BOSMAL	Instytut Badań i Rozwoju Motoryzacji BOSMAL Sp. z o.o. ul. Sarni Stok 93, 43-300 Bielsko-Biała		
POLITYKA			
Numer: **BOSMAL/A-12-03/02**		Data wydania: **06.09.2024**	
Tytuł: Bezpieczeństwo informacji i cyberbezpieczeństwo		Stron: **9**	Załączników: -

Spis treści

DOTYCZY (ROZDZIELNIK):

ZJ	ZT											
DN	NC	NA	NE	NK	NR	NZ	NL	NI	NB	NH	NP	IOD
DB	BD	BH	BM	BS	BW	BP	BE	BR				
NSZZ „S”				ZZ PRAC.			-					

Tylko do użytku wewnątrz BOSMAL

Egzemplarz papierowy: ZJ

Opracował:	Sprawdził:	Zatwierdził:
dr inż. Joanna Faber (Podpis)	dr inż. Arkadiusz Stojecki (Data, Podpis)	dr inż. Piotr Świątek (Data, Podpis)

1. CEL

Zebranie i przedstawienie zasad organizacyjnych i technicznych w zakresie nadzoru i zarządzania bezpieczeństwem informacji, w tym ochrony danych osobowych w BOSMAL, w celu zapewnienia poufności, dostępności i integralności przetwarzanych informacji.

2. ZAKRES STOSOWANIA

Polityka określa podstawowe zasady zarządzania bezpieczeństwem informacji i ma zastosowanie we wszystkich komórkach organizacyjnych BOSMAL.

3. ZAKRES OBOWIĄZYWANIA

Polityka obowiązuje wszystkie komórki organizacyjne oraz wszystkich pracowników BOSMAL.

4. ROZŁOŻENIE ODPOWIEDZIALNOŚCI

Opisano w punkcie 6.2

5. DEFINICJE I ZASTOSOWANE SKRÓTY

5.1. Definicje

Definicja	Opis
Bezpieczeństwo informacji	rozumiane jest przez: – zachowanie poufności, integralności i dostępności informacji, – ograniczenie dostępu do pomieszczeń BOSMAL, – właściwego zachowania w zakresie bezpieczeństwa informacji i cyberbezpieczeństwa (cyberhigiena)
Cyberbezpieczeństwo	ochrona systemu informatycznego przed cyberzagrożeniami
TISAX	ang. *Trusted Information Security Assesment Exchange*, standard dotyczący bezpieczeństwa informacji w branży motoryzacyjnej
System informatyczny	zgodnie z BOSMAL/P-4-12, zbiór urządzeń komputerowych wraz ze specjalistycznym oprogramowaniem, realizującym przetwarzanie danych i informacji. System informatyczny BOSMAL może składać się z mniejszych podsystemów
Użytkownik	zgodnie z BOSMAL/P-4-12, każdy pracownik posiadający dostęp do systemu informatycznego BOSMAL za pomocą aktywnego loginu i hasła
Poufność	dostęp do informacji mają tylko zainteresowane i upoważnione osoby
Integralność	zgodnie z BOSMAL/P-4-12, nienaruszalność, spójność i kompletność. Zapewnienie, że zmiany nie są wprowadzane w sposób nieautoryzowany oraz, że nie nastąpiło zniszczenie (informacji, zasobów aktywów itp.)

Definicja	Opis
Rozliczalność	zgodnie z BOSMAL/P-4-12, przypisanie właściciela aktywowi, zasobowi itp.
Dostępność	zgodnie z BOSMAL/P-1-06, właściwość określająca, że informacja jest możliwa do wykorzystania na żądanie, w założonym czasie przez osobę upoważnioną do dostępu do tej informacji
Aktywa informacyjne	zgodnie z BOSMAL/P-1-06, wszystkie zasoby informacyjne (informacje), które stanowią wartość dla BOSMAL
Aktywa wspierające	zgodnie z BOSMAL/P-1-06, aktywa służące przetwarzaniu aktywów informacyjnych
Prototyp	to pierwszy egzemplarz kontrolny (lub jeden z pierwszych egzemplarzy) wyrobu nowego, nie wprowadzonego dotąd na rynek. Prototyp stanowi przedmiot prób i badań, których cel wiąże się z przeznaczeniem wyrobu i ze sprawdzeniem dotyczącej tego wyrobu dokumentacji

