POLITYKA

BEZPIECZEŃSTWA TELEINFORMATYCZNEGO

W KNORR-BREMSE SYSTEMY POJAZDÓW SZYNOWYCH SP. Z O.O.

Autor	Ilość stron	Data wprowadzenia
Krzysztof Podolski, RK RODO sp. z o.o.	7	2 lutego 2023 r.

Wersja	Zakres modyfikacji	Autor modyfikacji	Data wprowadzenia
	Aktualizacja w zakresie stosowania nowych technologii w zakresie bezpieczeństwa.	Jakub Stawarz	08 kwietnia 2025 r.

DO UŻYTKU WEWNĘTRZNEGO

CELE

Celem niniejszej polityki jest ustanowienie ram dla zasad bezpieczeństwa dla spółki Knorr-Bremse Systemy Pojazdów Szynowych Sp. z o.o. (zwana dalej KBS), które zapewniają adekwatny poziom ochrony przetwarzanych danych osobowych, a w szczególności:

1. Określenie zasad zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych.
2. Zapewnienie poufności, dostępności oraz integralności informacji oraz danych osobowych.
3. Zasady zarządzania ciągłością usług oraz kopii zapasowych.
4. Zasady ochrony danych w fazie projektowania systemów IT.

ZAKRES

Niniejszy dokument dotyczy wszystkich systemów informacyjnych, które przechowują, przetwarzają i przesyłają dane w KBS. Dokument adresowany jest do wszystkich pracowników KB, partnerów, dostawców usług IT i wszystkich podwykonawców. Zakres obejmuje zabezpieczenia dedykowane klientom; to są wszystkie zalecenia i wytyczne, których należy używać podczas

interakcji z nimi (generowanie haseł, zarządzanie wrażliwymi danymi, ochrona danych w fazie projektowania).

REALIZACJA

Dokument główny przedstawia cele polityki bezpieczeństwa IT, zakres jej stosowania, zakresy odpowiedzialności oraz procedury zmian.

Dokumenty składowe zawierają zasady i zalecenia dotyczące wymagań organizacyjnych sformułowanych, jako minimalne standardy bezpieczeństwa IT, które są adresowane do grup docelowych takich jak: użytkownicy, dostawcy, partnerzy.

Należy stosować zalecenia zawarte w odrębnych dokumentach, które uzupełniają zasady i wymogi o charakterze głównie organizacyjnym.

ZASADY SŁUŻĄCE BEZPIECZEŃSTWU I OCHRONY INFORMACJI

ZASADY DOTYCZĄCE UPRAWNIEŃ

1. Dostęp do systemu informatycznego Organizacji i może uzyskać wyłącznie osoba, zarejestrowana w tym systemie przez Administratora. Rejestracja polega na nadaniu identyfikatora i przydzieleniu pierwszego hasła, które podczas logowania musi zostać zmienione.
2. Dostęp do systemu informatycznego służącego do przetwarzana danych osobowych może uzyskać wyłącznie osoba posiadająca upoważnienie do przetwarzania danych osobowych nadane przez Administratora Danych Osobowych, zwany dalej „ADO", która podpisała oświadczenie o zachowaniu poufności.
3. Nadanie i zmiana uprawnienia do dostępu do systemu informatycznego następuje na podstawie wniosków elektronicznych (realizowanych poprzez wewnętrzny system intranet) i akceptowanych zgodnie z hierarchią organizacji.
4. Powyższy zapis stosuje się do nowozatrudnionych pracowników jak i innych osób stale współpracujących, a także w przypadku zmiany przez pracownika komórki organizacyjnej lub merytorycznego zakresu obowiązków. Zmiana obowiązków pracownika powoduje utratę dotychczasowych uprawnień i dostępów do systemu informatycznego.
5. Uprawnienia i dostępy do systemu teleinformatycznego ustają z chwilą zakończenia świadczenia pracy na rzecz Organizacji, powodując wyrejestrowanie użytkownika z systemu informatycznego, co jest równoznaczne z zablokowaniem dostępów do wszelkich systemów informatycznych w Organizacji.
6. Komórka kadrowa, blokuje użytkownika oraz informuje niezwłocznie (nie później niż w ciągu 2 godzin), w formie wiadomości elektronicznej, Administratora IT, o rozwiązaniu lub wygaśnięciu stosunku pracy użytkownika. Administrator dokonuje blokady dostępów nie później niż w ciągu dwóch godzin do momentu uzyskania zgłoszenia. Dział IT wykonuje regularny przegląd uprawnień do systemów informatycznych identyfikując nieprawidłowości i wskazując sposób na ich usunięcie.

