Załącznik do zarządzenia Nr ...15.....
Generalnego Dyrektora Dróg Krajowych i Autostrad
z dnia ...14 marca..... 2013 r.

GDDKiA

POLITYKA

BEZPIECZEŃSTWA INFORMACJI

I. Spis treści

II. Deklaracja Generalnego Dyrektora

Intencją Generalnego Dyrektora jest zapewnienie odpowiedniego poziomu bezpieczeństwa informacji w GDDKiA.

Generalny Dyrektor wdraża System Zarządzania Bezpieczeństwem Informacji. Celem wdrożenia tego Systemu jest uzyskanie odpowiedniego poziomu bezpieczeństwa informacji w GDDKiA. Polityka Bezpieczeństwa Informacji jest podstawowym dokumentem zawierającym zbiór zasad i reguł, które są podstawą do zapewnienia bezpieczeństwa informacji w GDDKiA.

System Zarządzania Bezpieczeństwem Informacji określa odpowiedzialność za wdrożenie i aktualizację zasad bezpieczeństwa informacji oraz monitorowanie, nadzór nad przestrzeganiem obowiązujących regulacji, jak i sankcjonowanie istotnych przypadków nieprzestrzegania tych zasad.

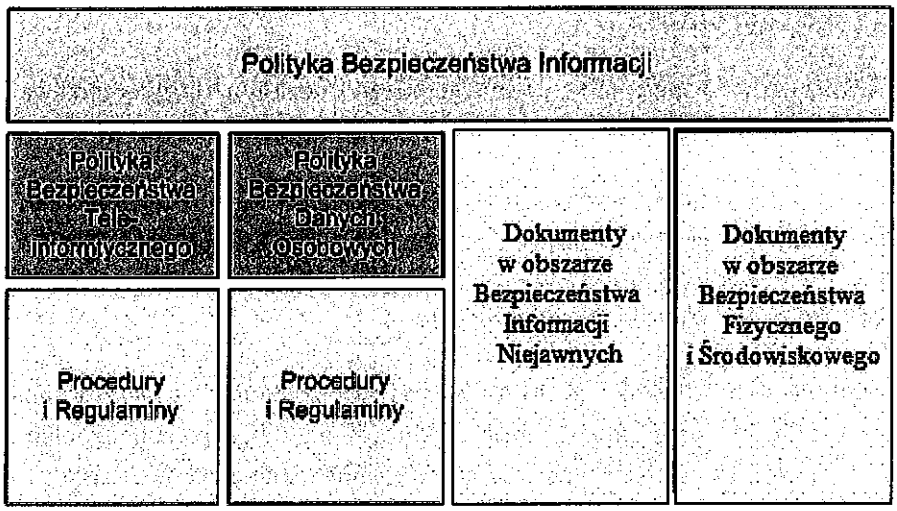
Metody przetwarzania informacji przyjęte w GDDKiA, jak również mechanizmy bezpieczeństwa służące do jej ochrony są zgodne z przepisami prawa obowiązującymi w Rzeczypospolitej Polskiej.

III. Struktura dokumentacji bezpieczeństwa

1. Obszar bezpieczeństwa informacji w GDDKiA został podzielony na cztery podobszary, zgodnie ze schematem 1.

Schemat 1. Podział obszaru bezpieczeństwa informacji.

2. Każdy podobszar opisany jest za pomocą zestawu wytycznych i reguł.
3. Wytyczne i reguły w poszczególnych podobszarach są zgodne z wymaganiami prawnymi, respektują cele i zadania GDDKiA oraz zasady bezpieczeństwa informacji określone w niniejszym dokumencie.
4. Zasady i stosowane zabezpieczenia w poszczególnych podobszarach udokumentowane są w postaci polityk szczegółowych, standardów, procedur, regulaminów, instrukcji. Dokumenty te mogą przybierać formę indywidualnych dokumentów lub łączonych.
5. Dokumentacja bezpieczeństwa informacji w GDDKiA zawiera co najmniej dwie Polityki szczegółowe:
   a) Politykę Bezpieczeństwa Teleinformatycznego,
   b) Politykę Bezpieczeństwa Danych Osobowych.
6. Schemat nr 2 przedstawia umiejscowienie Polityki Bezpieczeństwa Informacji w hierarchii dokumentów dotyczących bezpieczeństwa informacji.



Schemat 2. Umiejscowienie Polityki Bezpieczeństwa Informacji w hierarchii dokumentów dotyczących bezpieczeństwa informacji.

7. Polityka Bezpieczeństwa Informacji jest dokumentem nadrzędnym w stosunku do Polityk szczegółowych oraz pozostałych dokumentów dotyczących bezpieczeństwa w poszczególnych podobszarach.
8. Standardy, Procedury, Regulaminy i Instrukcje są dokumentami uzupełniającymi do Polityk szczegółowych oraz pozostałych dokumentów dotyczących bezpieczeństwa w poszczególnych podobszarach.

IV. Cel

Celem niniejszej Polityki Bezpieczeństwa Informacji jest wprowadzenie zasad bezpieczeństwa informacji tworzonych, przetwarzanych, przechowywanych i przekazywanych w GDDKiA oraz zapewnienie zgodności działań podejmowanych w obszarze ochrony informacji z regulacjami prawnymi.

