DZIENNIK URZĘDOWY

Głównego Inspektoratu Transportu Drogowego

Warszawa, dnia 19 września 2019 r.

Poz. 44

Z A R Z Ą D Z E N I E N R 4 3 / 2 0 1 9

G Ł Ó W N E G O I N S P E K T O R A T R A N S P O R T U D R O G O W E G O

z dnia 19 września 2019 r.

w sprawie wprowadzenia Systemu Zarządzania Bezpieczeństwem Informacji w Głównym Inspektoracie Transportu Drogowego

Na podstawie art. 24 ust. 1 i 2 rozporządzenia 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. UE L 119 z 04.05.2016, str. 1), art. 32 ust. 3 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125), art. 13 ust. 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2019 r. poz. 700, 730, 848 i 1590) w związku z § 20 rozporządzenia 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) oraz art. 52 ust. 1 ustawy z dnia 6 września 2001 r. o transporcie drogowym (Dz. U. z 2019 r. poz. 58, z późn. zm.[1)]) zarządza się, co następuje:

§ 1. W Głównym Inspektoracie Transportu Drogowego, zwanym dalej: GITD, ustanawia się, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali System Zarządzania Bezpieczeństwem Informacji, zwany dalej: SZBI, zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

---

1) Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2019 r. poz. 60, 125, 690, 730, 1123, 1180, 1466, 1495 i 1556.

2. SZBI odnosi się do ochrony informacji we wszystkich procesach, w których informacje są przetwarzane, w szczególności ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji.

§ 2. 1. Podstawową dokumentację SZBI stanowi:

1) Polityka Bezpieczeństwa Informacji, stanowiąca załącznik do zarządzenia;
2) Polityka Ochrony Danych Osobowych;
3) Polityka Bezpieczeństwa Teleinformatycznego.

2. Dokumenty, o których mowa w ust. 1 pkt 2 i 3, zostaną przedłożone do zatwierdzenia Głównemu Inspektorowi Transportu Drogowego w terminie 15 dni roboczych od dnia wejścia w życie niniejszego zarządzenia i zostaną wprowadzone w formie polityk lub innych dokumentów, na zasadach określonych w Polityce Bezpieczeństwa Informacji.

§ 3. Dyrektor Generalny Głównego Inspektoratu Transportu Drogowego zapewnia przeprowadzenie przynajmniej raz do roku audytu wewnętrznego w zakresie bezpieczeństwa informacji, zgodnie z wymogami określonymi w § 20 ust. 2 pkt 14 rozporządzenia 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, przez komórkę właściwą do spraw audytu wewnętrznego GITD lub uprawnione podmioty zewnętrzne.

§ 4. Dyrektorzy komórek organizacyjnych oraz naczelnicy delegatur terenowych GITD odpowiadają za wdrożenie i przestrzeganie SZBI w podległych sobie komórkach organizacyjnych.

§ 5. Zarządzenie wchodzi w życie z dniem ogłoszenia.

Główny Inspektor Transportu Drogowego: *A. Gajadhur*

Załącznik do zarządzenia nr 43/2019
Głównego Inspektora Transportu Drogowego
z dnia 19 września 2019 r. (poz. 44)

POLITYKA BEZPIECZEŃSTWA INFORMACJI W GŁÓWNYM INSPEKTORACIE TRANSPORTU DROGOWEGO

Rozdział 1

Przepisy ogólne

§ 1. 1. Polityka Bezpieczeństwa Informacji w Głównym Inspektoracie Transportu Drogowego określa podstawowe zasady zarządzania bezpieczeństwem informacji oraz podmioty odpowiedzialne za ochronę informacji w Głównym Inspektoracie Transportu Drogowego.

