej **Organizacją**, przyjmuje niniejsze wytyczne dotyczące bezpieczeństwa informacji i ochrony danych, zwane dalej **wytycznymi dotyczącymi bezpieczeństwa informacji**. Stanowią one część koncepcji bezpieczeństwa informacji organizacji. Poprzez wytyczne dotyczące bezpieczeństwa informacji zarząd wyraźnie potwierdza swoją odpowiedzialność za bezpieczeństwo informacji. Wytyczne dotyczące bezpieczeństwa informacji są ściśle związane z ustanowieniem procesu zapewniającego bezpieczeństwo informacji (Informationssicherheits-Managementsystem, w skrócie z niemieckiego **ISMS**), który został wdrożony przez organizację.

1. Wstęp

Organizacja wykorzystuje i przetwarza wiele informacji, aby wypełniać swoje zadania i obowiązki wobec klientów, partnerów umownych, usługodawców, urzędów i innych osób trzecich. W tym celu przetwarza również informacje wrażliwe, które wymagają wysokiego poziomu ochrony i które należy szczególnie chronić przed utratą, manipulacją lub nieuprawnionym dostępem osób trzecich. Obejmują one dane osobowe, poufne dane klientów, a także wewnętrzne dane wymagające ochrony, pochodzące z działów rozwoju, konstrukcji, produkcji, finansów, sprzedaży i innych obszarów. Oprócz danych cyfrowych dotyczy to również wszystkich informacji drukowanych i ustnych.

Kluczowe znaczenie dla ochrony informacji ma funkcja Organizacji jako dostawcy dla branży motoryzacyjnej. Obejmuje to na przykład rysunki techniczne na wczesnym etapie rozwoju służące do tworzenia wzorów i ofert. Ponadto istnieje duże zapotrzebowanie na ochronę klientów z innych branż, którzy mają odpowiednie wymagania w zakresie bezpieczeństwa informacji.

Należy również zapewnić niezawodną i stałą dostępność infrastruktury produkcyjnej i komunikacyjnej między Organizacją a klientami. Bezpieczeństwo informacji i technologii informatycznych (IT), w tym sterowania maszynami i urządzeniami (OT), odgrywa zatem kluczową rolę w realizacji zadań Organizacji.

Niniejsze wytyczne stanowią część koncepcji bezpieczeństwa informacji Organizacji i mają na celu przedstawienie strategii bezpieczeństwa oraz Organizacji bezpieczeństwa w przejrzystej i spójnej formie. Koncepcja bezpieczeństwa informacji zawiera dalsze szczegóły, w szczególności ramowe wytyczne dotyczące IT oraz drugorzędne wytyczne dotyczące IT, a także środki techniczne i organizacyjne służące osiągnięciu niezbędnego bezpieczeństwa informacji.

2. Zakres obowiązywania

Niniejsze wytyczne dotyczą firmy LEIBER Group GmbH & Co. KG (Emmingen-Liptingen) oraz LEIBER Poland GmbH z siedzibą w Rudolf-Diesel-Str. 1-3 w 78576 Emmingen, działającej na terytorium Rzeczypospolitej Polskiej poprzez LEIBER Poland GmbH Sp. z o. o. Oddział w Polsce, w tym wszystkich pracowników, kadry kierowniczej i partnerów zewnętrznych w odpowiednim obszarze odpowiedzialności.

Niniejsze wytyczne są wiążące dla wszystkich pracowników, dostawców i partnerów zewnętrznych, którzy mają dostęp do systemów informatycznych lub informacji wymagających ochrony w ramach Organizacji. W tym celu niniejsze wytyczne mogą być przekazywane stronom trzecim, również w wyrywkowej formie. O ile nie określono inaczej, głównymi osobami kontaktowymi w ramach Organizacji odpowiedzialnymi za komunikację z konkretną stroną trzecią są również osoby odpowiedzialne za przekazywanie niniejszych wytycznych, również w przypadku zmian.

3. Cele bezpieczeństwa

W Organizacji ochrona danych osobowych i bezpieczeństwo informacji mają najwyższy priorytet. Bezpieczeństwo informacji obejmuje nie tylko bezpieczeństwo systemów informatycznych i przechowywanych w nich danych, ale także bezpieczeństwo informacji nieprzetwarzanych elektronicznie.

Bezpieczeństwo informacji jest kluczowym czynnikiem zapewniającym długoterminową konkurencyjność. Do priorytetowych celów bezpieczeństwa informacji należy zatem spełnienie wymogów prawnych i umów zawartych z klientami, zapewnienie zdolności dostawczej, zabezpieczenie innowacji, a tym samym zachowanie konkurencyjności.

