DZIENNIK URZĘDOWY

GENERALNEJ DYREKCJI DRÓG KRAJOWYCH I AUTOSTRAD

Warszawa, dnia poniedziałek, 4 września 2023 r.

Poz. 33

ZARZĄDZENIE NR 33

GENERALNEGO DYREKTORA DRÓG KRAJOWYCH I AUTOSTRAD

z dnia 4 września 2023 r.

zmieniające zarządzenie w sprawie ustanowienia Systemu Zarządzania Bezpieczeństwem Informacji w Generalnej Dyrekcji Dróg Krajowych i Autostrad i określenia sposobu wprowadzania dokumentacji tego systemu

Na podstawie § 5 ust. 2 pkt 1 załącznika do zarządzenia Nr 27 Generalnego Dyrektora Dróg Krajowych i Autostrad z dnia 5 grudnia 2022 r. w sprawie ustalenia regulaminu organizacyjnego Generalnej Dyrekcji Dróg Krajowych i Autostrad (Dz. Urz. GDDKiA poz. 27 oraz z 2023 r. poz. 8 i 11), zarządza się, co następuje:

§ 1. W zarządzeniu Nr 23 Generalnego Dyrektora Dróg Krajowych i Autostrad z dnia 1 września 2021 r. w sprawie ustanowienia Systemu Zarządzania Bezpieczeństwem Informacji w Generalnej Dyrekcji Dróg Krajowych i Autostrad i określenia sposobu wprowadzania dokumentacji tego systemu zmienionym zarządzeniem Nr 4 Generalnego Dyrektora Dróg Krajowych i Autostrad z dnia 21 lutego 2022 r. zmieniającym zarządzenie w sprawie ustanowienia Systemu Zarządzania Bezpieczeństwem Informacji w Generalnej Dyrekcji Dróg Krajowych i Autostrad i określenia sposobu wprowadzania dokumentacji tego systemu oraz zarządzeniem Nr 22 Generalnego Dyrektora Dróg Krajowych i Autostrad z dnia 4 października 2022 r. zmieniającym zarządzenie w sprawie ustanowienia Systemu Zarządzania Bezpieczeństwem Informacji w Generalnej Dyrekcji Dróg Krajowych i Autostrad i określenia sposobu wprowadzania dokumentacji tego systemu wprowadza się następujące zmiany:

1) w § 3 uchyla się ust. 1;
2) załączniki nr 1 i 3 do zarządzenia Nr 23 Generalnego Dyrektora Dróg Krajowych i Autostrad z dnia 1 września 2021 r. w sprawie ustanowienia Systemu Zarządzania Bezpieczeństwem Informacji w Generalnej Dyrekcji Dróg Krajowych i Autostrad i określenia sposobu wprowadzania dokumentacji tego systemu otrzymują brzmienie określone odpowiednio w załączniku nr 1 i w załączniku nr 2 do niniejszego zarządzenia.

§ 2. Zarządzenie wchodzi w życie z dniem następującym po dniu ogłoszenia.

P.O. GENERALNY DYREKTOR
DRÓG KRAJOWYCH I AUTOSTRAD

Tomasz Żuchowski

Załączniki do zarządzenia Nr 33
Generalnego Dyrektora Dróg
Krajowych i Autostrad
z dnia 4 września 2023 r.

Załącznik nr 1

Załącznik nr 1

Polityka Bezpieczeństwa Informacji w Generalnej Dyrekcji Dróg Krajowych i Autostrad

Metryka dokumentu:

Sygnatura dokumentu	SZBI.I.2
Wersja dokumentu	2.0
Liczba stron	29

Spis treści

Wstęp

1. Bezpieczeństwo informacji jest jednym z najistotniejszych elementów budowania zaufania społecznego dla Generalnej Dyrekcji Dróg Krajowych i Autostrad, zwanej dalej „GDDKiA", i powinno być uwzględniane we wszystkich procesach składających się na system zarządzania informacją.
2. Bezpieczeństwo informacji należy rozumieć jako ochronę poufności, integralności i dostępności danych i informacji przetwarzanych w ramach systemów i procesów.

   - System zarządzania bezpieczeństwem informacji obejmuje wszystkie utrwalone na nośnikach elektronicznych i w dokumentach oraz nieutrwalone informacje wykorzystywane przez GDDKiA stanowiące jej własność lub powierzone jej przez inne podmioty.

   - Ryzyko związane z możliwością zaistnienia naruszeń bezpieczeństwa informacji podlega stałej ocenie, monitorowaniu i ograniczaniu.

   - Identyfikacja i szacowanie ryzyka opiera się o udokumentowane procedury, uwzględniające zarówno kryteria dotyczące działalności człowieka, jak i aspekty od niego niezależne.

   - Informacje zaklasyfikowane do określonej kategorii mają jednoznacznie określone zasady postępowania z nimi i ich ochrony podczas całego cyklu ich przetwarzania.

   - System zarządzania bezpieczeństwem informacji jest oparty o obowiązujące normy prawne i uznane standardy w tym zakresie.

Mając na uwadze powyższe, **Generalny Dyrektor Dróg Krajowych i Autostrad, zastępcy Generalnego Dyrektora Dróg Krajowych i Autostrad oraz Dyrektor Generalny GDDKiA (Kierownictwo GDDKiA)** deklarują zaangażowanie się w zapewnienie odpowiedniego poziomu ochrony bezpieczeństwa informacji, poprzez zapewnienie wdrożenia i utrzymania Systemu Zarządzania Bezpieczeństwem Informacji.

Kierownictwo GDDKiA zobowiązane jest do:

1) wspierania komórki organizacyjnej GDDKiA powołanej do zapewnienia bezpieczeństwa informacji w realizowaniu jej zadań, w tym zadania związanego z utrzymaniem i ciągłym doskonaleniem Systemu Zarzadzania Bezpieczeństwem Informacji;
2) zapewnienia zasobów niezbędnych do wdrożenia i utrzymania Systemu Zarządzania Bezpieczeństwem Informacji, w tym zapewnienia adekwatnych i proporcjonalnych do realizowanych zadań zabezpieczeń organizacyjnych i technicznych mających na celu minimalizację ryzyk związanych z ochroną informacji;

3) wspierania osób przyczyniających się do zapewnienia efektywnego działania Systemu Zarządzania Bezpieczeństwem Informacji.

Podstawowe zasady i odpowiedzialność w zakresie funkcjonowania Systemu Zarządzania Bezpieczeństwem Informacji określa niniejsza Polityka Bezpieczeństwa Informacji, opracowana zgodnie z obowiązującymi przepisami prawa i wewnętrznymi aktami normatywnymi, w szczególności:

- Rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. WE L 119 z 27.04.2016, str. 1 oraz Dz. Urz. UE L 127 z 23 maja 2018 r., str. 2),
- ustawą z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2022 r. poz. 902),
- ustawą z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2023 r. poz. 57,1123 i 1234),
- ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2023 r. poz.. 756 i 1030),
- ustawą z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego (Dz.U. poz. 1641 i z 2022 r. poz. 1700),
- ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781),
- ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 913),
- ustawą z dnia 22 listopada 2018 r. o dokumentach publicznych (Dz. U. z 2023 r. poz.1006),
- rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 18 stycznia 2007 r. w sprawie Biuletynu Informacji Publicznej (Dz. U. Nr 10, poz. 68),
- rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247),
- zarządzeniem nr 27 Generalnego Dyrektora Dróg Krajowych i Autostrad z dnia 5 grudnia 2022 r. w sprawie nadania Regulaminu Organizacyjnego Generalnej Dyrekcji Dróg Krajowych i Autostrad (Dz. Urz. GDDKiA poz. 27 oraz z 2023 r. poz. 8 i 11),

jak również w oparciu o wymagania Polskich Norm i dobrych praktyk w obszarze bezpieczeństwa informacji, w tym w szczególności z PN-ISO/IEC 27000, PN-ISO/IEC 27001, PN-ISO/IEC 27002, PN-ISO/IEC 27005, PN-EN ISO 22301, PN-EN ISO 22313, PN-EN ISO/IEC 27018.

Rozdział 1.
Przepisy ogólne.

§ 1.

1. Użyte w niniejszej Polityce Bezpieczeństwa Informacji pojęcia i skróty oznaczają:
   1) GDDKiA – Generalną Dyrekcję Dróg Krajowych i Autostrad, tj. Centralę i Oddziały GDDKiA wraz z Rejonami i Obwodami;
   2) SZBI – System Zarzadzania Bezpieczeństwem Informacji;
   3) aktywa informacyjne lub zasoby – wszystko to, co stanowi wartość dla GDDKiA z uwagi na zawarte w nim informacje i w związku z tym wymaga ochrony, w szczególności:
      a) zbiory danych i informacji przetwarzanych w GDDKiA, w tym w postaci udokumentowanej i nieudokumentowanej,
      b) zasoby ludzkie, tj. pracowników lub osoby współpracujące na innej podstawie niż stosunek pracy wraz z ich wiedzą, umiejętnościami, doświadczeniem i kwalifikacjami,
      c) zasoby informatyczne, tj. systemy informatyczne i ich moduły, urządzenia, aplikacje, usługi, a także inne rozwiązania i narzędzia informatyczne wykorzystywane do przetwarzania informacji i funkcjonujące w cyberprzestrzeni GDDKiA;
   4) ASI – administrator określonego zasobu informatycznego lub jego części, odpowiadający za jego nieprzerwane działanie, w tym za tworzenie kopii bezpieczeństwa, tzw. backup;
   5) audyt – zespół czynności mających na celu uzyskanie racjonalnego zapewnienia, że zabezpieczenia informacji, w tym przetwarzanych w systemach informatycznych, funkcjonują zgodnie z założeniami, są adekwatne do poziomu ryzyka, wymogów prawnych i obowiązujących norm;
   6) cyberbezpieczeństwo – odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy;
   7) cyberprzestrzeń GDDKiA – przestrzeń wirtualna powstająca w wyniku wzajemnych połączeń pomiędzy funkcjonującymi w GDDKiA systemami informatycznymi, w tym w ramach zarządzanych przez GDDKiA rozwiązań chmurowych, obejmująca sprzęt, oprogramowanie, dane, a także sposoby i środki ich przesyłania;
   8) dokumentacja SZBI – wszelkie spisane polityki, regulaminy, zasady, wytyczne, instrukcje, procedury, deklaracje, plany, zalecenia lub wyjaśnienia regulujące sposób postępowania

w zakresie zapewnienia bezpieczeństwa informacji, wprowadzone w GDDKiA w sposób opisany w Procedurze wprowadzania dokumentów;