Niniejsza Polityka Bezpieczeństwa Informacji określa zasady bezpieczeństwa informacji oraz przedstawia podstawowe wytyczne w obszarach bezpieczeństwa teleinformatycznego, danych osobowych, informacji niejawnych oraz bezpieczeństwa fizycznego i środowiskowego. Niniejsza Polityka Bezpieczeństwa Informacji określa również wytyczne w zakresie doboru mechanizmów bezpieczeństwa pod względem ich skuteczności, adekwatności do potrzeb GDDKiA, efektywności finansowej oraz zgodności z wymaganiami prawnymi i regulacyjnymi.

V. Zakres stosowania

Polityka ma zastosowanie do wszystkich informacji tworzonych, przetwarzanych, przechowywanych i przekazywanych w GDDKIA, jak również do wszystkich pracowników GDDKIA zatrudnionych w komórkach organizacyjnych Centrali i Oddziałów GDDKiA oraz podmiotów wykonujących prace na rzecz GDDKiA.

VI. Źródła bezpieczeństwa informacji

1. Polityka Bezpieczeństwa Informacji w GDDKiA jest wdrażana i realizowana z uwzględnieniem:
   a) szacowania ryzyka bezpieczeństwa informacji,
   b) przepisów o ochronie danych osobowych,

c) przepisów o ochronie informacji niejawnych,
d) przepisów o dostępie do informacji publicznej,
e) przepisów o informatyzacji podmiotów realizujących zadania publiczne,
f) pozostałych przepisów prawa stanowiących o ochronie informacji,
g) dokumentów wewnętrznych GDDKiA, w tym:
- Regulaminu organizacyjnego GDDKiA, Ramowego Regulaminu Organizacyjnego oddziału GDDKiA,
- Księgi Zarządzania Procesami.

2. Polityka została opracowana z uwzględnieniem PN-ISO/IEC 27001:2007 oraz metodyki zarządzania architekturą bezpieczeństwa SABSA (Sherwood Applied Business Security Architecture).

VII. Definicje, skróty i konwencje zwrotów

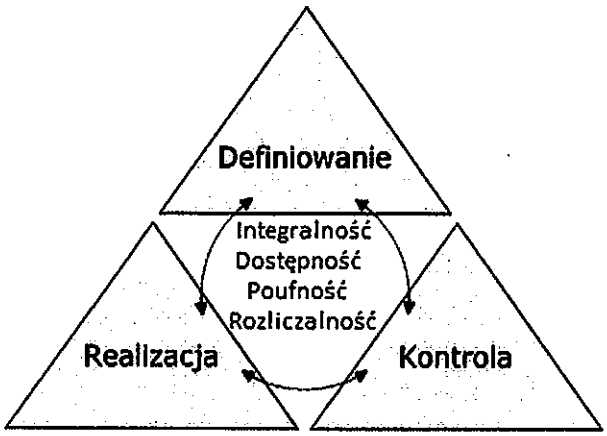
1. Poniżej przedstawione zostały definicje, skróty oraz konwencje zwrotów stosowanych w niniejszej Polityce. Definicje oraz zwroty są wspólne dla wszystkich dokumentów powiązanych i uzupełniających niniejszą Politykę.
   1) ABI – Administrator Bezpieczeństwa Informacji w rozumieniu przepisów o ochronie danych osobowych. Osoba wyznaczana przez Generalnego Dyrektora (Administratora danych osobowych w rozumieniu przepisów o ochronie danych osobowych - dalej „Ustawa").
   2) Akceptujący – właściwy przełożony wnioskującego, sprawujący merytoryczny nadzór nad jego zadaniami służbowymi,
   3) Aktywa/Zasoby – wszystko co stanowi wartość dla GDDKiA,
   4) Bezpieczeństwo informacji – zachowanie poufności, integralności, rozliczalności i dostępności informacji,
   5) Dokumentacja bezpieczeństwa – ogół dokumentów opisujących zasady bezpieczeństwa przetwarzania informacji w GDDKiA,
   6) Dostępność – właściwość informacji polegająca na byciu dostępnym i użytecznym na żądanie upoważnionego podmiotu,
   7) Dyrektor Generalny – Dyrektor Generalny Urzędu,
   8) GDDKiA – Generalna Dyrekcja Dróg Krajowych i Autostrad,
   9) Generalny Dyrektor – Generalny Dyrektor Dróg Krajowych i Autostrad,
   10) Incydent związany z bezpieczeństwem informacji – jest to pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia realizacji zadań i zagrażają bezpieczeństwu informacji,
   11) Integralność – właściwość polegająca na zapewnieniu dokładności i kompletności aktywów,
   12) Kierownik komórki organizacyjnej – dyrektorzy departamentów, biur oraz kierujący komórkami organizacyjnymi wchodzącymi w skład Centrali GDDKiA, naczelnicy wydziałów, kierownicy zespołów i kierujący wyodrębnionymi samodzielnymi stanowiskami wchodzącymi w skład Oddziałów,
   13) Komórka organizacyjna – Departamenty i Biura oraz wyodrębnione samodzielne stanowiska, wchodzące w skład Centrali GDDKiA oraz Wydziały, zespoły i wyodrębnione samodzielne stanowiska wchodzące w skład Oddziałów,