5.2. Zastosowane skróty

Skrót	Opis
BOSMAL, Instytut	Instytut Badań i Rozwoju Motoryzacji BOSMAL Spółka z ograniczoną odpowiedzialnością
BI	Bezpieczeństwo Informacji
SZBI	System Zarządzania Bezpieczeństwem Informacji
ASI	Administrator Systemów Informatycznych
ADO	Administrator Ochrony Danych
IOD	Inspektor Ochrony Danych
VDA ISA	ang. *VDA Information Security*, arkusz oceny TISAX

Nazwy komórek organizacyjnych – zgodnie z aktualnym regulaminem organizacyjnym BOSMAL/R-0-03.

6. SYSTEM ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI

6.1. Polityka SZBI i deklaracja Zarządu BOSMAL

W Instytucie Badań i Rozwoju Motoryzacji BOSMAL Sp. z o.o. wprowadza się System Zarządzania Bezpieczeństwem Informacji w celu spełnienia wymogów stron zainteresowanych oraz wymogów prawnych dotyczących bezpieczeństwa informacji, cyberbezpieczeństwa i ochrony danych. Zarząd Instytutu stale podejmuje działania mające na celu ochronę informacji, wdrożenie i stosowanie zasad bezpiecznej pracy z informacją i aktywami, właściwe reagowanie na zdarzenia i incydenty, identyfikację ryzyka, zapewnienie ciągłości działania Instytutu oraz zapewnienie odpowiedniej wiedzy i świadomości personelu. W tym celu SZBI objęto wszystkie komórki organizacyjne BOSMAL, a wymagania w zakresie bezpieczeństwa informacji zostały zintegrowane z pozostałymi systemami zarządzania wdrożonymi w BOSMAL.

Polityka SZBI jest zakomunikowana w BOSMAL i jest spójna ze strategicznymi kierunkami działalności Instytutu oraz zintegrowana z procesami biznesowymi. Polityka SZBI jest również dostępna dla stron zainteresowanych poprzez publikację na stronie internetowej BOSMAL (www.bosmal.com.pl).

Kierownictwo BOSMAL wykazuje zaangażowanie i deklaruje pełne wsparcie dla podejmowanych działań w zakresie utrzymywania, rozwijania i doskonalenia SZBI oraz zapewnia niezbędne środki i zasoby do realizacji celów, w tym wdrożenie i utrzymanie niezbędnych zabezpieczeń organizacyjnych, fizycznych, technicznych i personalnych.

W celu zapewnienia skutecznego funkcjonowania SZBI ustalone są określone zasady postępowania, zakomunikowane pracownikom oraz prowadzone są okresowe szkolenia i uświadamianie pracowników w celu podkreślenia ich roli w systemach informatycznych. Podejmowane działania są planowane, przeglądane i doskonalone.

6.2. Role, odpowiedzialności i uprawnienia

W celu skutecznego funkcjonowania SZBI Zarząd Instytutu wyznaczył:

- swojego przedstawiciela do nadzorowania, rozwijania i doskonalenia SZBI, koordynowania działań doskonalących i oceny skuteczności tych działań (Pełnomocnik Zarządu ds. Systemów Zarządzania),
- osobę odpowiedzialną za zapewnienie bezpieczeństwa informacji i cyberbezpieczeństwa oraz za techniczne utrzymanie systemu informatycznego (Administrator Systemów Informatycznych),
- przedstawiciela nadzorującego zapewnienie ochrony danych (Inspektor Ochrony Danych).