9) dostępność – właściwość polegająca na tym, że informacja, kiedy jest to konieczne, jest dostępna i użyteczna na żądanie upoważnionego podmiotu;
10) IOD – Inspektor Ochrony Danych w GDDKiA;
11) incydent bezpieczeństwa – niepożądane zdarzenie lub serię zdarzeń związanych z bezpieczeństwem informacji, które zagrażają lub mogą zagrażać bezpieczeństwu informacji i stwarzają prawdopodobieństwo utraty aktywów informacyjnych lub zakłócenia realizacji zadań, w przypadku ochrony danych osobowych incydent bezpieczeństwa jest określany jako naruszenie;
12) integralność – właściwość polegająca na tym, że dane nie zostaną zmodyfikowane w inny sposób niż celowe działanie danej osoby, zgodnie z oczekiwaniami;
13) KRI – Krajowe Ramy Interoperacyjności, ustanowione rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów informatycznych;
14) KSZRD – Krajowy System Zarządzania Ruchem Drogowym;
15) PBI – Politykę Bezpieczeństwa Informacji w GDDKiA wprowadzaną w drodze zarządzenia;
16) PBF – Politykę Bezpieczeństwa Fizycznego w GDDKiA wprowadzaną w drodze zarządzenia;
17) PBT – Politykę Bezpieczeństwa Teleinformatycznego w GDDKiA wprowadzaną w drodze zarządzenia;
18) PCD – Plan Ciągłości Działania;
19) PODO – Politykę Ochrony Danych Osobowych w GDDKiA wprowadzaną w drodze zarządzenia;
20) podatność – słabość lub wrażliwość aktywa lub grupy aktywów informacyjnych, która może wpłynąć na wystąpienie zagrożenia cyberbezpieczeństwa i jego ewentualne skutki, może dotyczyć w szczególności sposobu zarządzania lub postępowania personelu, zależności, relacji, kontaktów wewnętrznych i zewnętrznych, czynnika technologicznego, niedoskonałości zabezpieczeń;
21) poufność – właściwość polegającą na tym, że informacja jest udostępniana tylko podmiotom upoważnionym;
22) Procedura wprowadzania dokumentacji – Opis sposobu wprowadzania dokumentacji SZBI, stanowiący załącznik nr 3 do zarządzenia Generalnego Dyrektora Dróg Krajowych i Autostrad w sprawie ustanowienia Systemu Zarządzania Bezpieczeństwem Informacji

w Generalnej Dyrekcji Dróg Krajowych i Autostrad i określenia sposobu wprowadzania dokumentacji tego systemu;

23) RODO – rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych);
24) ryzyko – sytuację, w której określone zagrożenie wykorzysta podatność aktywa lub grupy aktywów informacyjnych, naruszając w ten sposób poufność, integralność lub dostępność informacji;
25) system informacyjny – system teleinformatyczny, o którym mowa w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, wraz z przetwarzanymi w nim danymi w postaci elektronicznej;
26) sytuacja awaryjna – zdarzenie w zakresie bezpieczeństwa informacji, którego skutki powodują utratę ciągłości funkcjonowania jednej lub kilku komórek organizacyjnych GDDKiA, poprzez zakłócenie możliwości normalnej realizacji ich zadań;
27) sytuacja kryzysowa – niespodziewane i niepożądane zdarzenie lub serię zdarzeń związanych z bezpieczeństwem informacji, w szczególności w systemach informatycznych, które mogą zakłócić lub zakłócają proces realizacji zadań GDDKiA; sytuacja kryzysowa może dotyczyć w szczególności bezpieczeństwa ludzi, mienia w znacznych rozmiarach lub środowiska, wywołując znaczne ograniczenia w funkcjonowaniu GDDKiA;
28) użytkownik – osoba, która uzyskała uprawnienie do dostępu i przetwarzania informacji w systemach informatycznych;
29) właściciel systemu – kierownik komórki organizacyjnej, dla której utrzymywana jest główna funkcjonalność systemu, odpowiedzialny za definiowanie potrzeb i celów funkcjonowania systemu informatycznego oraz uczestniczący w procesie zarządzania uprawnieniami;
30) zabezpieczenie – działanie lub rozwiązanie, które ogranicza prawdopodobieństwo wystąpienia zagrożenia lub minimalizuje jego negatywne skutki; wyróżnia się trzy rodzaje zabezpieczeń:
    a) organizacyjne – struktura organizacyjna, zarządzenia, regulaminy, polityki, procedury, instrukcje, zalecenia, zasady, wytyczne, klauzule w umowach, zakresy obowiązków pracowników, szkolenia, audyty, kontrole itp.,
    b) techniczne – systemy zabezpieczeń informatycznych, systemy kontroli dostępu, depozytory kluczy, urządzenia alarmowe, sygnalizacyjne lub monitoringu, oprogramowanie antywirusowe itp.,

c) fizyczne – ogrodzenia, drzwi, zabezpieczenia okien, zamki, pomieszczenia i meble plombowane, zamykane meble biurowe, szafy metalowe i sejfy, strefy ochronne, zabezpieczenia okablowań, klimatyzacja, itp.;

31) zagrożenie – zdarzenie, zjawisko, działanie lub zaniechanie, które może skutkować naruszeniem integralności, dostępności lub poufności informacji albo doprowadzić do szkody, w szczególności poprzez nieosiągnięcie celów GDDKiA.

§ 2.

SZBI objęte są wszystkie dane i informacje wykorzystywane w GDDKiA, niezależnie od formy i nośnika przetwarzania lub dystrybucji, np. ustne, pisemne, nagrania audio i wideo posiadane przez GDDKiA, w szczególności będące własnością GDDKiA lub jej powierzone w ramach umów lub porozumień z podmiotami zewnętrznymi.

§ 3.

1. Bezpieczeństwo informacji zapewnia się w budynkach i pomieszczeniach użytkowanych przez GDDKiA, jak również w miejscach i sytuacjach, w których realizowany jest dostęp do aktywów informacyjnych GDDKiA poza jej siedzibą.
2. Dyrektor Generalny GDDKiA określi, w drodze wytycznych stanowiących dokumentację SZBI, szczegółowe zasady bezpieczeństwa informacji, podczas wykonywania pracy poza lokalizacjami, o których mowa w ust. 1.

§ 4.

1. SZBI obejmuje wszystkie jednostki i komórki organizacyjne GDDKiA.
2. Postanowienia PBI i innej dokumentacji SZBI stosuje się odpowiednio do informacji przetwarzanych w ramach KSZRD. Dopuszcza się wprowadzanie, z zachowaniem Procedury wprowadzania dokumentacji, dokumentacji SZBI odnoszącej się wyłącznie do KSZRD. Dokumentacja ta może modyfikować i wyłączać stosowanie, w stosunku do KSZRD, innych dokumentów SZBI.
3. Do przestrzegania zasad bezpieczeństwa informacji określonych w dokumentacji SZBI zobowiązane są wszystkie osoby korzystające z aktywów informacyjnych GDDKiA, w szczególności:
   1) pracownicy GDDKiA;
   2) osoby odbywające praktykę, staż lub wolontariat w GDDKiA;
   3) podmioty świadczące, na podstawie umów cywilnoprawnych usługi, realizujące dostawy oraz wykonujące roboty budowlane mające istotne znaczenie dla bezpieczeństwa informacji przetwarzanych w GDDKiA określone na podstawie wytycznych, o których mowa w ust. 8;

4) pracownicy podmiotów zewnętrznych mający dostęp do aktywów informacyjnych GDDKiA, w zakresie określonym w umowie lub porozumieniu.

4. Za zapoznanie osób, o których mowa w ust. 3 pkt 1 i 2, z obowiązującymi w GDDKiA zasadami bezpieczeństwa informacji i sposobami ich ochrony, odpowiadają:
   1) pełnomocnik ds. bezpieczeństwa informacji w GDDKiA – w zakresie organizacji szkoleń z bezpieczeństwa informacji;
   2) kierownik komórki organizacyjnej, w której osoba, o której mowa w ust. 3 pkt 1 i 2, jest zatrudniana, odbywa staż, praktykę, wolontariat – w zakresie skierowania na szkolenie.
5. Szkolenia organizowane są jako:
   1) adaptacyjne – dla nowych pracowników GDDKiA, obejmujące zasady bezpieczeństwa informacji, zagrożenia bezpieczeństwa informacji, skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność karną i dyscyplinarną w tym zakresie, stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzeń i oprogramowania minimalizującego ryzyko błędów ludzkich;
   2) cykliczne – dla wszystkich pracowników GDDKiA, mające na celu uzupełnienie i utrwalenie wiedzy w zakresie bezpieczeństwa informacji.
6. Osoby, o których mowa w ust. 3 pkt 1 i 2, zobowiązane są do złożenia pisemnego oświadczenia o zapoznaniu z zasadami bezpieczeństwa informacji, sposobami ich ochrony i o zachowaniu poufności, przed rozpoczęciem wykonywania zadań związanych z korzystaniem z aktywów informacyjnych. Wzór oświadczenia stanowi załącznik nr 1 do PBI.
7. Oświadczenia, o których mowa w ust. 6:
   1) w odniesieniu do osób, o których mowa w ust. 3 pkt 1, przechowywane są w aktach osobowych;
   2) w odniesieniu do osób, o których mowa w ust. 3 pkt 2, przechowywane są wraz z dokumentacją dotyczącą odpowiednio stażu, wolontariatu, praktyki.
8. Dyrektor Generalny GDDKiA określi, w drodze wytycznych, stanowiących dokumentację SZBI, zasady bezpieczeństwa informacji podczas współpracy z podmiotami, o których mowa w ust. 3 pkt 3, i pracownikami, o których mowa w ust. 3 pkt 4.
9. Dyrektor Generalny GDDKiA określi, w drodze wytycznych, stanowiących dokumentację SZBI, zasady bezpieczeństwa osobowego, regulujące sprawy udzielenia, zmiany oraz odebrania dostępu użytkowników do poszczególnych rodzajów informacji.