14) Niezaprzeczalność – wynik działania mechanizmów uniemożliwiających wyparcie się utworzenia, modyfikacji bądź usunięcia informacji przez pracownika/podmiot,
15) Pełnomocnik ds. Ochrony Informacji Niejawnych – osoba wyznaczana przez Generalnego Dyrektora, pełniąca obowiązki pełnomocnika do spraw ochrony informacji niejawnych zgodnie z ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych,
16) Polityki szczegółowe – polityki uszczegóławiające Politykę Bezpieczeństwa Informacji,
17) Poufność – właściwość polegająca na tym, ze informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom, podmiotom lub procesom,
18) Pracownik / podmiot – osoba zatrudniona na podstawie stosunku pracy lub osoba świadcząca pracę na podstawie umowy cywilno-prawnej, zawartej z GDDKiA,
19) Procedura – dokument, w którym ustalony jest przebieg procesu oraz określone osoby odpowiedzialne za jego wykonanie wraz z ich uprawnieniami i zakresem odpowiedzialności,
20) Regulamin – dokument zawierający szczegółowy opis przeprowadzenia pojedynczych zadań w procesie, stanowiący doszczegółowienie zapisów w procedurze,
21) Rozliczalność – stan, w którym każdorazowe utworzenie, modyfikacja bądź usunięcie informacji może być jednoznacznie przypisane do pracownika / podmiotu, który daną czynność wykonał,
22) Strony trzecie – podmioty wykonujące prace na rzecz GDDKiA, które posiadają dostęp do zasobów teleinformatycznych, aktywów i zasobów informacyjnych GDDKiA na podstawie podpisanych umów i zobowiązań,
23) SZBI – system zarządzania bezpieczeństwem informacji,
24) Użytkownik – osoba uprawniona do bezpośredniego korzystania z zasobów teleinformatycznych,
25) Właściciel zasobu teleinformatycznego – osoba odpowiedzialna za koordynację działań związanych z zarządzaniem przydzielonym mu zasobem teleinformatycznym,
26) Wnioskujący – użytkownik składający wniosek o nadanie, aktualizację lub odebranie uprawnień dostępu do objętego wnioskiem zasobu teleinformatycznego dla siebie lub podlegającego mu użytkownika,
27) Zasoby teleinformatyczne – systemy informatyczne, programy, aplikacje, urządzenia, infrastruktura teleinformatyczna, w tym sieci teleinformatyczne, które służą do przetwarzania, wytwarzania, przechowywania lub przesyłania informacji w GDDKiA,
28) Zdarzenie związane z bezpieczeństwem informacji – jest określonym stanem systemu, usługi lub sieci, który wskazuje na możliwość naruszenia polityki bezpieczeństwa informacji, błąd zabezpieczenia lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem,
29) Zdarzenie krytyczne – zdarzenie związane z bezpieczeństwem informacji mogące bezpośrednio zagrozić bezpieczeństwu krytycznych procesów związanych ze statutowymi funkcjami GDDKiA,

2. Poniżej przedstawiono opis zastosowanej w niniejszej Polityce konwencji zwrotów.
   a) Wyrażenia „należy" oraz „musi" oznaczają obowiązek stosowania;
   b) Wyrażenie „powinno" oznacza wymóg dobrych praktyk, które należy stosować w każdym przypadku, gdy jest to możliwe bez angażowania nadmiernych lub nieadekwatnych środków.

VIII. Organizacja bezpieczeństwa informacji

1. Organizacja bezpieczeństwa informacji w GDDKiA funkcjonuje przy zachowaniu zasady rozdziału odpowiedzialności operacyjnej od odpowiedzialności kontrolnej i nadzorczej.



Schemat 3. Zasady rozdziału odpowiedzialności.

2. Naczelny Inspektor Bezpieczeństwa Informacji przy pomocy: Administratora Bezpieczeństwa Informacji, Pełnomocnika ds. Ochrony Informacji Niejawnych, Inspektora ds. Bezpieczeństwa Fizycznego oraz Inspektorów ds. Bezpieczeństwa Systemów Teleinformatycznych jest odpowiedzialny za zdefiniowanie i nadzór nad przestrzeganiem zasad bezpieczeństwa informacji.
3. Polityki szczegółowe, w szczególności Politykę Bezpieczeństwa Teleinformatycznego i Politykę Bezpieczeństwa Danych Osobowych, a także dokumenty w obszarze Bezpieczeństwa Informacji Niejawnych zatwierdza Generalny Dyrektor. Procedury i Regulaminy w obszarach określonych w Politykach szczegółowych oraz dokumenty w obszarze Bezpieczeństwa Fizycznego i Środowiskowego zatwierdza Dyrektor Generalny.
4. Za realizację i przestrzeganie zasad bezpieczeństwa informacji odpowiadają wszyscy pracownicy/podmioty posiadający dostęp do aktywów i zasobów informacyjnych GDDKiA. Realizację działań w obszarze bezpieczeństwa informacji koordynuje Naczelny Inspektor Bezpieczeństwa Informacji.
5. Funkcje kontrolne w zakresie skuteczności wdrożonych mechanizmów bezpieczeństwa informacji pełni Komitet ds. Bezpieczeństwa Informacji.
6. Każda z ról zdefiniowanych w organizacji bezpieczeństwa informacji GDDKiA ma przypisany zbiór odpowiedzialności i uprawnień.
7. Kilka ról może być przypisanych do pojedynczego pracownika oraz jedna rola może być przydzielona do kilku pracowników, przy zastrzeżeniu zachowania zasady rozdzielności ról.
8. Za bezpieczeństwo informacji w komórce organizacyjnej odpowiada kierownik tej komórki organizacyjnej.
9. Wszelkie incydenty związane z bezpieczeństwem informacji muszą być niezwłocznie zgłaszane zgodnie z odpowiednimi procedurami reagowania.