2. Zasady zarządzania bezpieczeństwem informacji w Głównym Inspektoracie Transportu Drogowego zostały opracowane zgodnie z obowiązującymi przepisami oraz w oparciu o wymagania Polskich i Międzynarodowych Norm i standardów w obszarze bezpieczeństwa informacji, oraz inne wewnętrzne akty normatywne, w szczególności:

1) 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. UE L 119 z 04.05.2016, str. 1);
2) ustawą z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. z 2019 r. poz. 1231);
3) ustawą z dnia 29 sierpnia 1997 r. - Ordynacja podatkowa (Dz. U. z 2019 r. poz. 900, z późn. zm.[1)]);
4) ustawą z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2019 r. poz. 1429);
5) ustawą z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2019 r. poz. 700, 730, 848 i 1590);
6) ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2019 r. poz. 742);
7) ustawą z dnia 25 lutego 2016 r. o ponownym wykorzystywaniu informacji sektora publicznego (Dz. U. z 2019 r. poz. 1446);
8) ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r. poz. 1000 i 1669 oraz z 2019 r. poz. 730);
9) ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560);

[1)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2019 r. poz. 924, 1018, 1495, 1520, 1553, 1556, 1649, 1655 i 1667.

10) ustawą z dnia 22 listopada 2018 r. o dokumentach publicznych (Dz. U. z 2019 r. poz. 53, 1091 i 1716);
11) ustawą z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125);
12) rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 18 stycznia 2007 r. w sprawie Biuletynu Informacji Publicznej (Dz. U. poz. 68);
13) 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);
14) rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 2 lipca 2019 r. w sprawie wymagań w zakresie bezpieczeństwa wytwarzania blankietów dokumentów publicznych (Dz. U. poz. 1266);
15) rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 2 lipca 2019 r. w sprawie wykazu minimalnych zabezpieczeń dokumentów publicznych przed fałszerstwem (Dz. U. poz. 1281);
16) rozporządzeniem Rady Ministrów z dnia 11 lipca 2019 r. w sprawie wykazu dokumentów publicznych (Dz. U. poz. 1289);
17) Polskimi i Międzynarodowymi Normami:
    a) PN-ISO/IEC 27001,
    b) PN-ISO/IEC 27002,
    c) PN-ISO/IEC 27005,
    d) PN-EN ISO 22301,
    e) PN-EN ISO 22313;
18) zarządzeniem nr 3/2018 Głównego Inspektora Transportu Drogowego z dnia 5 lutego 2018 r. w sprawie nadania regulaminu organizacyjnego Głównemu Inspektoratowi Transportu Drogowego (Dz. Urz. GITD z 2019 r. poz. 39);
19) obowiązującym w Głównym Inspektoracie Transportu Drogowego planem ochrony informacji niejawnych, w tym w razie wprowadzenia stanu nadzwyczajnego;
20) obowiązującym planem zarządzania kryzysowego Głównego Inspektoratu Transportu Drogowego.

§ 2. Użyte w Polityce Bezpieczeństwa Informacji Głównego Inspektoratu Transportu Drogowego pojęcia oznaczają:

1) aktywa (zasoby) – wszystko, co stanowi wartość dla GITD i w związku z tym wymaga ochrony, w szczególności:
   a) aktywa informacyjne (informacje) rozumiane jako wiedza, dane oraz wszelkie informacje wpływające na wartość GITD, w tym informacje udokumentowane,
   b) zasoby ludzkie – pracownicy, ich wiedza, umiejętności, doświadczenie i kwalifikacje,
   c) usługi i licencje,
   d) wartości niematerialne, w tym wizerunek, kultura organizacyjna, wartości etyczne,
   e) zasoby informatyczne: systemy informatyczne, aplikacje i inne rozwiązania informatyczne wykorzystywane do przetwarzania informacji,
   f) cyberprzestrzeń GITD,
   g) urządzenia dostępowe i oprogramowanie,
   h) zabezpieczenia fizyczne, środowiskowe, techniczne i organizacyjne,
   i) siedziba i nieruchomości oraz poszczególne pomieszczenia użytkowane przez GITD;
2) AMS – Administratora Merytorycznego Systemu;
3) ASI – Administratora Systemu Informatycznego;
4) audyt, kontrola oraz przegląd – czynności mające na celu uzyskanie racjonalnego zapewnienia, że zabezpieczenia informacji w tym systemów informatycznych funkcjonują zgodnie z założeniami, są adekwatne do poziomu ryzyka, wymogów prawnych i obowiązujących norm. Sprawdzeniu podlega, czy zabezpieczenia, w tym w systemie informatycznym i związanych z nim zasobach właściwie chronią informacje, zapewniają integralność, poufność i dostępność;
5) bezpieczeństwo informacji – zabezpieczenie i zachowanie informacji w zakresie integralności, dostępności i poufności przed nieautoryzowanym dostępem lub zmianą. Dodatkowo mogą być brane pod uwagę inne atrybuty jak rozliczalność, autentyczność, niezaprzeczalność oraz niezawodność;
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) dostępność – właściwość polegająca na tym, że informacja jest dostępna i użyteczna na żądanie upoważnionego podmiotu;
8) GITD – Główny Inspektorat Transportu Drogowego;
9) Główny Inspektor – Głównego Inspektora Transportu Drogowego;
10) incydent – pojedyncze zdarzenie lub seria niepożądanych zdarzeń, które mają lub mogą mieć niekorzystny wpływ na cyberbezpieczeństwo, w tym powodować lub móc spowodować obniżenie