Rozdział 2.
Zasady bezpieczeństwa i ochrony informacji w GDDKiA.

§ 5.

1. Ochrona informacji realizowana jest:
   1) poprzez zapewnienie:
      a) odpowiedniej jakości procesów ich przetwarzania, w szczególności poprzez adekwatność i skuteczność zabezpieczeń (lub ich grup), odpowiednie warunki ich użytkowania oraz sprawność i efektywność ich wykorzystywania,
      b) pracownikom szkoleń i innych akcji edukacyjnych w zakresie bezpieczeństwa informacji,
      c) właściwych zapisów w zakresie bezpieczeństwa informacji, w szczególności stosowanie klauzul poufności w umowach cywilnoprawnych z podmiotami zewnętrznymi, gdy wymaga tego przedmiot lub specyfika umowy,
      d) ciągłości działania procesów przetwarzania informacji w GDDKiA,
      e) gotowości do reagowania na sytuację awaryjną lub kryzysową,
      f) możliwości sprawnego odtworzenia aktywów informacyjnych w przypadku utraty dostępności lub integralności,
      g) spójnej polityki informacyjnej GDDKiA,
      h) działań kontrolnych w zakresie przestrzegania zasad bezpieczeństwa informacji określonych w GDDKiA, w tym audytów i przeglądów dokumentacji SZBI;
   2) przez zaangażowanie Kierownictwa GDDKiA w proces tworzenia oraz utrzymania SZBI;
   3) przez przypisanie odpowiedzialności za bezpieczeństwo określonych informacji konkretnym komórkom organizacyjnym lub użytkownikom, stosownie do zakresu realizowanych przez nich zadań;
   4) przez pracowników posiadających wiedzę, umiejętności i doświadczenie adekwatne do powierzonych zadań;
   5) dzięki ochronie fizycznej, technicznej i organizacyjnej aktywów informacyjnych przed przypadkowym lub niezgodnym z prawem wykorzystaniem, ujawnieniem, utraceniem, uszkodzeniem, zmodyfikowaniem, zniekształceniem, zniszczeniem lub nieuprawnionym dostępem;
   6) poprzez zabezpieczenie aktywów informacyjnych przed ich uszkodzeniem lub zniszczeniem w wyniku pożaru, zalania, zjawisk naturalnych lub innych zagrożeń;
   7) poprzez przestrzeganie zasad bezpieczeństwa informacji, o których mowa w § 7.
2. GDDKiA stosuje odpowiednie zabezpieczenia we wszystkich obszarach wskazanych w załączniku A do normy PN-ISO/IEC 27001. Dobór zabezpieczeń lub ich grup:

1) jest adekwatny do wymogów prawnych oraz wyników audytów i analiz ryzyka;
2) uzupełnia się wzajemnie, zapewniając wymagany poziom bezpieczeństwa informacji w sposób ciągły;
3) nie powoduje niepotrzebnego dublowania zabezpieczeń i uwzględnia racjonalne gospodarowanie środkami publicznymi, optymalizację potrzeb oraz ograniczenia i uwarunkowania prawno-organizacyjne GDDKiA;
4) następuje w deklaracjach stosowania zabezpieczeń.

3. Deklaracje stosowania zabezpieczeń określają rodzaje zabezpieczeń stosowanych w całej GDDKiA oraz, w razie potrzeby, poszczególnych lokalizacjach, w których przetwarzane są aktywa informacyjne GDDKiA.
4. Deklaracje stosowania zabezpieczeń opracowuje się dla Centrali GDDKiA oraz każdego z Oddziałów GDDKiA zgodnie z Procedurą wprowadzania dokumentacji. Deklaracja opracowana dla Centrali GDDKiA określa wybrane rodzaje zabezpieczeń, które w jednolity sposób są wykorzystywane w całej GDDKiA oraz wskazuje te rodzaje zabezpieczeń, które mogą być modyfikowane lub pomijane w Deklaracjach opracowywanych dla Oddziałów GDDKiA.

§ 6.

1. Poziom bezpieczeństwa informacji uznaje się za odpowiedni wówczas, gdy łącznie spełnione są następujące warunki:
   1) dokonano szacowania ryzyka w odniesieniu do bezpieczeństwa informacji;
   2) wdrożono skuteczne zabezpieczenia wymagane przepisami prawa i wynikające z szacowania ryzyka.
2. Skuteczność zabezpieczeń zachowuje się przy jednoczesnym zastosowaniu i uzupełnianiu się elementów regulujących obszary bezpieczeństwa fizycznego, technicznego i organizacyjnego.

§ 7.

1. Zasadami bezpieczeństwa informacji obowiązujące w GDDKiA są zasady:
   1) wiedzy koniecznej (ograniczonego dostępu do informacji) - pracownicy posiadają dostęp tylko do tych informacji, które są konieczne do realizacji powierzonych im zadań;
   2) indywidualnej odpowiedzialności - za utrzymanie odpowiedniego poziomu bezpieczeństwa poszczególnych aktywów informacyjnych lub ich elementów odpowiadają konkretne osoby, w zakresie nałożonych obowiązków i nadanych uprawnień;
   3) niewygody uzasadnionej - bezpieczeństwo co do zasady opiera się na ograniczeniach i jest niewygodne, jednakże środki ochrony powinny być dobrane w taki sposób, aby nadmiernie nie utrudniały realizacji celów i zadań GDDKiA;
   4) czystego biurka - podczas dłuższej nieobecności pracownika na stanowisku pracy dokumenty i informatyczne nośniki danych należy przechowywać w miarę możliwości

organizacyjno-technicznych w odpowiednio zabezpieczonych meblach biurowych lub szafach metalowych, sejfach, przeznaczonych do tego pomieszczeniach itp.;

5) nadzorowania dokumentów - wszystkie dokumenty zawierające informacje podlegające ochronie przechowuje się w miejscach zabezpieczonych przed dostępem osób nieuprawnionych;
6) czystego ekranu - na czas nieobecności pracownika dostęp do komputera jest blokowany, a po zakończeniu pracy komputer jest wyłączany, chyba że dany komputer musi pracować w trybie ciągłym - np.: serwer obsługujący systemy alarmowe, komputery administratorów, serwery do monitoringu; w czasie obecności pracownika monitor powinien być tak ustawiony, aby nie pozwalał na zapoznawanie się z wyświetlanymi treściami przez osoby postronne, nieupoważnione;
7) czystej tablicy - po zakończonym spotkaniu należy uprzątnąć wszystkie materiały oraz wyczyścić tablice;
8) czystej drukarki – po zakończeniu korzystania z drukarki lub urządzenia wielofunkcyjnego należy uprzątnąć lub zabrać z drukarki lub urządzenia wielofunkcyjnego wydrukowane dokumenty, dokumenty przeznaczone do skanowania, kopiowania lub wydrukowane kopie dokumentów;
9) czystego kosza - dokumenty papierowe, w tym brudnopisy i strony notatek są niszczone w sposób uniemożliwiający ich odczytanie;
10) podziału obowiązków w systemach informatycznych - pojedyncze osoby nie mogą wykonywać w całości zadań dotyczących zarządzania systemem informatycznym;
11) dyskrecji (ograniczonego zaufania i odpowiedzialnej konwersacji) - wszelkie informacje służbowe mogą być przekazywane wyłącznie w celu wykonywania zadań, w zakresie do tego niezbędnym oraz osobom uprawnionym do pozyskania tych informacji;
12) obecności koniecznej - prawo swobodnego przebywania w określonych miejscach istotnych dla bezpieczeństwa informacji mogą mieć tylko osoby upoważnione, przebywanie osób nieupoważnionych w tych miejscach jest możliwe wyłącznie w obecności osób upoważnionych;
13) zamykania pomieszczeń - niedopuszczalne jest pozostawienie niezabezpieczonego pomieszczenia służbowego po zakończeniu pracy, na zakończenie dnia pracy ostatnia wychodząca z pomieszczenia osoba jest obowiązana zamknąć drzwi oraz zabezpieczyć klucze do pomieszczenia;
14) stałej gotowości zabezpieczeń - niedopuszczalne jest tymczasowe wyłączanie mechanizmów zabezpieczających systemy funkcjonujące w GDDKiA bez zastosowania alternatywnych środków ochrony, systemy powinny być sprawne i przygotowane na zidentyfikowane zagrożenia;

15) prywatności kont w systemach - każdy użytkownik zobowiązany jest do pracy w systemach informatycznych na przypisanych lub udostępnionych mu kontach, zabronione jest udostępnianie poświadczeń do własnych kont, w tym również kart systemu kontroli dostępu, innym osobom;
16) poufności i integralności informacji uwierzytelniających - każdy użytkownik zobowiązany jest do zachowania poufności udostępnionych mu haseł, kodów dostępu, kodów PIN, i innych informacji uwierzytelniających go w szczególności w systemach informatycznych;
17) legalnego oprogramowania - na stacjach roboczych zainstalowane jest wyłącznie legalne oprogramowanie;
18) zgłaszania incydentów bezpieczeństwa - każdy użytkownik ma obowiązek niezwłocznie zgłosić wystąpienie lub podejrzenie wystąpienia incydentu mającego lub mogącego mieć wpływ na cyberbezpieczeństwo lub bezpieczeństwo informacji w GDDKiA;
19) automatyzacji kopii zapasowych - procesy tworzenia kopii zapasowych są odpowiednio planowane z uwzględnieniem wymogów prawnych i potrzeb GDDKiA, jak również powinny być zautomatyzowane oraz niemożliwe do przerwania;
20) ochrony nośników danych - dane kopiowane na nośniki i wynoszone poza pomieszczenia użytkowane przez GDDKiA są odpowiednio zabezpieczane na czas transportu i przechowywania, co najmniej poprzez szyfrowanie;
21) adekwatności zabezpieczeń - używane mechanizmy zabezpieczeń są adekwatne do zagrożeń, podatności, wartości aktywów informacyjnych, szacowania ryzyk oraz innych istotnych okoliczności;
22) kompleksowości ochrony - ochrona aktywów informacyjnych opiera się na stosowaniu różnych, wzajemnie uzupełniających się mechanizmów ochrony, w tym ochrony prawnej, fizycznej, technicznej i organizacyjnej;
23) ochrony niezbędnej - minimalny wymagany poziom bezpieczeństwa informacji wynika z obowiązujących przepisów prawa i szacowania i oceny ryzyka; możliwe jest zastosowanie wyższych poziomów bezpieczeństwa informacji, jeżeli uzasadniają to szczególne potrzeby GDDKiA;
24) bezpiecznej współpracy z podmiotami zewnętrznymi - dokumenty regulujące współpracę zawierają stosowne klauzule, w tym o zachowaniu poufności, zasadach postępowania z pozyskaną informacją, niszczenia lub zwrotu dokumentacji po jej wykorzystaniu, gdy wymaga tego przedmiot lub specyfika umowy;
25) doskonalenia systemu – SZBI jest stale monitorowany, analizowany i oceniany do zmieniających się warunków wewnętrznych i zewnętrznych;

26) podwyższonego poziomu ochrony zbiorów informacji - w szczególnie uzasadnionych przypadkach zbiorom danych zapewnia się wyższy poziom ochrony niż pojedynczym danym, które się na niego składają.