W związku z tym podczas planowania i wdrażania procesów biznesowych Organizacja zapewnia bezpieczeństwo informacji we wszystkich procesach i strukturach. Należy przy tym uwzględnić centralne plany i wytyczne pełnomocnika ds. bezpieczeństwa informacji, zespołu ISMS oraz centralnego działu IT. Bezpieczeństwo informacji jest zapewnione, gdy poufność, dostępność i integralność danych w systemach przetwarzających i przechowujących informacje są zabezpieczone. Służy ono ochronie przed zagrożeniami, zapobieganiu szkodom i minimalizowaniu wszystkich przewidywalnych ryzyk.

- **Poufność** oznacza, że dostęp do informacji mają wyłącznie uprawnione osoby i aplikacje.
- **Dostępność** znaczy, że dostęp do informacji i aplikacji jest możliwy w każdej chwili, gdy istnieje taka potrzeba.
- **Integralność** danych oznacza, że zapewniona jest trwałość procesów istotnych dla działalności oraz poprawność i kompletność danych

Ponadto wszyscy pracownicy we wszystkich lokalizacjach Organizacji są zobowiązani do przestrzegania lokalnych celów bezpieczeństwa. Konkretne środki bezpieczeństwa powinny być proporcjonalne pod względem ekonomicznym do potrzeb ochrony przetwarzanych informacji i wymaganej wydajności pracy pracowników. W tym celu w ramach ISMS regularnie i w zależności od sytuacji są identyfikowane i oceniane ryzyka związane z bezpieczeństwem informacji, a także podejmowane są odpowiednie środki zaradcze.

Wszyscy współpracownicy, wszystkie spółki powiązane, zarząd i wszyscy usługodawcy Organizacji są świadomi swojej odpowiedzialności za bezpieczeństwo informacji, w szczególności informacji w zakresie ich odpowiedzialności, i są zobowiązani do przestrzegania i wspierania wytycznych dotyczących bezpieczeństwa informacji.

Organizacja dokumentuje szczegółowy przegląd określonych celów w zakresie bezpieczeństwa informacji i ochrony danych w oddzielnym „wykazie wymagań dotyczących ISMS". Zawiera on cele prawne, umowne oraz własne cele bezpieczeństwa i w razie potrzeby jest dostosowywany i rozszerzany.

4. Organizacja bezpieczeństwa

Za bezpieczeństwo informacji w Organizacji odpowiada zarząd. Zarząd jest w szczególności odpowiedzialne za

- stworzenie ram organizacyjnych zapewniających trwałe bezpieczeństwo informacji,
- zdefiniowanie i ustalenie niezbędnych obowiązków i uprawnień,
- wprowadzenie systemu zarządzania bezpieczeństwem informacji i koncepcji bezpieczeństwa IT, w skrócie ISMS,
- zapewnienie, że wymagania ISMS zostaną włączone do procesów biznesowych,
- wdrożenie uzgodnionych środków bezpieczeństwa, w tym zapewnienie niezbędnych zasobów i kompetencji,
- wystarczająca i odpowiednia dokumentacja infrastruktury informatycznej oraz wszystkich środków bezpieczeństwa i działań zabezpieczających,
- wspieranie ciągłego doskonalenia ISMS.

W celu osiągnięcia celów związanych z bezpieczeństwem informacji wyznaczono inspektora ds. bezpieczeństwa informacji (z niemieckiego Informations-Sichierheitsbeauftragte, w skrócie **ISB**), który podlega bezpośrednio zarządowi. ISB doradza zarządowi we wszystkich kwestiach związanych z planowaniem i wdrażaniem bezpieczeństwa informacji w Organizacji. W ramach pełnionej funkcji regularnie składa zarządowi raporty dotyczące stanu bezpieczeństwa Organizacji, a w razie potrzeby informuje bezpośrednio zarząd o incydentach związanych z bezpieczeństwem. Mianowanie ISB jest potwierdzane na piśmie w oddzielnym akcie mianowania i zgłaszane przez zarząd w zakresie obowiązywania niniejszych wytycznych.

Zarząd kieruje Organizacją bezpieczeństwa informacji w zakresie obowiązywania niniejszych wytycznych i stale ją rozwija. Wyznacza osoby odpowiedzialne i określa ich obowiązki.