Wyznaczone osoby raportują bezpośrednio do Zarządu na temat skuteczności funkcjonowania SZBI oraz komunikują wymagania i zasady postępowania w Instytucie.

Za skuteczność wdrożonych działań, właściwe postępowanie i zabezpieczenie informacji i danych odpowiadają kierownicy komórek organizacyjnych, będący właścicielami informacji i aktywów w podległych im obszarach.

Wszyscy pracownicy Instytutu są zobowiązani do stosowania ustalonych i opisanych zasad postępowania w SZBI oraz właściwego postępowania z informacjami i aktywami i ich ochronę.

Każdy pracownik jest zobowiązany do zgłaszania zdarzeń wpływających na bezpieczeństwo informacji lub incydentów do bezpośredniego przełożonego oraz zgodnie z pkt. 7.9.

Nowo przyjmowani pracownicy, praktykanci, stażyści są informowani o zasadach bezpieczeństwa informacji i ochrony danych w ramach instruktażu wstępnego.

Auditorzy wewnętrzni, przeszkoleni z zakresu bezpieczeństwa informacji, odpowiadają za skuteczną ocenę funkcjonowania SZBI oraz zgłaszanie ZJ nieprawidłowości i potencjałów doskonalenia.

6.3. Cele Systemu Zarządzania Bezpieczeństwem Informacji

Wdrożenie i utrzymywanie SZBI ma na celu:

- zapewnienie ochrony informacji oraz danych osobowych przed nieupoważnionym dostępem, utratą, wyciekiem lub nieautoryzowaną modyfikacją,
- zapewnienie poufności, dostępności i integralności informacji (atrybuty bezpieczeństwa informacji) oraz danych osobowych przetwarzanych w BOSMAL,
- ochronę przed negatywnymi skutkami ataków, incydentów i naruszeń,

– zapewnienie ciągłości działania BOSMAL, w szczególności w zakresie kluczowych aktywów informacyjnych,

– zapewnienie odpowiedniej wiedzy i świadomości użytkowników,

– opisanie i zapewnienie jednolitego sposobu postępowania w ramach systemu informatycznego oraz w przypadku zidentyfikowanych incydentów i zagrożeń.

6.4. Zakres SZBI

System Zarządzania Bezpieczeństwem Informacji w BOSMAL obejmuje wszystkie komórki organizacyjne BOSMAL oraz wszystkie funkcje i stanowiska. Wdrażając SZBI uwzględniono:

– wymagania normy ISO/IEC 27001 oraz standardu TISAX (aktualny arkusz oceny VDA ISA),

– wymagania prawne,

– wymagania stron zainteresowanych i kontekst organizacji (aktualny wykaz znajduje się u Pełnomocnika Zarządu ds. Systemów Zarządzania).

Ochronie BI podlegają przetwarzane w BOSMAL aktywa i informacje (w tym dane osobowe), powstające w BOSMAL, jak i przekazane przez klientów BOSMAL na potrzeby realizacji na ich rzecz prac (wyroby lub usługi).

7. ZASADY POSTĘPOWANIA

7.1. Zasady ogólne

Wdrożone zasady postępowania, zabezpieczenia i rozwiązania zapewniają zachowanie trzech podstawowych atrybutów bezpieczeństwa informacji: poufności, dostępności i integralności.

W ramach SZBI zastosowanie mają następujące zasady:

1. **Zasada uprawnionego dostępu**: każdy pracownik posiada dostępy do zasobów tylko w zakresie koniecznym i zgodnie z nadanymi formalnie uprawnieniami.
2. **Zasada uprawnień koniecznych**: każdy pracownik posiada prawa dostępu do wyłącznie do tych informacji, które są konieczne do wykonywania powierzonych mu zadań.
3. **Zasada wiedzy koniecznej**: każdy pracownik posiada wiedzę o systemie, do którego ma dostęp, ograniczoną wyłącznie do zagadnień, które są konieczne do realizacji powierzonych mu zadań.
4. **Zasada potrzeby koniecznej**: prawa dostępu użytkownika wyłącznie do środków przetwarzania informacji (aktywów) koniecznych do wykonania obowiązków służbowych na rzecz BOSMAL i ograniczenie jego dostępu do pozostałych środków.
5. **Zasada świadomości zbiorowej**: wszyscy pracownicy są świadomi konieczności ochrony zasobów informacyjnych BOSMAL i aktywnie uczestniczą w tym procesie.
6. **Zasada indywidualnej odpowiedzialności**: za bezpieczeństwo poszczególnych elementów SZBI odpowiadają konkretne, zidentyfikowane osoby.
7. **Zasada obecności koniecznej**: prawo przebywania w określonych miejscach mają tylko osoby upoważnione.
8. **Zasada stałej gotowości**: system informatyczny i jego elementy pracują ciągle. Krytyczne elementy systemu informatycznego są ciągle aktualizowane w celu zachowania bezpieczeństwa informacji i ochrony danych.

9. **Zasada kompletności**: skuteczne zabezpieczenie jest możliwe tylko wtedy, gdy stosuje się podejście kompleksowe, uwzględniające wszystkie stopnie i elementy ogólnie pojętego procesu przetwarzania informacji.
10. **Zasada odpowiedniości**: używane mechanizmy muszą być adekwatne do sytuacji.

7.2. Dokumenty SZBI

System Zarządzania Bezpieczeństwem Informacji w BOSMAL jest opisany niniejszą polityką oraz Księgą Jakości Zintegrowanego Systemu Zarządzania. Szczegółowe informacje dotyczące postępowania w poszczególnych obszarach są opisane w stosownych procedurach i instrukcjach (pkt. 8 niniejszej polityki).

7.3. Klasyfikacja informacji i aktywów

Informacje w BOSMAL są klasyfikowane jako: publiczne (public), operacyjne (operational), poufne (confidential). Ustalono poziom ochrony informacji, aktywa wspierające informacje, właścicieli aktywów i informacji. Wszystkie informacje pozyskane od klientów i wytworzone na ich rzecz są traktowane jako poufne.

Sposób klasyfikacji i zasady postępowania z informacjami i aktywami oraz nadzór nad dokumentami i zapisami jest opisany w procedurze BOSMAL/P-1-06 „Zarządzanie udokumentowanymi informacjami".

7.4. Klasyfikacja projektów

Projekty realizowane w BOSMAL są podlegają normalnej lub wysokiej ochronie zgodnie z TISAX ('normal protection needs' oraz 'high protection needs').

7.5. System informatyczny

System informatyczny w BOSMAL jest nadzorowany w celu zapewnienia bezpieczeństwa informacji i ochrony danych, a działania są ujednolicone w ramach całego Instytutu. Szczegóły postępowania zawarto w procedurze BOSMAL/P-4-12 „Zarządzanie systemem informatycznym", w której opisano zasady postępowania w zakresie systemu informatycznego oraz kontroli dostępu w BOSMAL, w tym politykę haseł i uwierzytelnienia, zabezpieczenia sprzętu komputerowego, telefonów i nośników danych, nadawanie/odbieranie uprawnień, stosowane zabezpieczenia i bezpieczeństwo sieci, zarządzanie zmianami, nadzór nad oprogramowaniem i kopiami zapasowymi, zasady korzystania z poczty elektronicznej, podatności i zmiany, obowiązki użytkowników.

Postępowanie z danymi osobowymi jest opisane w procedurze BOSMAL/P-12-01 „Zarządzanie bezpieczeństwem przetwarzania danych osobowych".

7.6. Bezpieczeństwo fizyczne

Instytut został podzielony na cztery strefy dostępu: zieloną (ogólnego dostępu), żółtą (ograniczonego dostępu), czerwoną (zastrzeżonego dostępu), niebieską (najemców pomieszczeń). Dla stref wprowadzono oznaczenia graficzne oraz zdefiniowano minimalne zabezpieczenia, a dostępy do nich zostały ograniczone zgodnie z zasadą obecności koniecznej. Szczegóły zasad dostępu i stosowane zabezpieczenia techniczne obiektów i aktywów wspierających są opisane w polityce BOSMAL/A-12-03 „Bezpieczeństwo fizyczne".