2. Przy realizacji zasady czystego kosza i drukarki, o której mowa w ust. 1 pkt 8 i 9, niedopuszczalne jest wyrzucanie dokumentów do kosza. W celu zniszczenia dokumentów należy korzystać z niszczarek. Niszczenie nośników elektronicznych należy przeprowadzić zgodnie z zasadami określonymi w PBT.
3. Katalog zasad, o których mowa w ust. 1, może być rozszerzony i uszczegółowiony, w szczególności w innych dokumentach stanowiących dokumentację SZBI.
4. Zasady bezpieczeństwa informacji uwzględnia się w procesie opracowywania umów i porozumień przewidujących tworzenie i dostęp do aktywów informacyjnych GDDKiA.
5. Szczegółowe zasady bezpieczeństwa fizycznego, w tym zasady doboru i implementacji zabezpieczeń fizycznych, określa PBF.
6. Szczegółowe zasady bezpieczeństwa informatycznego określa PBT.
7. Szczegółowe zasady ochrony danych osobowych określa PODO.

Rozdział 3.
Odpowiedzialność i uprawnienia w zakresie bezpieczeństwa informacji.

§ 8.

Odpowiedzialność za bezpieczeństwo informacji w GDDKiA ponoszą wszystkie osoby i podmioty, o których mowa w § 4 ust. 3, w zakresie odpowiednim do nałożonych na nie obowiązków, posiadanych uprawnień lub postanowień określonych w umowach, porozumieniach i innych pisemnych formach współpracy regulujących obszar bezpieczeństwa informacji.

§ 9.

1. Generalny Dyrektor Dróg Krajowych i Autostrad:
   1) zarządza bezpieczeństwem informacji w GDDKiA oraz decyduje o celach i sposobach przetwarzania informacji, w tym danych osobowych, jako ich administrator;
   2) wydaje zarządzenie wprowadzające PBI i PODO w GDDKiA;
   3) wyznacza pełnomocnika ds. bezpieczeństwa informacji oraz, w razie potrzeby, osobę zastępującą go w czasie nieobecności,
   4) wyznacza pełnomocnika ds. cyberbezpieczeństwa oraz, w razie potrzeby, osobę zastępującą go w czasie nieobecności;
   5) wyznacza IOD oraz, w razie potrzeby, osobę zastępującą go w czasie nieobecności;
   6) wyznacza pełnomocnika ds. ochrony informacji niejawnych;

7) akceptuje ryzyko.

2. Pełnomocnik ds. cyberbezpieczeństwa jest odpowiedzialny za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa zgodnie z art. 21 ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. W razie jego nieobecności osobą odpowiedzialną za utrzymywanie kontaktów są, zgodnie z kolejnością:
   1) pełnomocnik ds. bezpieczeństwa informacji;
   2) osoba zastępująca pełnomocnika ds. cyberbezpieczeństwa;
   3) osoba zastępująca pełnomocnika ds. bezpieczeństwa informacji;
   4) inna osoba wyznaczona przez Generalnego Dyrektora Dróg Krajowych i Autostrad.
3. Zastępcy Generalnego Dyrektora Dróg Krajowych i Autostrad, Dyrektor Generalny GDDKiA oraz Dyrektorzy Oddziałów GDDKiA odpowiadają, w zakresie swojej właściwości, za nadzorowanie bezpieczeństwa informacji w GDDKiA.
4. Dyrektor Generalny GDDKiA:
   1) wydaje zarządzenie wprowadzające PBF, PBT i PCD;
   2) zatwierdza dokumentację SZBI, inną niż określona w pkt 1 lub w ust. 1 pkt 2;
   3) zapewnia, nie rzadziej niż raz w roku, audyt w zakresie bezpieczeństwa informacji w Centrali GDDKiA, realizowany przez komórkę właściwą do spraw audytu wewnętrznego GDDKiA lub uprawnione podmioty zewnętrzne, i akceptuje jego wyniki;
   4) powołuje w Centrali GDDKiA Zespół ds. zarządzania ryzykiem;
   5) określa kierownikom komórek organizacyjnych Centrali GDDKiA zadania mające na celu zapewnienie bezpieczeństwa informacji w podległych im komórkach, w szczególności poprzez akceptowanie planów postępowania z ryzykiem;
   6) akceptuje odstępstwa od zasad określonych w dokumentacji SZBI;
   7) egzekwuje odpowiedzialność pracowników GDDKiA za naruszenia związane z bezpieczeństwem informacji, w zakresie adekwatnym do nałożonych na nich obowiązków i posiadanych uprawnień.
5. Dyrektor Oddziału GDDKiA:
   1) wyznacza koordynatora ds. bezpieczeństwa informacji w Oddziale GDDKiA i osobę zastępującą go w czasie nieobecności;
   2) wyznacza koordynatora ds. Ochrony Danych Osobowych w Oddziale GDDKiA i osobę zastępującą go w czasie nieobecności;
   3) powołuje w Oddziale GDDKiA Zespół ds. zarządzania ryzykiem;
   4) określa kierownikom komórek organizacyjnych w Oddziale GDDKiA zadania mające na celu zapewnienie bezpieczeństwa informacji, w szczególności poprzez akceptowanie planów postępowania z ryzykiem;

5) przekazuje do Centrali GDDKiA, najpóźniej do 31 stycznia każdego roku, plan postępowania z ryzykiem w Oddziale GDDKiA.

6. Pełnomocnik ds. bezpieczeństwa informacji:
   1) nadzoruje działania wewnętrznej komórki organizacyjnej do spraw bezpieczeństwa informacji w Centrali GDDKiA, do zadań której należy w szczególności wspieranie pełnomocnika ds. bezpieczeństwa informacji w zakresie:
      a) koordynowania przebiegu identyfikacji aktywów informacyjnych,
      b) koordynowania i wspierania działań komórek organizacyjnych Centrali GDDKiA i Oddziałów GDDKiA w zakresie bezpieczeństwa informacji, w szczególności poprzez koordynację realizacji planów postępowania z ryzykiem w Centrali GDDKiA i Oddziałach GDDKiA,
      c) koordynowania procesu klasyfikacji informacji przetwarzanych w GDDKiA,
      d) opracowywania propozycji wdrażania, zmieniania i wycofywania mechanizmów bezpieczeństwa oraz opiniowania możliwości zastosowania odstępstw od zasad określonych w dokumentacji SZBI, z wyłączeniem polityk wprowadzanych w drodze zarządzenia,
      e) rozwiązywania incydentów bezpieczeństwa informacji, w zakresie nie zastrzeżonym do kompetencji innych osób i opracowywanie rekomendacji w zakresie przyszłych działań zaradczych,
      f) opracowywania projektów PBI i PODO oraz opracowywanie projektów ich aktualizacji,
      g) opracowywania projektów Deklaracji stosowania zabezpieczeń w Centrali GDDKiA oraz PCD w Centrali GDDKiA,
      h) opracowywania projektów dokumentacji SZBI niezastrzeżonej dla innych osób,
      i) koordynowania funkcjonowania systemu ochrony danych osobowych w GDDKiA,
      j) prowadzenia, we współpracy z pełnomocnikiem ds. cyberbezpieczeństwa i IOD oraz kierownikiem komórki organizacyjnej GDDKiA właściwej do spraw szkoleń, działań informacyjnych dotyczących ochrony informacji, a także planowanie i organizację szkoleń w tym zakresie;
      k) współpracy z koordynatorami ds. bezpieczeństwa informacji w Oddziałach GDDKiA, w tym udzielanie wyjaśnień i rekomendacji w zakresie związanym z funkcjonowaniem SZBI,
      l) organizowania, nie rzadziej niż raz na dwa lata, przeglądów SZBI i koordynowania realizacji ustaleń wynikających z tych przeglądów;
   2) jest uprawniony do:

a) formułowania zaleceń w zakresie związanym z funkcjonowaniem SZBI, w tym w porozumieniu i we współpracy z pełnomocnikiem ds. cyberbezpieczeństwa oraz IOD,
b) formułowania, we współpracy z pełnomocnikiem ds. cyberbezpieczeństwa, rozwiązań w zakresie zabezpieczeń organizacyjnych, fizycznych lub technicznych zwiększających skuteczność zarządzania w obszarze SZBI,
c) występowania do pracowników GDDKiA o złożenie wyjaśnień, w szczególności w przypadku wystąpienia incydentów bezpieczeństwa informacji lub nieprawidłowości w zakresie funkcjonowania SZBI, w przypadkach niezastrzeżonych do kompetencji innych osób,
d) podejmowania działań w celu wyjaśniania incydentów bezpieczeństwa informacji, w zakresie niezastrzeżonym do kompetencji innych osób, i koordynowania wyjaśniania incydentów bezpieczeństwa wspólnych dla kilku obszarów bezpieczeństwa informacji,
e) koordynowania, we współpracy z pełnomocnikiem ds. cyberbezpieczeństwa, procesu zarządzania ryzykiem w Centrali GDDKiA, w szczególności poprzez inicjowanie i kierowanie pracami zespołu ds. zarządzania ryzykiem,
f) rekomendowania rozwiązań organizacyjno-technicznych zwiększających skuteczność zarządzania w obszarze SZBI;