W miarę możliwości ISB należy włączać na wczesnym etapie do projektów, które wymagają wprowadzenia nowego oprogramowania i sprzętu informatycznego, a w wyniku tego generują lub przetwarzają informacje poufne lub wymagające ochrony, aby już na etapie planowania uwzględnić aspekty związane z bezpieczeństwem. Odpowiedzialny kierownik projektu jest zobowiązany do poinformowania ISB w odpowiednim czasie o takich projektach.

W przypadku danych osobowych to samo dotyczy inspektora ochrony danych (IOD) Organizacji. W miarę możliwości należy go włączyć w takie projekty na wczesnym etapie, aby zapewnić zgodne z prawem przetwarzanie danych osobowych i zminimalizować specyficzne ryzyko związane z automatycznym przetwarzaniem danych dla praw i wolności osób, których dane dotyczą. Organizacja zwraca przy tym uwagę na technologie przyjazne dla ochrony danych (Privacy by Design) oraz domyślne ustawienia programów i procedur przetwarzania danych przyjazne dla ochrony danych (Privacy by default).

Inspektor ochrony danych i inspektor bezpieczeństwa informacji są w razie potrzeby angażowani w audyty dotyczące bezpieczeństwa informacji. Inspektor ochrony danych pełni funkcję doradczą i jest osobą kontaktową dla zarządu, pracowników i przedstawicieli pracowników we wszystkich sprawach związanych z ochroną danych. Ponadto służy on zewnętrznym usługodawcom pomocą w kwestiach dotyczących ochrony danych.

Dział IT organizacji jest głównym adresatem kontaktowym dla pracowników i stron trzecich w kwestiach dotyczących bezpieczeństwa informacji i ochrony danych.

5. Środki bezpieczeństwa

Środki techniczne i organizacyjne są określane w Organizacji na podstawie oceny ryzyka w planie działań. Obejmują one również przepisy dotyczące pracowników i zewnętrznych usługodawców, które są dokumentowane w wytycznych dotyczących IT i ewentualnie w porozumieniach zakładowych. Te wytyczne dotyczące IT lub porozumienia zakładowe są przekazywane pracownikom Organizacji i zewnętrznym usługodawcom i są dla nich wiążące.

Obejmuje to następujące cele i środki techniczne oraz organizacyjne:

- Organizacja bezpieczeństwa informacji w zakresie obowiązywania niniejszych wytycznych,
- Zapewnienie bezpieczeństwa personelu przed rozpoczęciem, w trakcie trwania, po zakończeniu lub w przypadku zmiany stosunku zatrudnienia,
- Wartości i informacje Organizacji zostały zidentyfikowane, a odpowiednie zakresy odpowiedzialności za ich ochronę zostały określone zgodnie z ich znaczeniem,
- Dostęp do informacji i urządzeń przetwarzających informacje jest kontrolowany i ograniczony zgodnie z koncepcjami uprawnień,
- Zapewnienie bezpieczeństwa operacyjnego, w szczególności ochrona przed złośliwym oprogramowaniem, utratą danych, kradzieżą danych, integralność systemów informatycznych i danych oraz ich odzyskiwanie w przypadku awarii, w tym planowanie awaryjne i postępowanie w przypadku incydentów związanych z bezpieczeństwem informacji.

Aby wszyscy pracownicy Organizacji mogli prawidłowo i skutecznie wdrażać określone środki bezpieczeństwa, zespół ISMS udokumentuje dalsze wytyczne dotyczące postępowania z informacjami, systemami i aplikacjami informatycznymi oraz innymi istotnymi kwestiami, a także przekaże je użytkownikom w odpowiedniej formie.

6. Poprawa bezpieczeństwa

Niniejsze wytyczne dotyczące bezpieczeństwa informacji, wymagania dotyczące ISMS, wynikające z nich środki i wytyczne są regularnie sprawdzane pod kątem aktualności i skuteczności oraz odpowiednio dostosowywane. W celu zmierzenia skuteczności zespół ISMS będzie sprawdzał odpowiednie procesy poprzez audyty wewnętrzne. Zarząd wspiera ciągłe podnoszenie poziomu bezpieczeństwa. Wszyscy współpracownicy są zobowiązani do zgłaszania ewentualnych ulepszeń lub słabych punktów.

7. Postanowienia końcowe

Niniejsze wytyczne dotyczące bezpieczeństwa informacji wchodzą w życie z chwilą ich ogłoszenia. Aktualna wersja niniejszych wytycznych zostanie opublikowana w księdze jakości.

Naruszenia niniejszych wytycznych i innych obowiązujących dokumentów może skutkować konsekwencjami w zakresie prawa pracy i prawa cywilnego.

Ruda Śląska, dnia 17.12.2025 r.