7.7. Zasoby ludzkie i świadomość personelu

BOSMAL posiada politykę kadrową, której celem jest pozyskiwanie pracowników o najlepszych kwalifikacjach, doświadczeniu i umiejętnościach w celu realizacji celów i zadań na rzecz Instytutu. Zasady obowiązujące przy zatrudnianiu pracowników, niezbędne szkolenia i instruktaże wstępne i stanowiskowe są uregulowane w procedurze BOSMAL/P-2-02 „Zarządzanie personelem".

W celu stałego zwiększania świadomości personelu w zakresie BI i ich roli w utrzymaniu SZBI prowadzone są szkolenia wewnętrzne i rozmowy z pracownikami oraz przygotowywane są materiały informacyjne i szkoleniowe do samokształcenia.

7.8. Ryzyko i szanse

BOSMAL podejmuje działania mające na celu identyfikację ryzyka w bezpieczeństwie informacji. W tym celu dokonywana jest identyfikacja aktywów i zagrożeń, analiza zagrożeń i skutków zagrożeń oraz podatności, a na podstawie wyników analizy ryzyka określane są środki ograniczające ryzyko. Zidentyfikowane ryzyka są okresowo przeglądane i aktualizowane.

Sposób postępowania opisano w instrukcji BOSMAL/I-1-07 „Zarządzanie ryzykiem", w tym postępowanie z ryzykiem w procesach, związanym z realizacją zlecenia, ryzykiem w bezpieczeństwie informacji. Dodatkowo w instrukcji zdefiniowano sposób określania kontekstu organizacji i stron zainteresowanych.

7.9. Incydenty, zdarzenia i niezgodności

W BOSMAL ustalono sposób i kanały zgłaszania zdarzeń i incydentów dotyczących bezpieczeństwa informacji, cyberbezpieczeństwa i ochrony danych osobowych. Szczegóły postępowania opisano w procedurze BOSMAL/P-12-02 „Zarządzanie incydentami bezpieczeństwa informacji". Każdy pracownik BOSMAL oraz inna strona zainteresowana ma obowiązek zgłoszenia zidentyfikowanej lub podejrzenia możliwości wystąpienia sytuacji niebezpiecznej/niepożądanej w szeroko rozumianym bezpieczeństwie informacji:

- zgłoszenia dotyczące bezpieczeństwa informacji w zakresie cyberbezpieczeństwa systemów informatycznych lub kontroli dostępu należy kierować do ASI BOSMAL,
- zgłoszenia dotyczące danych osobowych należy kierować do ADO i/lub IOD BOSMAL,
- zgłoszenia dotyczące fizycznych dostępów, infrastruktury, mediów należy kierować do kierownika Działu BR.,
- zgłoszenia dotyczące dostawców należy kierować do kierownika Działu Zakupów,
- zgłoszenia dotyczące systemów zarządzania, w tym SZBI oraz niezgodności w zakresie BI należy kierować do Pełnomocnika Zarządu ds. Systemów Zarządzania.

Zgłoszenia podlegają analizie i w uzasadnionych przypadkach podjęciu działań korygujących lub doskonalących (zgodnie z BOSMAL/P-1-03). W przypadku stwierdzenia niezgodności w jakimkolwiek obszarze, wystawiana jest karta niezgodności, a w przypadkach tego wymagających przeprowadzany jest audit wewnętrzny w danym obszarze. Incydenty i niezgodności w SZBI są raportowane Zarządowi BOSMAL.

Świadomie lub celowe nie stosowanie się do ustalonych zasad SZBI lub naruszanie BI/ochrony danych przez personel stanowi wykroczenie względem dyscypliny pracy i podlega karom za naruszenie porządku i dyscypliny pracy, zgodnie z BOSMAL/R-0-04 „Regulamin pracy".