7. Koordynator ds. bezpieczeństwa informacji w Oddziale GDDKiA:
   1) organizuje, we współpracy z koordynatorem ds. ochrony danych osobowych, szkolenia z zakresu bezpieczeństwa informacji w Oddziale GDDKiA;
   2) inicjuje oraz nadzoruje działania wdrożeniowe, korygujące i zapobiegawcze w zakresie bezpieczeństwa informacji w Oddziale GDDKiA i informuje o ich wynikach pełnomocnika ds. bezpieczeństwa informacji;
   3) wyjaśnia incydenty bezpieczeństwa informacji w Oddziale GDDKiA, w zakresie niezastrzeżonym do kompetencji innych osób i koordynuje wyjaśnianie incydentów bezpieczeństwa wspólnych dla kilku obszarów bezpieczeństwa informacji;
   4) kieruje pracami zespołu ds. zarządzania ryzykiem w Oddziale GDDKiA i je inicjuje;
   5) składa zapotrzebowania na środki finansowe z przeznaczeniem na realizację zadań w zakresie bezpieczeństwa informacji w Oddziale GDDKiA;
   6) jest uprawniony do:
      a) formułowania zaleceń w zakresie związanym z funkcjonowaniem SZBI w Oddziale GDDKiA, w tym w porozumieniu i we współpracy z koordynatorem ds. ochrony danych osobowych,
      b) występowania do pracowników Oddziału GDDKiA o złożenie wyjaśnień, w szczególności w przypadku wystąpienia incydentów bezpieczeństwa informacji

i nieprawidłowości w zakresie funkcjonowania SZBI, w przypadkach niezastrzeżonych do kompetencji innych osób,

c) rekomendowania rozwiązań organizacyjno-technicznych zwiększających skuteczność zarządzania w obszarze SZBI w Oddziale GDDKiA.

8. Kierownicy komórek organizacyjnych realizujących zadania zarządzania zasobami ludzkimi w Centrali GDDKiA lub w Oddziałach GDDKiA, we współpracy z pełnomocnikiem ds. bezpieczeństwa informacji i IOD lub odpowiednimi koordynatorami podejmują działania w celu zapewnienia pracownikom GDDKiA szkoleń w zakresie bezpieczeństwa informacji, w szczególności w ramach organizacji szkoleń adaptacyjnych i cyklicznych.
9. Kierownicy komórek organizacyjnych realizujących zadania związane z działalnością promocyjną i informacyjną w Centrali GDDKiA lub w Oddziałach GDDKiA podejmują działania w celu zapewnienia bezpieczeństwa informacji, których ujawnienie w ramach realizacji tych zadań mogłoby narazić na szkodę interes GDDKiA.
10. Kierownicy komórek organizacyjnych realizujących zadania udostępniania informacji publicznej w Centrali GDDKiA lub w Oddziałach GDDKiA uwzględniają zasady bezpieczeństwa informacji, podczas realizacji obowiązku udostępniania informacji publicznej.
11. Kierownicy komórek organizacyjnych realizujących zadania w zakresie zapewnienia ochrony fizycznej w Centrali GDDKiA lub Oddziałach GDDKiA:
    1) koordynują funkcjonowanie ochrony fizycznej obiektów GDDKiA, w tym w szczególności ochrony przed nieuprawnionym dostępem do stref ograniczonego dostępu;
    2) zapewniają niezbędne dla bezpieczeństwa informacji zabezpieczenia oraz prawidłowe ich funkcjonowanie.
12. Pełnomocnik ds. cyberbezpieczeństwa:
    1) opracowuje, we współpracy z pełnomocnikiem ds. bezpieczeństwa informacji oraz kierownikiem komórki organizacyjnej realizującej zadania w zakresie informatyki w Centrali GDDKiA, projekt PBT oraz opracowuje projekty jej aktualizacji;
    2) koordynuje sprawy związane z bezpieczeństwem systemów teleinformatycznych;
    3) analizuje zdarzenia związane z bezpieczeństwem teleinformatycznym;
    4) kontroluje zgodność funkcjonowania systemów teleinformatycznych z SZBI;
    5) wyjaśnia sprawy związane z incydentem bezpieczeństwa przy współpracy z pełnomocnikiem ds. bezpieczeństwa informacji i IOD;
    6) monitoruje realizację działań z zakresu bezpieczeństwa systemów teleinformatycznych oraz bezpieczeństwa cyberprzestrzeni GDDKiA;
    7) jest uprawniony do kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa.
13. Kierownicy komórek organizacyjnych realizujących zadania w zakresie informatyki w Centrali GDDKiA lub Oddziałach GDDKiA:

1) zapewniają bezpieczeństwo zasobów informatycznych funkcjonujących w GDDKiA;
2) wspierają właścicieli systemów w budowie, rozwoju i utrzymaniu systemów będących w ich właściwości merytorycznej.

14. IOD realizuje zadania określone w PODO, a w szczególności:
    1) monitoruje przestrzeganie przepisów prawa i aktów wewnętrznych GDDKiA w zakresie ochrony danych osobowych, z wyłączeniem obszarów zastrzeżonych do właściwości komórki ds. kontroli;
    2) działa na rzecz podniesienia świadomości osób przetwarzających dane osobowe w GDDKiA, w tym poprzez współorganizowanie szkoleń i udzielanie wyjaśnień;
    3) opiniuje projekty przepisów prawa i aktów wewnętrznych w zakresie ich zgodności z przepisami o ochronie danych osobowych;
    4) podejmuje działania w celu wyjaśnienia okoliczności naruszenia ochrony danych osobowych w zakresie niezastrzeżonym dla innych osób i rekomenduje działania zaradcze wobec przyszłych zagrożeń;
    5) uczestniczy w procesie zarządzania ryzykiem, w szczególności udziela zaleceń w zakresie oceny skutków przetwarzania dla ochrony danych osobowych;
    6) współpracuje z komórkami organizacyjnymi GDDKiA w ramach zapewnienia realizacji praw osób, których dane dotyczą;
    7) współpracuje z organem nadzorczym w zakresie ochrony danych osobowych, w tym w zakresie zgłaszania i wyjaśniania okoliczności naruszeń;
    8) pełni funkcję punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO oraz prowadzi konsultacje we wszelkich innych sprawach;
    9) współpracuje z koordynatorami ds. ochrony danych osobowych w Oddziałach GDDKiA, w tym udziela wyjaśnień i rekomendacji w zakresie związanym z ochroną danych osobowych.
15. Koordynator ds. ochrony danych osobowych w Oddziale GDDKiA realizuje zadania określone w PODO, a w szczególności:
    1) monitoruje przestrzeganie przepisów prawa i aktów wewnętrznych GDDKiA w zakresie ochrony danych osobowych w Oddziale GDDKiA;
    2) działa na rzecz podniesienia świadomości osób przetwarzających dane osobowe w Oddziale GDDKiA, w tym poprzez współorganizowanie szkoleń i udzielanie wyjaśnień;
    3) podejmuje działania w celu wyjaśnienia okoliczności naruszenia ochrony danych osobowych w Oddziale GDDKiA w zakresie niezastrzeżonym dla innych osób i rekomenduje działania zaradcze wobec przyszłych zagrożeń;
    4) uczestniczy w procesie zarządzania ryzykiem;

5) współpracuje z komórkami organizacyjnymi Oddziału GDDKiA w ramach zapewnienia realizacji praw osób, których dane dotyczą.

16. Dopuszcza się łączenie funkcji koordynatora ds. ochrony danych osobowych i koordynatora ds. bezpieczeństwa informacji w Oddziale GDDKiA.
17. Dopuszcza się czasowe zastępowanie koordynatora ds. bezpieczeństwa informacji i koordynatora ds. ochrony danych osobowych w Oddziale GDDKiA w czasie jego nieobecności przez odpowiedniego koordynatora z innego Oddziału GDDKiA.
18. Odpowiedzialność i uprawnienia pełnomocnika ds. ochrony informacji niejawnych, określają przepisy o ochronie informacji niejawnych.
19. Kierownicy komórek organizacyjnych GDDKiA, w zakresie swojej właściwości, odpowiadają za:
    1) przestrzeganie zasad bezpieczeństwa informacji przez osoby i podmioty, o których mowa w § 4 ust. 3;
    2) ochronę aktywów informacyjnych;
    3) opracowanie instrukcji i procedur bezpieczeństwa dla procesów pozostających we właściwości komórki organizacyjnej, którą kierują;
    4) zapewnienie ciągłości działania mechanizmów bezpieczeństwa informacji w ramach funkcjonowania komórki, w tym w sytuacjach awaryjnych i kryzysowych, w szczególności przez:
        a) zarządzanie wiedzą i kompetencjami podległych pracowników w taki sposób, aby zapewnić ciągłość realizacji zadań, w tym zastępowalność pracowników i zachowanie zasad bezpieczeństwa informacji,
        b) zarządzanie dostępem do informacji w taki sposób, aby zastępujący się nawzajem pracownicy mieli możliwość przetwarzania informacji niezbędnych do wykonania powierzonych im zadań, z zachowaniem rozliczalności wykonywanych czynności,
        c) zarządzanie nieobecnościami podległych pracowników w taki sposób, aby dostępny był przynajmniej jeden pracownik posiadający kompetencje niezbędne do wykonania zadania wymagającego dostępu do określonego zasobu informacji,
        d) umożliwienie pracownikom GDDKiA udziału w szkoleniach z zakresu bezpieczeństwa informacji oraz innych wydarzeniach podnoszących ich wiedzę i umiejętności z tego zakresu,
        e) zachowanie właściwego trybu zgłaszania i postępowania w sytuacji wystąpienia incydentów bezpieczeństwa informacji, w tym przez osoby i podmioty zewnętrzne, z którymi GDDKiA ma zawarte umowy lub realizuje inne formy współpracy, a które należą do zakresu właściwości danej komórki.