jakości lub przerwanie realizacji zadań publicznych realizowanych przez GITD, w szczególności z wykorzystaniem systemów informatycznych;

11) incydent bezpieczeństwa informacji – pojedyncze zdarzenie lub seria niepożądanych zdarzeń związanych z bezpieczeństwem informacji, które zagrażają lub mogą zagrozić bezpieczeństwu informacji oraz stwarzają znaczne prawdopodobieństwo utraty aktywów lub zakłócenia realizacji zadań;
12) integralność – właściwość polegającą na zapewnieniu dokładności i kompletności informacji;
13) IOD – inspektora ochrony danych powoływanego na podstawie przepisów RODO oraz ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości;
14) KRI – rozporządzenie 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;
15) KSPO – Krajowy System Poboru Opłat;
16) PBI – Politykę Bezpieczeństwa Informacji Głównego Inspektoratu Transportu Drogowego;
17) PBT – Politykę Bezpieczeństwa Teleinformatycznego Głównego Inspektoratu Transportu Drogowego, stanowiącą dokument wewnętrzny zatwierdzany przez Głównego Inspektora i udostępniany w całości lub w części na zasadzie wiedzy uzasadnionej;
18) PODO – Politykę Ochrony Danych Osobowych Głównego Inspektoratu Transportu Drogowego, stanowiącą dokument wewnętrzny zatwierdzany przez Głównego Inspektora i udostępniany w całości lub w części na zasadzie wiedzy uzasadnionej;
19) podatność – słabość lub wrażliwość aktywa lub grupy aktywów w zakresie funkcjonowania GITD, która może wpłynąć na wystąpienie zagrożenia i jego ewentualne skutki. Podatność może dotyczyć w szczególności sposobu zarządzania lub postępowania, personelu, zależności, relacji, kontaktów wewnętrznych i zewnętrznych, czynnika technologicznego, niedoskonałości zabezpieczeń;
20) poufność – właściwość polegającą na tym, że informacja nie jest udostępniana ani ujawniana nieautoryzowanym osobom, podmiotom lub procesom;
21) 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);