10. Generalny Dyrektor:

1) zapewnia odpowiedni poziom bezpieczeństwa informacji;
2) akceptuje plany postępowania z ryzykiem oraz określa akceptowalny poziom ryzyka po wdrożeniu mechanizmów bezpieczeństwa;
3) zatwierdza wysokość nakładów finansowych przeznaczonych na realizację zadań w zakresie bezpieczeństwa informacji;
4) pełniąc funkcję Administratora Danych Osobowych w rozumieniu przepisów o ochronie danych osobowych, wyznacza osobę pełniącą rolę Administratora Bezpieczeństwa Informacji.

11.Dyrektor Generalny:

1) zatwierdza Procedury i Regulaminy dla obszarów określonych w Politykach szczegółowych oraz dokumenty w obszarze Bezpieczeństwa Fizycznego i Środowiskowego w Centrali GDDKiA;
2) zapewnia zgodność stosowanych przez GDDKiA polityk i procedur bezpieczeństwa z obowiązującymi przepisami prawa, wymogami wynikającymi z podpisanych umów i zobowiązań oraz dobrymi praktykami.

12.Komitet ds. Bezpieczeństwa Informacji:

1) W skład Komitetu ds. Bezpieczeństwa Informacji (KBI) wchodzą:
   a) Dyrektor Generalny – przewodniczący KBI,
   b) Dyrektor Biura Generalnego Dyrektora – wiceprzewodniczący KBI, Naczelny Inspektor Bezpieczeństwa Informacji,
   c) Dyrektor Biura Organizacyjno - Administracyjnego – Inspektor ds. Bezpieczeństwa Fizycznego,
   d) Dyrektor Departamentu Informacji i Informatyki – Inspektor ds. Bezpieczeństwa Systemów Teleinformatycznych,
   e) Administrator Bezpieczeństwa Informacji,
   f) Pełnomocnik ds. Ochrony Informacji Niejawnych.
2) Na posiedzenia Komitetu ds. Bezpieczeństwa Informacji mogą zostać zaproszone również inne osoby np. w charakterze eksperta w danej dziedzinie. Dodatkowe osoby nie biorą udziału w głosowaniu, a jedynie mogą pełnić funkcję opiniotwórczą.
3) Komitet ds. Bezpieczeństwa Informacji pełni kontrolę nad realizacją działań operacyjnych i strategicznych w zakresie bezpieczeństwa informacji oraz realizacją planów zarządzania ryzykiem.
4) Komitet ds. Bezpieczeństwa Informacji opiniuje propozycje nakładów finansowych przeznaczonych na realizację zadań strategicznych i operacyjnych w zakresie bezpieczeństwa informacji.
5) Komitet ds. Bezpieczeństwa Informacji opiniuje wyniki cyklicznej analizy ryzyka w obszarze bezpieczeństwa informacji oraz plany zarządzania ryzykiem w obszarze bezpieczeństwa informacji a następnie wnioskuje o ich przyjęcie przez Generalnego Dyrektora.
6) Komitet ds. Bezpieczeństwa Informacji wnioskuje o wykonanie audytów/kontroli w obszarze bezpieczeństwa informacji oraz opiniuje ich wyniki.
7) Komitet ds. Bezpieczeństwa Informacji opiniuje zmiany w procedurach z zakresu bezpieczeństwa informacji.
8) Komitet ds. Bezpieczeństwa Informacji opiniuje projekty zmian i aktualizacji Polityki Bezpieczeństwa Informacji.

9) Komitet ds. Bezpieczeństwa Informacji zatwierdza wdrożenie, zmiany i wycofanie mechanizmów bezpieczeństwa oraz odstępstwa od Polityki Bezpieczeństwa Informacji.
10) Przewodniczący Komitetu ds. Bezpieczeństwa Informacji decyduje o terminach obrad oraz dodatkowym składzie osobowym obrad Komitetu ds. Bezpieczeństwa Informacji.
11) Komitet ds. Bezpieczeństwa Informacji podejmuje decyzje w trybie głosowania. W przypadku równego podziału głosów, decydujący głos ma Przewodniczący Komitetu. W przypadku braku porozumienia, Przewodniczący KBI ma prawo rozstrzygać spory i podejmować decyzje w sprawach z zakresu działania Komitetu ds. Bezpieczeństwa Informacji.

13. Naczelny Inspektor Bezpieczeństwa Informacji:

1) koordynuje realizację działań zmierzających do zapewnienia odpowiedniego poziomu bezpieczeństwa informacji GDDKiA;
2) jest odpowiedzialny za koordynację definiowania, wdrażania i monitorowania działania środków ochrony informacji (zabezpieczeń);
3) odpowiada za koordynację i nadzór nad pracą Inspektorów ds. Bezpieczeństwa Systemów Teleinformatycznych;
4) opracowuje propozycje nakładów finansowych przeznaczonych na realizację zadań strategicznych i operacyjnych w zakresie bezpieczeństwa informacji;
5) jest odpowiedzialny za cykliczne przeprowadzanie przeglądu aktualności Polityki Bezpieczeństwa Informacji;
6) opiniuje projekty aktualizacji i zmian procedur z zakresu bezpieczeństwa informacji;
7) jest odpowiedzialny za przeprowadzanie cyklicznej analizy ryzyka w GDDKiA w poszczególnych obszarach bezpieczeństwa informacji;
8) definiuje zabezpieczenia aktywów i zasobów informacyjnych wspólnie z Inspektorami ds. Bezpieczeństwa Systemów Teleinformatycznych.