20. Właściciel systemu odpowiada za merytoryczne funkcjonowanie systemu informatycznego, w tym:
    1) weryfikację i potwierdzanie jego zgodności z wymaganiami funkcjonalnymi;
    2) inicjowanie prac nad rozwojem systemu;
    3) proces zarządzania uprawnieniami użytkowników obejmujący:
        a) zakładanie, zmianę, blokowanie lub usuwanie kont,
        b) nadawanie, odbieranie, modyfikację uprawnień,
        c) okresowe przeglądy kont i uprawnień w systemie.
21. ASI odpowiada za utrzymanie ciągłości działania systemu informatycznego, m.in. poprzez zapewnienie bezpieczeństwa i bezawaryjnego funkcjonowania infrastruktury i oprogramowania, wykonywanie kopii bezpieczeństwa oraz realizację innych zadań szczegółowo określonych i opisanych w PBT.
22. Osoby reprezentujące GDDKiA przy zawieraniu umów cywilnoprawnych lub odpowiedzialne za realizację umów cywilnoprawnych zawieranych przez GDDKiA odpowiadają za prawidłowość realizacji tych umów, z uwzględnieniem bezpieczeństwa informacji przetwarzanych w GDDKiA.
23. Pracownicy i współpracownicy GDDKiA oraz inne osoby i podmioty wymienione w § 4 ust. 3 odpowiadają za przestrzeganie zasad wynikających z dokumentacji SZBI, w zakresie jaki ich dotyczy, a w szczególności:
    1) stosują się do zaleceń wydawanych dla sytuacji typowych w zakresie bezpieczeństwa informacji;
    2) chronią udostępnione im aktywa informacyjne;
    3) niezwłocznie reagują w przypadku wystąpienia lub podejrzenia wystąpienia incydentu bezpieczeństwa oraz postępują zgodnie z wypracowanymi procedurami reagowania na incydenty bezpieczeństwa lub podejrzenia wystąpienia incydentu bezpieczeństwa informacji;
    4) zabezpieczają dane i informacje przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów prawa oraz nieuprawnioną zmianą, utratą, uszkodzeniem lub zniszczeniem;
    5) zachowują w tajemnicy informacje pozyskane w ramach wykonywania obowiązków służbowych oraz przestrzegają zasad bezpiecznego ich przetwarzania, w tym w systemach informatycznych, w zakresie nadanych im uprawnień lub wskazanym w upoważnieniu do przetwarzania danych osobowych.

Rozdział 4.
Klasyfikacja informacji i zasady postępowania z informacjami.

§ 10.

1. Informacje przetwarzane w GDDKiA podlegają klasyfikacji z uwagi na ich wartość dla procesów realizowanych w GDDKiA, a także konieczność zachowania poufności w przypadku, gdy wymagają tego przepisy prawa, w tym prawa do prywatności osób fizycznych.
2. Klasyfikacja informacji odbywa się w oparciu o wytyczne w sprawie klasyfikacji informacji przetwarzanych w GDDKiA.
3. Jedna informacja lub jeden zakres danych może zostać zaklasyfikowany do różnych klas lub podklas.
4. Jeden dokument może zawierać informacje zaklasyfikowane do różnych klas lub podklas.

§ 11.

1. Wytyczne w zakresie klasyfikacji informacji przetwarzanych w GDDKiA regulują**:**
   1) zasady klasyfikacji informacji do poszczególnych klas i podklas;
   2) sposoby oznaczania nośników informacji sklasyfikowanych;
   3) sposób postępowania z informacjami zaklasyfikowanymi do poszczególnych klas i podklas.
2. Sposób postępowania z informacjami zaklasyfikowanymi jednocześnie do kilku klas regulują zasady obowiązujące dla klasy, dla której ustanowiono wyższy poziom zabezpieczeń.
3. Szczegółowe zasady postepowania z informacjami niejawnymi regulują odrębne przepisy, w szczególności przepisy ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych.

Rozdział 5.
Incydent bezpieczeństwa informacji.

§ 12.

1. Każdy incydent bezpieczeństwa lub jego podejrzenie podlega obowiązkowemu zgłoszeniu.
2. Szczegółowe zasady zgłaszania, obsługi oraz odpowiedzialności za rozwiązywanie incydentów bezpieczeństwa określają procedury reagowania na incydenty lub podejrzenia wystąpienia incydentu bezpieczeństwa informacji stanowiące dokumentację SZBI.
3. Zasady wynikające z procedur, o których mowa w ust. 2, obowiązują osoby, o których mowa w § 4 ust. 3 pkt 1 i 2.

4. Za ustalenie i egzekwowanie zasad współpracy w zakresie zgłaszania i obsługi incydentów podczas współpracy z podmiotami zewnętrznymi odpowiadają kierownicy komórek organizacyjnych GDDKiA w zakresie realizowanych zadań na podstawie odpowiedniej umowy lub innego dokumentu regulującego zasady współpracy.

Rozdział 6.
Zarządzanie ryzykiem.

§ 13.

1. Zarządzanie ryzykiem w obszarze bezpieczeństwa informacji jest procesem ciągłym obejmującym następujące działania:
   1) szacowanie ryzyka, w tym jego identyfikację i ocenę;
   2) postępowanie z ryzykiem, w tym jego akceptacja lub ograniczanie,
   3) informowanie o ryzyku,
   4) monitorowanie i przegląd ryzyka.
2. Szacowanie ryzyka w obszarze bezpieczeństwa informacji jest obligatoryjne i przeprowadzane cykliczne, nie rzadziej niż raz w roku, do dnia 30 października.
3. Szacowanie ryzyka przeprowadza się również:
   1) przed opracowaniem zasad bezpieczeństwa dla określonego obszaru przetwarzania informacji;
   2) w przypadku planowania istotnych zmian w danym obszarze przetwarzania informacji;
   3) przed wdrożeniem nowego systemu lub narzędzia informatycznego, w którym przetwarzane będą informacje oraz w przypadku planowania istotnych zmian w tym systemie.
4. Szacowanie ryzyka przeprowadza:
   1) zespół ds. zarządzania ryzykiem - w przypadkach, o których mowa w ust. 1 i ust. 3 pkt 1 i 2;
   2) właściciel systemu informatycznego - w przypadkach, o których mowa w ust. 3 pkt 3.
5. Opracowywany jest plan postępowania z ryzykiem, który podlega zatwierdzeniu odpowiednio przez Dyrektora Generalnego GDDKiA lub Dyrektora Oddziału GDDKiA.
6. W GDDKiA przyjmuje się matematyczny model szacowania ryzyka uwzględniający co najmniej prawdopodobieństwo zmaterializowania się zagrożenia na skutek wykorzystania istniejących podatności oraz jego skutek dla interesów GDDKiA wynikających z konieczności zapewnienia bezpieczeństwa informacji. Analiza ryzyka naruszenia praw lub wolności osób fizycznych może uwzględniać inne zmienne.

7. Zarządzanie ryzykiem odbywa się w oparciu o jednolitą dla wszystkich jednostek i komórek organizacyjnych GDDKiA procedurę, zatwierdzaną przez Dyrektora Generalnego GDDKiA.
8. Zarządzanie ryzykiem podlega udokumentowaniu.

Rozdział 7.
Ciągłość działania.

§ 14.

1. PCD określają w szczególności:
   1) rodzaje zabezpieczeń stosowanych w celu zapewnienia stałego dostępu do aktywów informacyjnych;
   2) sposób postępowania w przypadku wystąpienia zdarzeń zagrażających ciągłości działania;
   3) osoby odpowiedzialne za realizację działań zapewniających ciągłość działania.
2. PCD opracowuje się w dwóch częściach, w której:
   1) część pierwsza zawiera opis najważniejszych działań mających zapewnić ciągłość działania i stanowi dokumentację SZBI;
   2) część druga zawiera szczegółowe rozwiązania mogące ulegać częstym aktualizacjom oraz wskazuje osoby odpowiedzialne za realizację poszczególnych działań.
3. PCD opracowuje się dla Centrali GDDKiA oraz każdego z Oddziałów GDDKiA. Część pierwsza PCD ciągłości działania jest zatwierdzana zgodnie z Procedurą wprowadzania dokumentacji. PCD opracowany dla Centrali GDDKiA określa wybrane rodzaje zabezpieczeń i sposobów postępowania, które w jednolity sposób są stosowane w całej GDDKiA.

Rozdział 8.
Działania kontrolne.

§ 15.

1. W ramach działań kontrolnych przeprowadza się w szczególności audyty, kontrole, sprawdzenia, przeglądy, bieżące działania korygujące.
2. Informacje o stwierdzonych niezgodnościach oraz działaniach korygujących podlegają obowiązkowemu dokumentowaniu.
3. Audyty mogą być realizowane w ramach:
   1) kontroli wewnętrznych prowadzonych w Centrali GDDKiA i Oddziałach GDDKiA;
   2) audytów wewnętrznych;

3) kontroli prowadzonych na podstawie ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (Dz. U. z 2020 r. poz. 224);
4) ocen efektywności i skuteczności działania SZBI przeprowadzanych przez niezależne podmioty zewnętrzne;
5) testów bezpieczeństwa systemów teleinformatycznych realizowanych przez niezależne podmioty zewnętrzne;
6) audytów i sprawdzeń prowadzonych przez IOD.

4. Osoby przeprowadzające audyt posiadają odpowiednie kwalifikacje, doświadczenie oraz znajomość metodyki prowadzenia audytu.
5. Audyty są prowadzone z zachowaniem obiektywności i bezstronności procesu audytu, w szczególności niezbędne jest zapewnienie, aby osoby realizujące audyt nie były odpowiedzialne za przegląd tej części systemu, w której realizacji biorą udział w ramach obowiązków służbowych.
6. Zadania związane z prowadzeniem audytu mogą zostać powierzone podmiotowi zewnętrznemu zapewniającemu:
   1) realizację zgodnie ze standardami audytowania systemów zarządzania bezpieczeństwem informacji określonymi w polskich i międzynarodowych normach, w tym PN-ISO/IEC 19011;
   2) wykwalifikowanych audytorów, w tym audytora wiodącego, posiadających certyfikaty potwierdzające wiedzę w zakresie audytowania na zgodność z normą PN-ISO/IEC 27001;
   3) odpowiednie doświadczenie potwierdzone referencjami.

Rozdział 9.
Postanowienia końcowe.

§ 16.

1. Dokumentacja SZBI, z wyłączeniem polityk wprowadzanych na mocy zarządzenia (PBI, PBF, PBT i PODO), tworzona jest w formie pisemnej i podlega zatwierdzeniu zgodnie z kompetencjami określonymi w przepisach rozdziału 3.
2. Dokumentację SZBI, z wyłączeniem polityk wprowadzanych na mocy zarządzenia (PBI, PBF, PBT i PODO), tworzy się wg wzoru określonego w załączniku nr 2 do PBI. Wzór określony w załączniku nr 2 do PBI jest wykorzystywany do tworzenia załączników do polityk wprowadzanych na mocy zarządzenia (PBI, PBF, PBT i PODO).