7.10. Ciągłość działania BOSMAL

Zapewnienie ciągłości działania BOSMAL i odporności na wypadek sytuacji kryzysowych jest kluczowe dla realizacji celów biznesowych Instytutu. Sposób postępowania opisano w procedurze BOSMAL/P-12-04 „Plany ciągłości działania", w której opisano praktyki i odpowiedzialności na wypadek wystąpienia sytuacji kryzysowej. W celu sprawnego przywrócenia działalności po sytuacji kryzysowej opracowane są plany ciągłości działania dla obszarów krytycznych, a aktualność planów i adekwatność ustalonych procedur jest sprawdzana podczas systematycznych testów.

7.11. Skuteczność i doskonalenie SZBI

Skuteczność wdrożonego systemu SZBI w BOSMAL jest oceniana podczas auditów wewnętrznych oraz w gronie najwyższego kierownictwa podczas przeglądu Systemów Zarządzania. Na podstawie danych wejściowych ustalane są zadania mające na celu doskonalenie SZBI.

7.12. Łańcuch dostaw i współpraca z dostawcami

Dostawcy usług informatycznych BOSMAL są objęci nadzorem, w ramach którego są poddawani okresowym ocenom, analizie ryzyka, a w razie konieczności auditom. Wymagania w zakresie bezpieczeństwa informacji są komunikowane w łańcuchu dostaw w postaci Podręcznika dostawcy, który zawiera również arkusz samooceny dostawcy pod względem stosowanych u niego środków technicznych i organizacyjnych zapewniających bezpieczeństwo informacji. Metodyka zapewnienia bezpieczeństwa informacji BOSMAL przekazywanym dostawcom oraz wymagania stawiane dostawcom są opisane w instrukcji BOSMAL/I-6-03 „Realizacja usług informatycznych w BI" i procedurze BOSMAL/P-6-10 „Zarządzanie dostawcami".

8. DOKUMENTY ZWIĄZANE

Oznaczenie	Opis
KJ ZSZ	Księga Jakości Zintegrowanego Systemu Zarządzania
BOSMAL/A-12-03	Bezpieczeństwo fizyczne
BOSMAL/R-0-04	Regulamin pracy
BOSMAL/P-1-03	Doskonalenie i działania korygujące
BOSMAL/P-1-06	Zarządzanie udokumentowanymi informacjami
BOSMAL/P-2-02	Zarządzanie personelem
BOSMAL/P-4-12	Zarządzanie systemem informatycznym
BOSMAL/P-6-10	Zarządzanie dostawcami
BOSMAL/P-12-01	Zarządzanie bezpieczeństwem przetwarzania danych osobowych
BOSMAL/P-12-02	Zarządzanie incydentami bezpieczeństwa informacji
BOSMAL/P-12-04	Plany ciągłości działania
BOSMAL/I-1-07	Zarządzanie ryzykiem
BOSMAL/I-6-03	Realizacja usług informatycznych w BI
BOSMAL/I-6-03 Zał. 1	Podręcznik dostawcy

Oznaczenie	Opis
PN-EN ISO/IEC 27001	Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności, Systemy zarządzania bezpieczeństwem informacji. Wymagania

9. ZAŁĄCZNIKI

9.1. Formularze

Rodzaj dokumentu	Tytuł dokumentu	Okres przechowywania (w latach)
-	-	-

9.2. Załączniki

Rodzaj dokumentu	Tytuł dokumentu	Okres przechowywania (w latach)
-	-	-

TABELA ZMIAN		
Data wydania	**Edycja**	**Opis zmiany**
10.05.2022 **06.09.2024**	01 **02**	**Treść całkowicie przeredagowano i zmieniono, zmian nie zaznaczono. Włączono zapisy polityki BOSMAL/A-12-05 celem jej wycofania.**