14. Administrator Bezpieczeństwa Informacji:

1) składa Generalnemu Dyrektorowi raporty o stanie ochrony danych osobowych, po uzyskaniu opinii Komitetu ds. Bezpieczeństwa Informacji;
2) ustawowym obowiązkiem Administratora Bezpieczeństwa Informacji jest nadzorowanie przestrzegania stosowanych w GDDKiA zasad ochrony przetwarzania danych osobowych, o których mowa w przepisach o ochronie danych osobowych.
3) w swoim zakresie kompetencyjnym Administrator Bezpieczeństwa Informacji:
   a) jest odpowiedzialny za koordynowanie działań wyjaśniających i naprawczych związanych z naruszeniem bezpieczeństwa danych osobowych,
   b) we współpracy z Inspektorem ds. Bezpieczeństwa Systemów Teleinformatycznych, jest odpowiedzialny za nadzór nad cykliczną analizą zgodności sposobu przechowywania i przetwarzania danych osobowych z odpowiednimi regulacjami prawnymi,
   c) we współpracy z Inspektorem ds. Bezpieczeństwa Systemów Teleinformatycznych oraz komórką organizacyjną GDDKiA właściwą w sprawach legislacji, jest odpowiedzialny za przeprowadzanie przeglądów aktualności Polityki Bezpieczeństwa Danych Osobowych oraz uszczegóławiających ją regulacji wewnętrznych, zarówno pod kątem jej zgodności z obowiązującymi przepisami prawa, innymi wewnętrznymi uregulowaniami (w tym komponentami SZBI) jak i kompletności i adekwatności reguł, z częstotliwością nie mniejszą niż raz w roku,

d) we współpracy z Inspektorem ds. Bezpieczeństwa Systemów Teleinformatycznych definiuje mechanizmy bezpieczeństwa w zakresie ochrony danych osobowych przetwarzanych przez GDDKiA,
e) jest odpowiedzialny za weryfikację i opiniowanie wszelkich dokumentów definiujących zasady bezpieczeństwa danych osobowych, w tym tych opracowywanych i zatwierdzanych przez Komitet ds. Bezpieczeństwa Informacji,
f) ma prawo do prowadzenia kontroli oraz wnioskowania o przeprowadzenie audytu/kontroli w zakresie bezpieczeństwa danych osobowych, przy czym uprawnienia kontrolne nie obejmują stałych uprawnień dostępu do systemów, a jedynie na czas prowadzonych czynności.

15. Pełnomocnik ds. Ochrony Informacji Niejawnych:

1) odpowiada za zapewnienie przestrzegania przepisów o ochronie informacji niejawnych.

16. Inspektor ds. Bezpieczeństwa Systemów Teleinformatycznych:

1) odpowiada za realizację zadań zmierzających do zapewnienia bezpieczeństwa informacji przechowywanej lub przetwarzanej w systemach informacyjnych w GDDKiA;
2) W swoim zakresie kompetencyjnym Inspektor ds. Bezpieczeństwa Systemów Teleinformatycznych:
   a) jest odpowiedzialny za nadzór nad procesem wykrywania i obsługi przypadków naruszenia bezpieczeństwa informacji,
   b) współpracuje z audytorami wewnętrznymi oraz zewnętrznymi w trakcie audytów bezpieczeństwa,
   c) ma prawo do prowadzenia kontroli oraz wnioskowania o przeprowadzenie audytu w zakresie bezpieczeństwa informacji,
   d) we współpracy z Administratorem Bezpieczeństwa Informacji oraz komórką organizacyjną GDDKiA właściwą ds. legislacji jest odpowiedzialny za przeprowadzanie przeglądów aktualności Polityki Bezpieczeństwa Informacji oraz uszczegóławiających ją regulacji zarówno pod kątem jej zgodności z obowiązującymi przepisami prawa, innymi wewnętrznymi uregulowaniami (w tym komponentami SZBI) jak i kompletności i adekwatności reguł, z częstotliwością nie mniejszą niż raz w roku,
   e) we współpracy z Naczelnym Inspektorem Bezpieczeństwa Informacji przygotowuje projekty aktualizacji i zmian Polityki Bezpieczeństwa Informacji,
   f) we współpracy z Naczelnym Inspektorem Bezpieczeństwa Informacji definiuje mechanizmy bezpieczeństwa informacji, koordynuje ich wdrożenie i monitoruje ich efektywność,
   g) raportuje do Naczelnego Inspektora Bezpieczeństwa Informacji stan bezpieczeństwa informacji oraz przypadki naruszenia bezpieczeństwa informacji,
   h) opracowuje i koordynuje realizację programu szkoleń w zakresie bezpieczeństwa informacji i systemów informacyjnych,
   i) opracowuje propozycję projektów i związanych z nimi nakładów finansowych dotyczących realizacji zadań strategicznych i operacyjnych w zakresie bezpieczeństwa informacji,
   j) informuje Administratora Bezpieczeństwa Informacji o wszelkich zmianach wprowadzonych w zasobach teleinformatycznych GDDKiA, mogących mieć wpływ na aktualność Polityki Bezpieczeństwa Danych Osobowych.