22) ryzyko – potencjalną sytuację, w której określone zagrożenie wykorzysta podatność aktywa lub grupy aktywów, powodując w ten sposób naruszenie poufności, integralności, dostępności lub innych atrybutów bezpieczeństwa informacji;
23) system informacyjny, system informatyczny – 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;
24) sytuacja awaryjna – zdarzenie, którego skutki powodują utratę ciągłości działania GITD; może dotyczyć jednej lub kilku komórek organizacyjnych, których procesy zostały zakłócone;
25) sytuacja kryzysowa – niespodziewane i niepożądane zdarzenie lub seria zdarzeń związanych z bezpieczeństwem przetwarzania informacji, w szczególności w systemach informatycznych, które mogą zakłócić lub zakłócają proces realizacji zadań GITD (sytuacja może dotyczyć w szczególności bezpieczeństwa ludzi, mienia w znacznych rozmiarach lub środowiska, wywołując znaczne ograniczenia w funkcjonowaniu GITD);
26) SZBI – System Zarządzania Bezpieczeństwem Informacji, odnoszący się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji, obejmujący strukturę organizacyjną, polityki, planowane działania, odpowiedzialności, zasady, procedury, procesy i aktywa. W szczególności SZBI w GITD obejmuje PBI, PBT, PODO, odrębne SZBI, w tym certyfikowane za zgodność z normą PN-ISO/IEC 27001 dla systemów informatycznych GITD, inne polityki, procedury, instrukcje, wytyczne, zalecenia, obowiązujące wewnętrzne akty normatywne i inne odnoszące się bezpośrednio i pośrednio do bezpieczeństwa informacji i cyberbezpieczeństwa. SZBI w GITD w szczególności nie ma formy zamkniętego katalogu i podlega ciągłym zmianom, doskonaleniu i adaptowaniu do potrzeb, celów, strategii, zadań i zmieniającego się otoczenia;
27) użytkownik – osobę, która uzyskała uprawnienie do dostępu i przetwarzania informacji w systemach informatycznych;
28) Właściciel Systemu – kierującego komórką organizacyjną GITD lub jego zastępcę, wskazanego w uzgodnieniu z Dyrektorem Generalnym GITD, odpowiedzialnego za zainicjowanie powstania systemu, ustalenie założeń i funkcjonalności systemu oraz określanie kierunków jego rozwoju, jak również zapewnienie jego poprawnego i nieprzerwanego działania, zgodnie z wymogami prawa oraz celami i potrzebami GITD i interesariuszy;
29) zabezpieczenie – działanie lub rozwiązanie, które ogranicza prawdopodobieństwo wystąpienia zagrożenia lub minimalizuje jego negatywne skutki oraz wpływa na osiągnięcie celów. Wyróżnia się trzy rodzaje zabezpieczeń:

a) organizacyjne (struktury organizacyjne, polityki, procedury postępowania, zarządzenia, instrukcje, regulaminy, klauzule w umowach, zakresy obowiązków pracowników, szkolenia, audyty, kontrole itp.),
b) techniczne (systemy bezpieczeństwa informatycznego, systemy kontroli dostępu, depozytory kluczy, urządzenia alarmowe, sygnalizacyjne lub monitoringu, oprogramowanie antywirusowe itp.),
c) fizyczne (ogrodzenie, drzwi, pomieszczenia plombowane, zamykane szafy, sejfy, strefy ochronne itp.) i środowiskowe (np.: bezpieczeństwo okablowania, klimatyzacja, systemy podtrzymania zasilania itp.);

30) zagrożenie – zdarzenie, zjawisko, działanie lub zaniechanie, które może skutkować naruszeniem integralności, dostępności, poufności informacji albo doprowadzić do szkody lub nieosiągnięcia celów GITD.

§ 3. 1. PBI jest obok PBT i PODO dokumentem stanowiącym podstawową dokumentację SZBI w GITD.

2. PBI objęte są wszystkie informacje wykorzystywane przez GITD, niezależnie od formy i nośnika przetwarzania lub dystrybucji (ustne, pisemne, nagrania audio i wideo), utrwalone na nośnikach elektronicznych, w systemach komputerowych oraz wytworzone w dokumentach, będące własnością GITD oraz powierzone w ramach umów lub porozumień z kontrahentami lub wykonawcami.

3. Przepisy PBI należy uwzględniać w procesie opracowania innej dokumentacji SZBI, w szczególności polityk, procedur, instrukcji i wytycznych.

4. Obowiązujące w GITD regulacje wewnętrzne należy procedować i wdrażać z uwzględnieniem założeń zapewniających ochronę aktywów, w szczególności aktywów informacyjnych.

5. PBI nie ingeruje w treść odrębnych SZBI, w tym certyfikowanych na zgodność z Polską Normą PN-ISO/IEC 27001, które funkcjonują lub mogą funkcjonować w GITD w odniesieniu do systemów informatycznych, a także w treść dokumentów wynikających z przepisów o ochronie informacji niejawnych oraz przepisów o zarządzaniu kryzysowym.

§ 4. PBI ma zastosowanie do wszystkich komórek organizacyjnych GITD i obejmuje zakresem nie tylko pomieszczenia użytkowane przez GITD, ale także miejsca i sytuacje, w których informacje związane z działalnością GITD są przetwarzane poza jego siedzibą, w szczególności w kontekście zdalnego korzystania z sieci komputerowej GITD, w tym telepracy.