7. W ramach nadawania uprawnień do danych przetwarzanych w systemach IT KBS należy stosować zasadę „minimalnych uprawnień", to znaczy przydzielać minimalne uprawnienia, które są konieczne do wykonywania pracy na danym stanowisku. Pracując na stacji roboczej każdy pracownik powinien posiadać tylko takie uprawnienia, jakie są wymagane do realizacji jego obowiązków.
8. Uprawnienia do katalogów współdzielonych przydzielane użytkownikom lub grupie do obiektu lub właściwości obiektu są nadawane za pośrednictwem Acitve Directory (lub panelu usług Microsoft 365). Zgodnie z powyższą zasadą, użytkownik otrzymuje wyłącznie potrzebny mu do pracy dostęp do katalogów współdzielonych.

ZASADA WIELWARSTWOWYCH ZABEZPIECZEŃ

Wszystkie systemy informatyczne w KBS przetwarzające dane osobowe muszą być chronione równolegle na wielu poziomach m.in. poprzez adekwatne metody uwierzytelnienia użytkowników, stosowanie oprogramowania antywirusowego, systemów typu firewall, odpowiednią konfigurację systemu aktualizacji systemu operacyjnego oraz realizację kopii bezpieczeństwa.

ZASADA OGRANICZENIA DOSTĘPU

Domyślnymi uprawnieniami w systemach IT powinno być zabronienie dostępu. Dopiero w przypadku zaistnienia potrzeby, administrator IT przyznaje stosowne uprawnienia. Domyślnie dostęp do systemów przetwarzających dane osobowe jest zabroniony. Stosowny dostęp zostaje przyznany osobie, której zajmowane stanowisko wiąże się z koniecznością pracy w tego typu systemie.

Zasady zabezpieczenia stacji roboczych

Stosowane zabezpieczenia stacji roboczych:

1. Wszystkie stacje robocze przetwarzające dane osobowe podłączone są do domeny firmowej. Taka konfiguracja wymusza automatyczną implementację jednolitych zabezpieczeń (polityka haseł, blokady zewnętrznych nośników, szyfrowanie, etc.).
2. Stacje robocze posiadają włączoną blokadę zapisu zewnętrznych nośników za pośrednictwem GPO i nie zezwalają na podłączenie urządzeń służących do magazynowania danych jak: pendrive, napęd optyczny usb, karty pamięci, przenośne stacje cd/dvd, smartphone).
3. W celu zabezpieczenia danych na dysku twardym każda stacja robocza jest szyfrowana (mechanizm Bitlocker). W szczególnych przypadkach szyfrowanie może być czasowo wyłączone, wyłącznie na zatwierdzony wniosek użytkownika. Wyjątki takie podlegają cyklicznemu przeglądowi.
4. Wymuszony wygaszacz ekranu, który po automatycznej aktywacji blokuje dostęp do stacji roboczej.
5. Wymuszona automatyczna instalacja aktualizacji systemu operacyjnego.

6. Zdalny dostęp do zasobów organizacji odbywa się z wykorzystaniem kanału szyfrowanego VPN, uwierzytelniania Active Directory oraz klucza bezpieczeństwa Yubico. Zgodnie z regulaminem pracy każde uruchomienie laptopa poza siecią biurową, wymaga uwierzytelnienia kluczem Yubico i pracy sieci VPN.
7. Utwardzenie domyślnych ustawień systemowych, m.in. brak uprawnień lokalnego administratora, szyfrowanie dysku, automatyczne aktualizacje, włączony firewall, etc.
8. Użytkownicy stacji roboczych pracują na profilach o ograniczonych uprawnieniach, uniemożliwiających instalację oprogramowania ingerującego w system operacyjny.

ZASADY DOTYCZĄCE HASEŁ

Dostęp do systemów informatycznych w Organizacji jest zabezpieczony przy pomocy haseł. Rozpoczęcie pracy przez nowego pracownika odbywa się przy użyciu hasła startowego (przekazanego przez dział IT), które automatycznie musi zostać zmienione na hasło własne użytkownika. Organizacja stosuje następującą politykę dotyczącą haseł:

1. prawidłowe hasło składa się z co najmniej 12 znaków (duże i małe litery, cyfry lub znaków specjalnych takich, jak np.: !@#$%), nie zawiera znaku spacji i znaków dialektycznych (np. polskich liter). Powyższe wymogi wymuszone są przez system rejestrowania hasła, który uniemożliwia pominięcie w/w reguł;
2. nie mogą przybierać prostych form, np. 123456789, Krzysztof1, Styczen2022, nawiązywać wprost do nazwy organizacji, imienia, nazwiska czy zajmowanego stanowiska, etc;
3. po 10 nieudanych próbach konto zostaje zablokowane, a jego odblokowanie wymaga użycia Bitlocker Recovery Key.
4. W przypadku przetwarzania danych osobowych, użytkownik ma obowiązek zmiany hasła nie rzadziej niż raz na 90 dni, o ile system informatyczny nie wymusi takiej zmiany. Kolejne hasła nie mogą się powtarzać. W przypadku gdy system teleinformatyczny nie wymusza zmiany hasła automatycznie użytkownik jest zobowiązany do dokonania takiej zamiany z sposób manualny;
5. w celu zarządzania dużą ilością haseł stosuje się menadżera haseł;
6. dla kont w usłudze Microsoft 365 włączone jest dwuskładnikowe logowanie, a hasła zmienia się raz na rok.