17.Inspektor ds. Bezpieczeństwa Fizycznego:

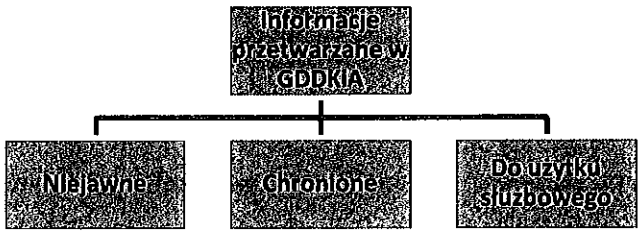
1) realizuje zadania zmierzające do zapewnienia bezpieczeństwa fizycznego i środowiskowego w Centrali GDDKiA;
2) definiuje i wdraża mechanizmy bezpieczeństwa w zakresie bezpieczeństwa fizycznego i środowiskowego we współpracy z Naczelnym Inspektorem Bezpieczeństwa Informacji.

18.Struktury systemu bezpieczeństwa informacji w Oddziałach GDDKiA

1) Dyrektor Oddziału odpowiada za zapewnienie na terenie Oddziału osób odpowiedzialnych oraz szczegółowych procedur w zakresie bezpieczeństwa informacji. Polityka Bezpieczeństwa Informacji oraz polityki szczegółowe i procedury przyjęte w Centrali GDDKiA stanowią ramowe wytyczne w tym zakresie. W oddziałach GDDKiA nie tworzy się funkcji Naczelnego Inspektora Bezpieczeństwa Informacji oraz nie powołuje się Komitetu ds. Bezpieczeństwa Informacji;
2) Dyrektor Oddziału musi ustanowić Inspektora ds. Bezpieczeństwa Systemów Teleinformatycznych oraz Administratora Bezpieczeństwa Informacji w Oddziale;
3) Dyrektor Oddziału powinien wyznaczyć osobę odpowiedzialną za realizację zadań zmierzających do zapewnienia bezpieczeństwa fizycznego i środowiskowego w Oddziale.

IX. Klasyfikacja informacji w GDDKiA

1. W celu zapewnienia właściwego poziomu ochrony, w GDDKiA wszystkie informacje tworzone, przetwarzane, przechowywane i przekazywane muszą podlegać obowiązkowi inwentaryzacji i klasyfikacji (kategoryzację informacji przedstawia Schemat 4). Informacje są klasyfikowane z uwzględnieniem ich wartości, wymagań prawnych, wrażliwości i krytyczności dla GDDKiA.



Schemat 4. Schemat kategoryzacji informacji

2. Przyjmuje się podział informacji według 3 stopniowej kategoryzacji:
   a) **niejawne** – informacje podlegające ochronie na mocy przepisów o ochronie informacji niejawnych;
   b) **chronione** - (dane osobowe, dane klienta, dane finansowo-księgowe, dane użytkowników Krajowego Systemu Poboru Opłat, hasła, klucze kryptograficzne, logi, kopie bezpieczeństwa, itp.);
   c) **do użytku służbowego** – informacje dostępne dla grupy pracowników upoważnionych z uwagi na realizowane zadania regulaminowe.
3. Informacje nieskłasyfikowane są informacjami jawnymi.
4. Stosowane środki ochrony przetwarzania informacji i przetwarzających je zasobów informacyjnych w GDDKiA powinny być dobierane adekwatnie do kategorii danych i występujących zagrożeń.

X. Bezpieczeństwo danych osobowych

1. Dane osobowe w GDDKiA są przetwarzane i chronione zgodnie z przepisami o ochronie danych osobowych (dalej Ustawa), przepisów wykonawczych wydanych na podstawie Ustawy. Dane osobowe podlegają ochronie w ramach ich przetwarzania w przeznaczonych do tego celu zbiorach i zasobach oraz w ramach ich przekazywania pomiędzy tymi zbiorami i zasobami oraz stronami trzecimi.
2. Administrator danych osobowych stosuje środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpiecza dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zamianą, utratą, uszkodzeniem lub zniszczeniem.
3. Poufność, integralność i rozliczalność przetwarzania danych osobowych musi być zapewniona niezależnie od formy i miejsca ich przetwarzania. Administratorem danych osobowych (w rozumieniu Ustawy) przetwarzanych w GDDKiA jest Generalny Dyrektor.
4. Administrator danych osobowych wyznacza ABI, nadzorującego przestrzeganie zasad ochrony o których mowa w pkt 3 niniejszego rozdziału.
5. ABI ma obowiązek reagowania (zgodnie z odpowiednią procedurą) na wszelkie wykryte naruszenia bezpieczeństwa danych osobowych oraz naruszenia przepisów Ustawy oraz regulacji wewnętrznych GDDKiA w zakresie ochrony danych osobowych.
6. Wszystkie osoby upoważnione do przetwarzania danych osobowych bądź uprawnione do dostępu do zasobów teleinformatycznych, w których informacje takie są przetwarzane, mają obowiązek zgłaszania (zgodnie z odpowiednią procedurą reagowania) incydentów związanych z bezpieczeństwem danych osobowych.
7. Niniejsza Polityka jest dokumentem nadrzędnym do Polityki Bezpieczeństwa Danych Osobowych w GDDKiA oraz powiązanych z nią dokumentów uzupełniających, obejmujących swoim zakresem szczegółowe wytyczne w zakresie ochrony w GDDKiA danych osobowych.