3. Dokumentacja SZBI jest przekazywana, po zatwierdzeniu, pełnomocnikowi ds. bezpieczeństwa informacji lub odpowiednio do koordynatora ds. bezpieczeństwa informacji w Oddziale GDDKiA.
4. Pełnomocnik ds. bezpieczeństwa informacji odpowiada za podanie do wiadomości pracowników GDDKiA dokumentacji SZBI, poprzez zamieszczanie jej na stronach wewnętrznego portalu intranetowego GDDKiA.

Załącznik nr 1

Oświadczenie o zapoznaniu z zasadami bezpieczeństwa informacji, sposobami ich ochrony i zachowaniu poufności

Niniejszym oświadczam, że zapoznałam/zapoznałem* się z Polityką Bezpieczeństwa Informacji w Generalnej Dyrekcji Dróg Krajowych i Autostrad i zobowiązuję się do jej przestrzegania.

Zobowiązuję się do zachowania w tajemnicy informacji prawnie chronionych, do których mam lub będę miał/a* dostęp w związku z wykonywaniem przeze mnie obowiązków pracowniczych lub innych wykonywanych na rzecz Generalnej Dyrekcji Dróg Krajowych i Autostrad na podstawie …….....……

W szczególności zobowiązuję się do ochrony informacji prawnie chronionych i wewnętrznych przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz ich przypadkową utratą, zniszczeniem lub uszkodzeniem, a także do nieujawniania sposobów zabezpieczenia tych informacji, zarówno w trakcie wykonywania zadań, jak i po ich zakończeniu.

Oświadczam, że bez upoważnienia nie będę wykorzystywał/a* informacji, w tym danych osobowych pochodzących ze zbiorów Generalnej Dyrekcji Dróg Krajowych i Autostrad, jak i zbiorów powierzonych do przetwarzania Generalnemu Dyrektorowi Dróg Krajowych i Autostrad przez inne podmioty.

Mam świadomość, że celem Polityki Bezpieczeństwa Informacji jest zapewnienie odpowiedniego poziomu bezpieczeństwa informacji, w tym danych osobowych, przetwarzanych w Generalnej Dyrekcji Dróg Krajowych i Autostrad, a naruszenia związane z bezpieczeństwem informacji mogą skutkować odpowiedzialnością karną lub dyscyplinarną na zasadach i w trybie przewidzianym w przepisach prawa, w tym w szczególności w ustawie z dnia 21 listopada 2008 r. o służbie cywilnej, ustawie z dnia 26 czerwca 1974 r. Kodeks pracy oraz ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych.

……..……..

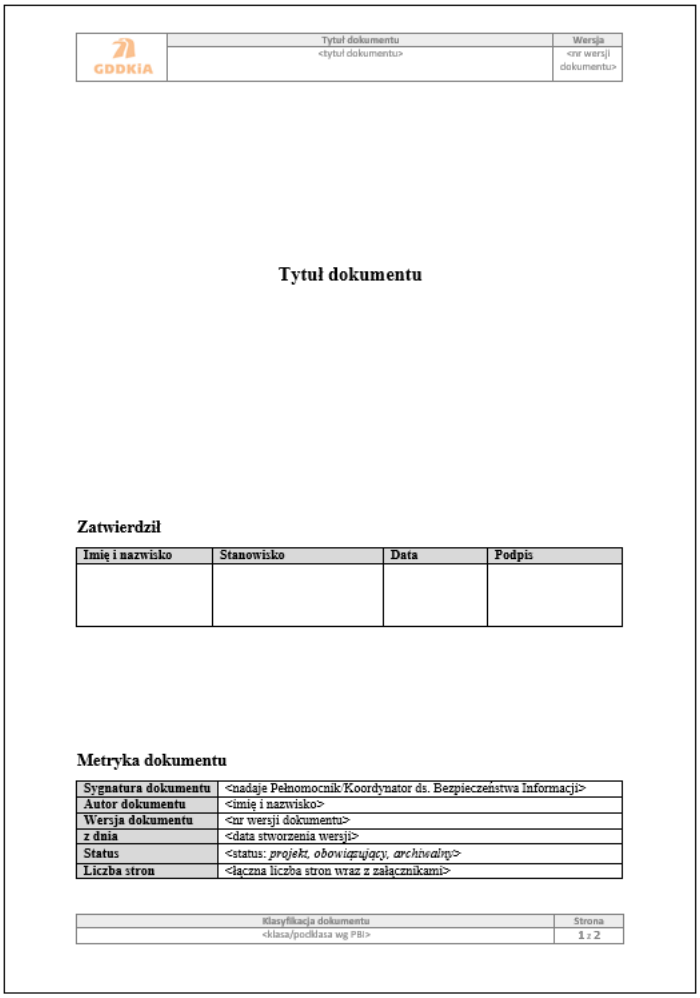
data złożenia oświadczenia, czytelny podpis

* niepotrzebne skreślić

Załącznik nr 2

Wzór dokumentu innego niż zarządzenie, stanowiącego dokumentację Systemu Zarządzania Bezpieczeństwem Informacji w GDDKiA

Pierwsza strona dokumentu:



GDDKiA	Tytuł dokumentu	Wersja
	<tytuł dokumentu>	<nr wersji dokumentu>

Tytuł dokumentu

Zatwierdził

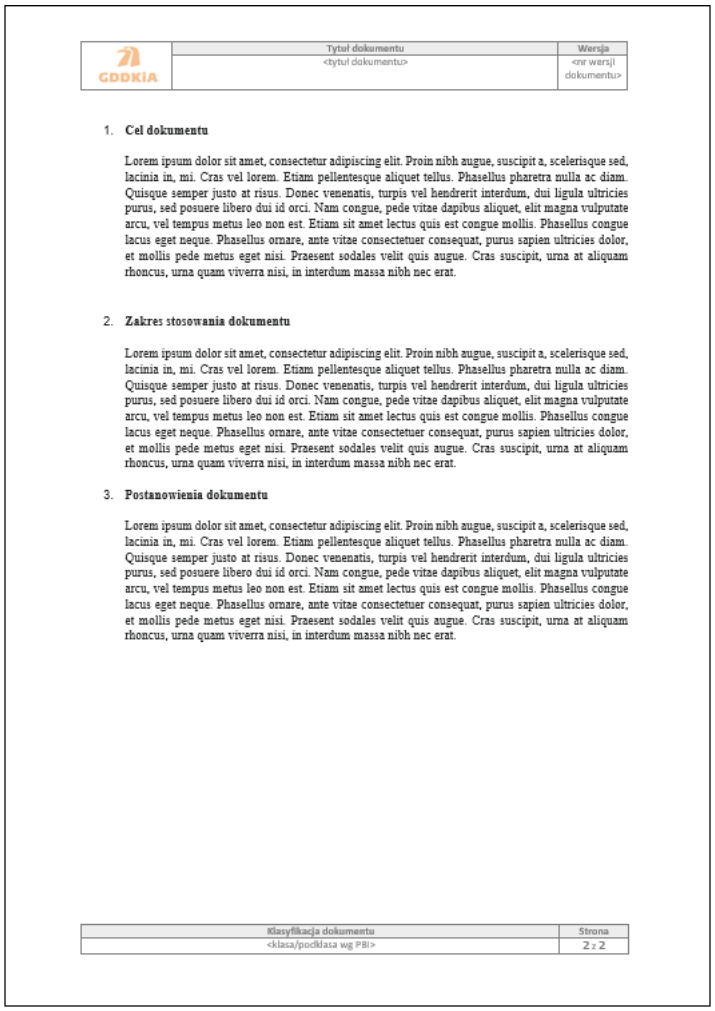
Imię i nazwisko	Stanowisko	Data	Podpis

Metryka dokumentu

Sygnatura dokumentu	<nadaje Pełnomocnik/Koordynator ds. Bezpieczeństwa Informacji>
Autor dokumentu	<imię i nazwisko>
Wersja dokumentu	<nr wersji dokumentu>
z dnia	<data stworzenia wersji>
Status	<status: *projekt, obowiązujący, archiwalny*>
Liczba stron	<łączna liczba stron wraz z załącznikami>

Klasyfikacja dokumentu	Strona
<klasa/podklasa wg PBI>	1 z 2

Kolejne strony dokumentu:



GDDKiA	Tytuł dokumentu	Wersja
	<tytuł dokumentu>	<nr wersji dokumentu>

1. **Cel dokumentu**

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Proin nibh augue, suscipit a, scelerisque sed, lacinia in, mi. Cras vel lorem. Etiam pellentesque aliquet tellus. Phasellus pharetra nulla ac diam. Quisque semper justo at risus. Donec venenatis, turpis vel hendrerit interdum, dui ligula ultricies purus, sed posuere libero dui id orci. Nam congue, pede vitae dapibus aliquet, elit magna vulputate arcu, vel tempus metus leo non est. Etiam sit amet lectus quis est congue mollis. Phasellus congue lacus eget neque. Phasellus ornare, ante vitae consectetuer consequat, purus sapien ultricies dolor, et mollis pede metus eget nisi. Praesent sodales velit quis augue. Cras suscipit, urna at aliquam rhoncus, urna quam viverra nisi, in interdum massa nibh nec erat.

2. **Zakres stosowania dokumentu**

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Proin nibh augue, suscipit a, scelerisque sed, lacinia in, mi. Cras vel lorem. Etiam pellentesque aliquet tellus. Phasellus pharetra nulla ac diam. Quisque semper justo at risus. Donec venenatis, turpis vel hendrerit interdum, dui ligula ultricies purus, sed posuere libero dui id orci. Nam congue, pede vitae dapibus aliquet, elit magna vulputate arcu, vel tempus metus leo non est. Etiam sit amet lectus quis est congue mollis. Phasellus congue lacus eget neque. Phasellus ornare, ante vitae consectetuer consequat, purus sapien ultricies dolor, et mollis pede metus eget nisi. Praesent sodales velit quis augue. Cras suscipit, urna at aliquam rhoncus, urna quam viverra nisi, in interdum massa nibh nec erat.