Dodatkowo użytkownicy zobowiązani są do stosowania w praktyce następujących zasad:

1. podejrzenie lub stwierdzenie, że z hasłem mogły zapoznać się osoby nieuprawnione powoduje konieczność niezwłocznej jego zmiany;
2. zabronione jest zapisywanie haseł przez użytkowników oraz ich przechowywanie w miejscach łatwo dostępnych;
3. zabronione jest powierzanie haseł osobom trzecim, w tym współpracownikom oraz przełożonym;

4. zabronione jest stosowanie ustawień, które umożliwiają automatyczne zapamiętywanie haseł;
5. nieprzechowywanie danych w miejscach publicznych (np. zapisywanie haseł dostępowych w łatwo dostępnych miejscach);
6. ochrona danych dostępowych przed kradzieżą przez osoby trzecie;
7. zabrania się przenoszenia niezabezpieczonych danych poufnych poza teren Organizacji. W szczególności zabrania się przenoszenia danych poufnych na nośnikach elektronicznych (np.: pendrive, nośniki CD) poza teren Organizacji.

ZASADA PRZETWARZANIA DANYCH NA KOMPUTERACH SŁUŻBOWYCH

Zabrania się korzystania z firmowej infrastruktury IT w celach prywatnych. Organizacja nie dopuszcza do pracy komputerów prywatnych pracowników.

W wyjątkowych sytuacjach, czasowo umożliwiany jest dostęp do ograniczonych zasobów firmy przez system Citrix z uwierzytelnianiem 3 składnikowym.

ZASADA UTRZYMYWANIA DOKUMENTACJI

Organizacja prowadzi dokumentację w zakresie:

1. sieci IT (stosowane urządzenia, zabezpieczenia, topologia, itp.)
2. rejestracji naruszeń / incydentów bezpieczeństwa,
3. dostępów do zbiorów danych / systemów i sprzętu udzielonego pracownikom,
4. procedury zachowania ciągłości działania w przypadku wystąpienia zdarzeń krytycznych.

ZASADA DOMYŚLNEJ OCHRONY DANYCH

1. Administrator Danych Osobowych zapewnia, aby narzędzia techniczne służące do

wsparcia procesu przetwarzania danych osobowych przechowywały wyłącznie niezbędną ilość danych, konieczną do osiągnięcia celu przewarzania danych. Obowiązek ten odnosi się do:

1. ilości gromadzonych danych osobowych;
2. zakresu ich przetwarzania i okresu przechowywania;
3. dostępności tylko dla osób uprawnionych.

2. Przy wdrożeniu narzędzi technicznych Administrator Danych Osobowych powinien uwzględnić następujące elementy:

1. aktualny poziom wiedzy technicznej oraz koszt implementacji;
2. zakres i cel przetwarzania danych osobowych;

3. analiza ryzyka związana z możliwością ujawnienia danych osobom nieuprawnionym.

3. Każdorazowo przed wdrożeniem nowego narzędzia informatycznego służącego do przetwarzania danych osobowych konieczne jest potwierdzenie przeprowadzenia analizy uwzględnienia ochrony danych w fazie projektowania oraz domyślnej ochrony danych.

4. Za przeprowadzenie analizy, o której mowa w ust. 3 odpowiada Inspektor Ochrony Danych, wspierany w tym zakresie przez Administratora IT.

MONITORING BEZPIECZEŃSTWA

W celu zapewnienia ochrony informacji Administrator IT ma prawo monitorować aktywność użytkowników w ramach wykorzystywanych systemów informatycznych w celu zapewniania bezpieczeństwa, ciągłości przetwarzania danych Organizacji oraz zgodności z przepisami prawa. W przypadku rażących naruszeń zapisów niniejszej polityki oraz innych, przepisów prawa, Administratora IT powiadamia o nadużyciach Zarząd Organizacji. Elementy monitoringu to między innymi:

1. analiza oprogramowania wykorzystanego na stacjach roboczych,
2. analiza stacji roboczych pod względem wykorzystania nielegalnego oprogramowania/plików multimedialnych oraz innych elementów naruszających Prawo Autorskie,
3. analiza odwiedzanych stron WWW,
4. analiza godzin pracy na stanowiskach komputerowych,
5. analiza dostępów (autoryzowanych oraz nieautoryzowanych) do systemów IT będących w posiadaniu Organizacji,
6. analiza ruchu sieciowego pod względem komunikacji, szkodliwej dla bezpieczeństwa danych Organizacji.