XI. Bezpieczeństwo informacji niejawnych

1. Informacje niejawne muszą być przetwarzane zgodnie z dokumentami dotyczącymi bezpieczeństwa w obszarze informacji niejawnych.
2. Szczegółowe wytyczne dotyczące zasad ochrony informacji niejawnych GDDKiA zostały określone odrębnymi dokumentami.

XII. Bezpieczeństwo fizyczne i środowiskowe

1. Miejsca przetwarzania informacji muszą być zabezpieczone w sposób gwarantujący integralność, dostępność, poufność i rozliczalność przetwarzanych informacji.
2. Dla miejsc przetwarzania informacji muszą być zdefiniowane strefy bezpieczeństwa adekwatne do kategorii informacji w nich przetwarzanych.
3. Strefy bezpieczeństwa muszą być zaakceptowane przez Inspektora ds. Bezpieczeństwa Fizycznego. Określone strefy bezpieczeństwa powinny podlegać okresowemu przeglądowi. W wyniku przeglądu aktualizuje się informacje na temat stref.
4. Miejsca przetwarzania informacji muszą być zabezpieczone przed zdarzeniami, mogącymi spowodować uszkodzenie, zniszczenie lub kradzież nośników informacji.

5. Zastosowane środki dla miejsc przetwarzania informacji chroniące przed dostępem osób nieupoważnionych muszą być adekwatne do kategorii informacji przetwarzanej na nośnikach informacji zlokalizowanych w tych pomieszczeniach. W szczególności pomieszczenia te mogą być objęte mechanizmami kontroli dostępu fizycznego, oddzielone barierami ochronnymi, objęte systemem monitoringu lub nadzorowane przez służby ochrony mienia.

XIII. Bezpieczeństwo osobowe

1. Role i zakresy odpowiedzialności pracowników GDDKiA w obszarze bezpieczeństwa informacji powinny być określone i udokumentowane w opisie stanowiska pracy. Wymaganie określenia oraz udokumentowania roli oraz zakresu odpowiedzialności w obszarze bezpieczeństwa informacji dotyczy również innych osób, którym GDDKiA zleca wykonanie prac. Role i zakresy odpowiedzialności, o których mowa, powinny zawierać co najmniej zapisy dotyczące:
   a) konieczności ochrony informacji GDDKiA i przestrzegania zasad określonych w Polityce Bezpieczeństwa Informacji,
   b) konieczności uczestnictwa w konkretnych działaniach i procesach bezpieczeństwa informacji funkcjonujących w ramach GDDKiA,
   c) określenia odpowiedzialności służbowej, karnej,
   d) określenia zobowiązania do informowania o zaobserwowanych zdarzeniach związanych z bezpieczeństwem informacji.
2. Określenie ról i zakresów odpowiedzialności pracowników w obszarze bezpieczeństwa informacji oraz wykonywanie ich przeglądów, spoczywa na kierownikach komórek organizacyjnych, osób dokonujących naboru i zarządzających podległym im personelem. Przeglądy powinny być przeprowadzane po każdorazowej zmianie organizacyjnej, mogącej mieć wpływ na role i zakresy odpowiedzialności w danej komórce organizacyjnej.
3. Wykonywana weryfikacja musi być zgodna z obowiązującymi przepisami prawa, regulacjami wewnętrznymi, etyką oraz powinna uwzględniać potrzeby związane z realizacją zadań oraz wymagany poziom dostępu do zasobów informacji GDDKiA i dostrzeżone w związku z tym ryzyko bezpieczeństwa. Wymaganie to dotyczy również weryfikacji pracowników zmieniających stanowisko lub pełnioną rolę.
4. W zależności od wymaganego poziomu dostępu do informacji GDDKiA, częścią zobowiązań pracowników powinno być odbycie wymaganych szkoleń i podpisanie stosownych oświadczeń w odniesieniu do zapewnienia bezpieczeństwa informacji.
5. Kierownicy komórek organizacyjnych są odpowiedzialni za nadzór nad wypełnianiem przez podległych im pracowników zaleceń i warunków zatrudnienia oraz zasad bezpieczeństwa określonych w Polityce Bezpieczeństwa Informacji.
6. W stosunku do wszystkich pracowników, którzy naruszyli bezpieczeństwo informacji w GDDKiA, przyczynili się do jego naruszenia poprzez przypadkowe lub celowe działanie albo nie dopełnili swoich obowiązków - powinno zostać przeprowadzone postępowanie dyscyplinarne. Postępowanie to musi być przeprowadzone z uwzględnieniem rodzaju, wagi i wpływu naruszenia bezpieczeństwa informacji na funkcjonowanie i bezpieczeństwo GDDKiA.