3. **Postanowienia dokumentu**

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Proin nibh augue, suscipit a, scelerisque sed, lacinia in, mi. Cras vel lorem. Etiam pellentesque aliquet tellus. Phasellus pharetra nulla ac diam. Quisque semper justo at risus. Donec venenatis, turpis vel hendrerit interdum, dui ligula ultricies purus, sed posuere libero dui id orci. Nam congue, pede vitae dapibus aliquet, elit magna vulputate arcu, vel tempus metus leo non est. Etiam sit amet lectus quis est congue mollis. Phasellus congue lacus eget neque. Phasellus ornare, ante vitae consectetuer consequat, purus sapien ultricies dolor, et mollis pede metus eget nisi. Praesent sodales velit quis augue. Cras suscipit, urna at aliquam rhoncus, urna quam viverra nisi, in interdum massa nibh nec erat.

Klasyfikacja dokumentu	Strona
<klasa/podklasa wg PBI>	2 z 2

Załącznik nr 2

Załącznik nr 3

Opis sposobu wprowadzania dokumentacji SZBI

§ 1. 1. Propozycje wprowadzenia nowej polityki, regulaminu, zasad, wytycznych, instrukcji, procedur, deklaracji, planów, zaleceń lub wyjaśnień, a także propozycje ich zmian podlegają zgłoszeniu, za pośrednictwem kanałów komunikacji elektronicznej, pełnomocnikowi ds. bezpieczeństwa informacji.

2. Propozycje, o których mowa w ust. 1, zawierają cel i zakres proponowanych rozwiązań oraz, o ile to możliwe, treść projektowanych postanowień.

3. Propozycje, o których mowa w ust. 1, podlegają:

1) opiniowaniu pod kątem merytorycznym oraz w zakresie spójności SZBI;
2) weryfikacji pod kątem poprawności prawnej i legislacyjnej.

4. Czynności, o których mowa w ust. 3 pkt 1, dokonuje pełnomocnik ds. bezpieczeństwa informacji. W przypadku gdy zakres propozycji dotyczy obszaru bezpieczeństwa fizycznego, bezpieczeństwa teleinformatycznego lub ochrony danych osobowych, pełnomocnik ds. bezpieczeństwa informacji zasięga opinii odpowiednio kierownika komórki ds. ochrony fizycznej Centrali Generalnej Dyrekcji Dróg Krajowych i Autostrad, dalej: „GDDKiA”, kierownika komórki ds. informatycznych Centrali GDDKiA, pełnomocnika ds. cyberbezpieczeństwa lub Inspektora Ochrony Danych.

5. Weryfikacji, o której mowa w ust. 3 pkt 2, dokonuje kierownik komórki ds. prawnych Centrali GDDKiA.

6. Pozytywna opinia, o której mowa w ust. 3 pkt 1, stanowi podstawę do:

1) podjęcia działań mających na celu opracowanie nowej polityki, regulaminu, zasad, wytycznych, instrukcji, procedur, deklaracji lub planów;
2) wprowadzenia zmiany w istniejącej polityce, regulaminie, zasadach, wytycznych, instrukcjach, procedurach, deklaracjach lub planach.

§ 2. Propozycje wprowadzenia lub zmiany polityki, stanowiącej dokument wprowadzany mocą zarządzenia, proceduje się zgodnie z zarządzeniem zarządzeniem nr 38 Generalnego Dyrektora Dróg Krajowych i Autostrad z dnia 31 grudnia 2021 r. w sprawie prowadzenia prac legislacyjnych w Generalnej Dyrekcji Dróg Krajowych i Autostrad.

§ 3. 1. Nowy regulamin, zasady, wytyczne, instrukcje, procedury, deklaracje lub plany oraz ich zmiany podlegają zatwierdzeniu przez Dyrektora Generalnego GDDKiA.

2. Dokument, o którym mowa w ust. 1, lub jego zaktualizowana wersja, jest publikowany w Intranecie, na stronie przeznaczonej do zamieszczania danych o zarządzaniu bezpieczeństwem informacji w GDDKiA.

3. Z dniem następującym po dniu publikacji dokument, o którym mowa w ust. 1, lub wprowadzona zmiana stają się obowiązujące dla wszystkich pracowników GDDKiA i wchodzą w skład dokumentacji SZBI.

§ 4. 1. Projekt wprowadzenia zasad, wytycznych, instrukcji, procedur, deklaracje lub planów lub ich zmian mających obowiązywać w jednym z Oddziałów GDDKiA, w szczególności projekt deklaracji stosowania zabezpieczeń w Oddziale GDDKiA i projekt części pierwszej planu ciągłości działania w Oddziale GDDKiA, są opracowywane przez komórki wewnętrzne Oddziału GDDKiA z uwzględnieniem obowiązujących wytycznych lub wzorów, a następnie przedkładane pełnomocnikowi ds. bezpieczeństwa informacji do akceptacji.

2. Przed dokonaniem akceptacji projektu, o którym mowa w ust. 1, pełnomocnik ds. bezpieczeństwa informacji może zasięgnąć opinii innych komórek organizacyjnych Centrali GDDKiA, pełnomocnika ds. cyberbezpieczeństwa lub Inspektora Ochrony Danych.

3. W przypadku zaakceptowania projektu, o którym mowa w ust. 1, pełnomocnik ds. bezpieczeństwa informacji przekazuje go do zatwierdzenia właściwemu Dyrektorowi Oddziału GDDKiA.

4. Zatwierdzony dokument, o którego projekcie jest mowa w ust. 1, lub jego zaktualizowana wersja, jest publikowany w Intranecie, na stronie przeznaczonej do zamieszczania danych o zarządzaniu bezpieczeństwem informacji w GDDKiA.

5. Z dniem następującym po dniu publikacji w Intranecie dokument, o którego projekcie jest mowa w ust. 1, lub wprowadzona zmiana, stają się obowiązujące dla wszystkich pracowników Oddziału GDDKiA i wchodzą w skład dokumentacji SZBI.

§ 5. 1. Propozycja wprowadzenia nowych zaleceń lub wyjaśnień lub propozycja zmian istniejących zaleceń lub wyjaśnień, zgłoszona zgodnie z § 1 ust. 1, podlega ocenie i akceptacji, zgodnie z właściwością wynikającą z treści wyjaśnień, odpowiednio przez:

1) pełnomocnika ds. bezpieczeństwa informacji - w zakresie spójności z SZBI;

2) kierownika komórki ds. ochrony fizycznej Centrali GDDKiA - w zakresie bezpieczeństwa fizycznego;
3) kierownika komórki ds. informatycznych Centrali GDDKiA - w zakresie bezpieczeństwa teleinformatycznego po uzyskaniu opinii pełnomocnika ds. cyberbezpieczeństwa;
4) pełnomocnika ds. bezpieczeństwa informacji - w zakresie ochrony danych osobowych po uzyskaniu opinii Inspektora Ochrony Danych.

2. Inspektor Ochrony Danych może opracowywać, zgodnie ze swoją właściwością, zalecenia lub wyjaśnienia lub zmiany istniejących zaleceń lub wyjaśnień, po uzyskaniu opinii pełnomocnika ds. bezpieczeństwa informacji.

§ 6. 1. Zalecenia, wyjaśnienia lub ich zmiany, po ich zatwierdzeniu, zgodnie z właściwością, przez pełnomocnika ds. bezpieczeństwa informacji, kierownika komórki ds. ochrony fizycznej Centrali GDDKiA, kierownika komórki ds. informatycznych Centrali GDDKiA, pełnomocnika ds. cyberbezpieczeństwa lub Inspektora Ochrony Danych, są publikowane w Intranecie, na stronie przeznaczonej do zamieszczania danych o zarządzaniu bezpieczeństwem informacji w GDDKiA.

2. Z dniem następującym po dniu publikacji w Intranecie zalecenia, wyjaśnienia lub ich zmiany wchodzą w skład dokumentacji SZBI.

§ 7. 1. W uzasadnionych przypadkach można odstąpić od stosowania regulaminu, zasad, wytycznych, instrukcji, procedur, deklaracji, planów, zaleceń lub wyjaśnień określonych w dokumentacji obligatoryjnej SZBI.

2. Odstępstwo, o którym mowa w ust. 1, następuje wyłącznie na wniosek Dyrektora Oddziału GDDKiA lub kierownika komórki organizacyjnej Centrali GDDKiA.

3. Wniosek, o którym mowa w ust. 2, wraz z uzasadnieniem, Dyrektor Oddziału GDDKiA lub kierownik komórki organizacyjnej Centrali GDDKiA, kieruje do Dyrektora Generalnego GDDKiA za pośrednictwem pełnomocnika ds. bezpieczeństwa informacji.

4. Pełnomocnik ds. bezpieczeństwa informacji dokonuje weryfikacji i analizy możliwości zastosowania zaproponowanych odstępstw mając na względzie konieczność zapewnienia poufności, integralności i dostępności informacji przetwarzanych w GDDKiA.

5. W przypadku gdy wniosek, o którym mowa w ust. 2, dotyczy obszaru bezpieczeństwa fizycznego, bezpieczeństwa teleinformatycznego lub ochrony danych osobowych, pełnomocnik ds. bezpieczeństwa informacji zasięga opinii odpowiednio kierownika komórki

ds. ochrony fizycznej Centrali GDDKiA, kierownika komórki ds. informatycznych Centrali GDDKiA, pełnomocnika ds. cyberbezpieczeństwa lub Inspektora Ochrony Danych.

6. Po dokonaniu weryfikacji i analizy wniosku oraz zasięgnięciu opinii, o których mowa w ust. 5, pełnomocnik ds. bezpieczeństwa informacji przekazuje wniosek wraz z rekomendacją Dyrektorowi Generalnemu GDDKiA.

7. Zgodę na odstępstwo, o którym mowa w ust. 1, wydaje Dyrektor Generalny GDDKiA.

8. Zgoda na odstępstwo ma charakter konkretny, dotyczący danej sprawy, tymczasowy i obowiązuje w okresie w niej oznaczonym.

§ 8. Publikowanie dokumentacji i informowanie o tej publikacji w Intranecie pracowników GDDKiA jest obowiązkiem pełnomocnika ds. bezpieczeństwa informacji.