Monitoring bezpieczeństwa odbywa się z zachowaniem obowiązującego prawa.

BEZPIECZEŃSTWO INFRASTRUKTURY SIECIOWEJ

1. Lokalna sieć komputerowa Organizacji oddzielona jest od sieci publicznej zaporą sieciową. W ramach zapory sieciowej zdefiniowano reguły zabraniające inicjacji połączeń dostępowych do sieci lokalnej z sieci publicznej. Działanie zapory sieciowej oddzielającej sieć lokalną Organizacji od sieci publicznej jest na bieżąco monitorowane.
2. Dla kluczowych w funkcjonowaniu Organizacji systemów teleinformatycznych opracowywane są szczegółowe procedury awaryjne. Przez kluczowe dla funkcjonowania Organizacji systemy teleinformatyczne rozumie się systemy, których ewentualna awaria powoduje niemożność terminowego wywiązania się Organizacji ze zobowiązań w stosunku do podmiotów zewnętrznych.
3. Systemy IT przechowujące dane poufne (np. dane osobowe) są odpowiednio zabezpieczone w zależności od ich zastosowanie oraz zidentyfikowanych ryzyk.

Stosowane zabezpieczenia mają na celu dbanie o poufność, integralność, dostępność oraz rozliczalność danych przetwarzanych w systemach

4. W celu zwiększenia bezpieczeństwa stosuje się segmentację sieci (oddzielenie serwerów dostępnych publicznie od sieci lokalnej lub segmentację wewnątrz sieci lokalnej).

BEZPIECZEŃSTWO FIZYCZNE

1. W celu zapewnienia wysokich standardów ochrony danych osobowych Organizacja stosuje elektroniczne systemy zabezpieczeń. Do takich systemów zalicza się systemy sygnalizacji włamania i napadu (SSWiN), systemy kontroli dostępu (SKD), systemy telewizji dozorowej (CCTV).
2. Przeglądy okresowe systemów SSWiN, SKD i CCTV wykonywane są w ramach rocznego przeglądu stanu funkcjonowania systemu ochrony danych osobowych.
3. Z uwagi na konieczność świadczenia wysokich standardów ochrony danych osobowych Organizacja archiwizuje nagrania z kamer CCTV przez 14 dni.

KOPIE ZAPASOWE

Wszelkie kopie zapasowe realizowane są za pomocą dedykowanego systemu, który wykonuje kopie kluczowych systemów IT (poprzez zastosowanie m.in tzw. migawek oraz pełnych kopii maszyn wirtualnych). Dodatkowo w systemie przechowywane są również punkty odzyskiwania, zasady tworzenia kopii zapasowych, harmonogramy, czas retencji kopii zapasowych. Z racji na publiczny charakter dokumentu, dokładny opis znajduje się w dokumentacji dotyczącej konfiguracji systemu kopii zapasowych, który jest do wglądu za zgodą Administratora IT.

NARUSZENIE BEZPIECZEŃSTWA

1. Wszelkie podejrzenia naruszenia bezpieczeństwa danych w Organizacji są zgłaszane za pomocą prowadzonego Rejestru incydentów i naruszeń bezpieczeństwa IT.
2. Każdy incydent jest odnotowywany w stosownej bazie danych, a Zarząd Organizacji podejmuje stosowne kroki zaradcze.

WERYFIKACJA PRZESTRZEGANIA POLITYKI BEZPIECZEŃSTWA

1. Zarząd okresowo wykonuje wewnętrzny lub zewnętrzny audyt bezpieczeństwa mający na celu wykrycie ewentualnych uchybień w realizacji założeń polityki bezpieczeństwa.
2. Administrator IT dokonuje cyklicznego przeglądu Polityki w zakresie aktualności postanowień zawartych w jej treści nie rzadziej niż raz w roku i proponuje Zarządowi wprowadzenie niezbędnych aktualizacji.
3. Niniejsza Polityka obowiązuje od dnia 08 kwietnia 2025 r. zastępując dotychczasowe regulacje dotyczące ochrony bezpieczeństwa teleinformatycznego.

4. Wszelkie zmiany Polityki wymagają zachowania formy pisemnej.

W imieniu Organizacji:

Prezes Zarządu

Jacek Biłas

Dyrektor ds. Personalnych

Łukasz Zalibowski