XIV. Kontrola dostępu do informacji

1. Wszelkie czynności lub zaniechania mogące umożliwić nieuprawniony dostęp do informacji są zabronione.

2. Pracownicy/podmioty oraz strony trzecie współpracujące z GDDKiA muszą zapobiegać nieautoryzowanemu i nieuprawnionemu dostępowi, naruszeniu bezpieczeństwa, kradzieży lub uszkodzeniu informacji.
3. Informacje muszą być zabezpieczone przy wykorzystaniu mechanizmów ochrony przed nieautoryzowanym dostępem.
4. Dostęp do informacji GDDKiA musi być nadawany zgodnie z odpowiednimi procedurami szczegółowymi

XV. Zarządzanie zdarzeniami bezpieczeństwa informacji

1. Wykrywanie przypadków naruszenia bezpieczeństwa informacji jest realizowane poprzez wdrożenie odpowiednich środków kontrolnych, administracyjno-organizacyjnych i techniczno-programowych.
2. Dobór działań i środków reagowania na przypadki naruszenia bezpieczeństwa informacji musi być adekwatny do zagrożenia dla działalności operacyjnej GDDKiA i potencjalnych strat.
3. Każdy przypadek naruszenia bezpieczeństwa informacji należy odpowiednio udokumentować i raportować.
4. Każde naruszenie bezpieczeństwa informacji podlega odpowiedzialności karnej, a sprawca naruszenia będzie odpowiadał za nie zgodnie z obowiązującymi przepisami prawa i regulacjami wewnętrznymi GDDKiA.
5. Przyczyny wystąpienia naruszeń bezpieczeństwa informacji muszą być analizowane, a mechanizmy bezpieczeństwa odpowiednio modyfikowane w celu zminimalizowania ryzyka ponownego wystąpienia przypadków naruszenia bezpieczeństwa informacji.
6. Incydenty związane z bezpieczeństwem informacji muszą być wykrywane, rejestrowane i monitorowane w sposób ciągły w celu ich identyfikowania i zapobiegania ich wystąpieniu w przyszłości.
7. Incydenty bezpieczeństwa informacji muszą być niezwłocznie zgłaszane do osób odpowiedzialnych za ich obsługę, zgodnie z obowiązującymi procedurami szczegółowymi.
8. Dokumentacja incydentów bezpieczeństwa powinna zawierać opis incydentu wraz z przypisaną kategorią i priorytetem, czas zgłoszenia i rozwiązania incydentu, działania podejmowane po otrzymaniu zgłoszenia i ich właścicieli.
9. Dokumentacja incydentów musi umożliwiać przeprowadzenie audytu/kontroli procesu. Audyt lub kontrola poprawności procesu zarządzania incydentami powinna być przeprowadzana nie rzadziej niż raz w roku.
10. Obowiązek zgłaszania incydentów bezpieczeństwa oraz wszelkich potencjalnych podatności mają wszyscy użytkownicy oraz podmioty zewnętrzne mające dostęp do zasobów teleinformatycznych GDDKiA.
11. Proces zarządzania incydentami bezpieczeństwa jest opisany w odpowiednich procedurach szczegółowych.

XVI. Zgodność

1. Wszelkie wymagania wynikające z ustaw, zarządzeń i umów oraz podejścia GDDKiA do ich wypełnienia są określone, udokumentowane i aktualizowane dla każdego systemu informacyjnego w GDDKiA.

2. Wszystkie materiały, które objęte są prawami do własności intelektualnej oraz oprogramowanie prawnie zastrzeżone mogą być użytkowane wyłącznie przy zachowaniu pełnej zgodności z tymi prawami.
3. Informacje są chronione przed utratą, zniszczeniem lub sfałszowaniem zgodnie z wymaganiami ustawowymi, regulacjami wewnętrznymi oraz wymaganiami umownymi.
4. Zapewnia się zgodność ochrony danych osobowych i prywatności z odpowiednimi przepisami prawa, regulacjami wewnętrznymi i, jeśli to wymagane, z zapisami umów.
5. Używanie zabezpieczeń kryptograficznych jest zgodne z odpowiednimi umowami, prawami i regulacjami wewnętrznymi.
6. Kierownicy komórek organizacyjnych i Dyrektorzy Oddziałów zostali zobowiązani do zapewnienia, że wszystkie procedury bezpieczeństwa obszaru, za który są odpowiedzialni, wykonywane są prawidłowo, tak aby osiągnąć zgodność z politykami bezpieczeństwa i standardami.
7. Systemy informacyjne są regularnie sprawdzane pod względem zgodności ze standardami wdrażania zabezpieczeń.
8. Wszelkie instrukcje bezpieczeństwa wykorzystywane przez GDDKiA muszą być zgodne z przepisami prawa, procedurami i politykami.
9. Stosowanie się do zasad określonych w przepisach prawa, Polityce Bezpieczeństwa Informacji oraz innych regulacjach mających zastosowanie w GDDKiA, musi podlegać audytom/kontrolom przeprowadzanym okresowo oraz po wprowadzeniu zmian mających wpływ na sposób zabezpieczenia informacji. Okresowe audyty/kontrole zgodności powinny być przeprowadzane nie rzadziej niż raz w roku.
10. Wszelkie niezgodności powinny być niezwłocznie zgłaszane do Dyrektora Generalnego w celu podjęcia przez niego odpowiednich działań mających na celu dostosowanie niezgodnych postanowień do odpowiednich wymogów.
11. Za zapewnienie zgodności działań pracowników GDDKiA z obowiązującymi politykami, procedurami bezpieczeństwa odpowiedzialni są kierownicy komórek organizacyjnych GDDKiA, którzy w tym zakresie odpowiadają bezpośrednio przed Dyrektorem Generalnym.

Biuro Generalnego Dyrektora

Zbigniew Mitek
Zastępca Dyrektora