§ 5. 1. Do przestrzegania PBI zobowiązane są wszystkie osoby korzystające z zasobów GITD, w szczególności:

1) pracownicy GITD;
2) osoby świadczące usługi, realizujące dostawy oraz wykonujący roboty budowlane na rzecz GITD na podstawie umów cywilnoprawnych;
3) eksperci oraz osoby odbywające praktykę, staż lub wolontariat, w zakresie określonym odpowiednio w umowie z ekspertem, umowie o odbywaniu praktyki lub stażu, programie praktyki lub stażu, porozumieniu o świadczeniu wolontariatu;
4) pracownicy podmiotów zewnętrznych realizujący inne, niż określone w pkt 2 – 3 usługi na rzecz GITD na podstawie zawartych umów i porozumień.

2. Za zapoznanie z PBI osób, o których mowa w ust. 1, odpowiada w przypadku:

1) nowo zatrudnionego pracownika GITD oraz pracowników aktualnie wykonujących obowiązki wynikające ze stosunku pracy na rzecz GITD – kierujący komórką organizacyjną GITD, w której pracownik będzie zatrudniony lub bezpośredni przełożony pracownika;
2) osób świadczących usługi na podstawie umów cywilnoprawnych – kierujący komórką organizacyjną GITD odpowiedzialny za realizację umowy zawartej z tą osobą;
3) stażystów, wolontariuszy, praktykantów i ekspertów – kierujący komórką organizacyjną GITD, w której będą odbywać staż, wolontariat, praktykę lub wykonywać pracę jako eksperci lub wyznaczona przez niego osoba;
4) pracowników podmiotów zewnętrznych, o których mowa w ust. 1 pkt 4 – kierujący komórką organizacyjną GITD odpowiedzialny za realizację umowy z podmiotem zewnętrznym.

3. Osoby, o których mowa w ust. 1, zobowiązane są do złożenia własnoręcznie podpisanego oświadczenia o zapoznaniu z treścią PBI przed rozpoczęciem wykonywania przez nie zadań służbowych. Wzór oświadczenia stanowi załącznik nr 1 do PBI.

4. Oświadczenie, o którym mowa w ust. 3, może również zostać złożone w formie dokumentu elektronicznego, opatrzonego podpisem zaufanym, osobistym lub kwalifikowanym podpisem elektronicznym, np. z wykorzystaniem e-usługi dostępnej na stronie: obywatel.gov.pl.

5. Oświadczenia, o których mowa w ust. 3 i 4:

1) w odniesieniu do osób, o których mowa w ust. 1 pkt 1 i 3, przechowywane są przez IOD;
2) w odniesieniu do osób, o których mowa w ust. 1 pkt 2, przechowywane są przy danej umowie cywilnoprawnej;
3) w odniesieniu do osób, o których mowa w ust. 1 pkt 4, przechowywane są przez komórkę organizacyjną GITD odpowiedzialną za umowę z podmiotem zewnętrznym, przy tej umowie.

6. Treść oświadczenia, o którym mowa w ust. 3, może podlegać modyfikacji i dostosowaniu do danej umowy.

7. Użytkowników serwisów internetowych i aplikacji mobilnych udostępnianych przez GITD obowiązują postanowienia właściwych dla tych serwisów polityk prywatności udostępnionych w tych serwisach i aplikacjach.

Rozdział 2

Zasady dotyczące bezpieczeństwa informacji

§ 6. 1. PBI realizowana jest w GITD poprzez:

1) zapewnienie odpowiedniej jakości procesów przetwarzania informacji, w szczególności skuteczności i adekwatności działania zabezpieczeń (lub ich grup) i środków chroniących przed nieuprawnionym ujawnieniem, odpowiednich warunków do ich użytkowania oraz sprawności i efektywności ich wykorzystywania;
2) pracowników posiadających odpowiednią wiedzę, umiejętności i doświadczenie adekwatne do powierzonych zadań;
3) ochronę fizyczną, techniczną i organizacyjną aktywów GITD przed dostępem osób nieupoważnionych, w szczególności przed nieuprawnionym wykorzystaniem, kradzieżą, uszkodzeniem, nieuprawnioną modyfikacją lub zniszczeniem;
4) zabezpieczenie systemów informatycznych eksploatowanych w GITD przed zagrożeniami;
5) zabezpieczenie aktywów GITD przed ich uszkodzeniem lub zniszczeniem w wyniku pożaru, zalania, ataku terrorystycznego, zjawisk naturalnych lub innych zagrożeń;
6) zapewnienie ciągłości działania procesów przetwarzania informacji w GITD;
7) zapewnienie możliwości sprawnego odtworzenia aktywów w przypadku ich zniszczenia;
8) zapewnienie gotowości do reakcji na sytuację awaryjną lub kryzysową;
9) zapewnienie rozwiązań organizacyjnych i systemowych regulujących zasady i sposób zarządzania bezpieczeństwem informacji;
10) zapewnienie spójnej polityki informacyjnej GITD;
11) zapewnienie właściwych zapisów w zakresie bezpieczeństwa informacji, w szczególności stosowanie klauzul poufności w umowach cywilnoprawnych z kontrahentami lub wykonawcami, gdy wymaga tego przedmiot lub specyfika umowy;
12) zapewnienie pracownikom szkoleń i innych akcji promocyjno-edukacyjnych z zakresu bezpieczeństwa informacji;
13) zapewnienie działań kontrolnych w zakresie przestrzegania zasad określonych w GITD;
14) przestrzeganie zasad bezpieczeństwa informacji, o których mowa w § 8.

2. Stosowanie zabezpieczeń lub ich grup powinno uwzględniać następujące zasady:

1) zabezpieczenia powinny być adekwatne do wymogów prawnych oraz wyników audytów i analiz ryzyka bezpieczeństwa informacji;
2) zabezpieczenia fizyczne, techniczne i organizacyjne powinny uzupełniać się wzajemnie (grupy zabezpieczeń), zapewniając wymagany poziom bezpieczeństwa informacji;
3) w doborze zabezpieczeń należy kierować się w szczególności:
   a) adekwatnością,
   b) zaleceniami Polskiej Normy PN-ISO 27002,
   c) wynikami szacowania ryzyka;
4) świadomość pracowników w zakresie bezpieczeństwa informacji powinna być doskonalona, w szczególności poprzez różne formy podnoszenia kwalifikacji;
5) należy unikać niepotrzebnego dublowania zabezpieczeń, przy uwzględnieniu racjonalnego gospodarowania środkami publicznymi, optymalizacji potrzeb oraz ograniczeń i uwarunkowań prawno-organizacyjnych GITD;
6) należy podejmować działania na rzecz utrzymania standardów współpracy GITD z osobami i podmiotami zewnętrznymi, poprzez stosowanie zasad regulujących kwestie poufności w ramach realizacji umów, porozumień, listów intencyjnych i innych form relacji, obowiązujących strony również po ustaniu współpracy.

3. Szczegółowe metody i sposoby implementacji zabezpieczeń, o których mowa w ust. 1, mogą być określone w innych dokumentach stanowiących dokumentację SZBI.

§ 7. 1. Skuteczność SZBI zachowuje się przy jednoczesnym zastosowaniu i uzupełnianiu się elementów regulujących obszary bezpieczeństwa fizycznego i środowiskowego, technicznego, organizacyjnego.

2. Poziom bezpieczeństwa informacji jest odpowiedni wówczas, gdy spełnione są następujące warunki:
1) dokonano szacowania ryzyka w odniesieniu do bezpieczeństwa informacji;
2) wdrożono skuteczne zabezpieczenia wymagane przepisami prawa i PBI.

§ 8. 1. W GITD stosuje się następujące zasady dotyczące bezpieczeństwa informacji:
1) wiedzy koniecznej (ograniczonego dostępu do informacji) – pracownicy posiadają dostęp tylko do tych informacji, które są konieczne do realizacji powierzonych im zadań. Zasada ta dotyczy głównie informacji wrażliwych oraz podlegających prawnej ochronie (m.in.: tajemnica przedsiębiorstwa, tajemnica skarbowa, dane osobowe). Zasada ta ma ograniczone znaczenie dla pewnych grup informacji, w szczególności informacji dostępnych publicznie;

2) indywidualnej odpowiedzialności – za utrzymanie odpowiedniego poziomu bezpieczeństwa poszczególnych aktywów lub ich elementów odpowiadają konkretne osoby, w zakresie nałożonych obowiązków i nadanych uprawnień. Zasada ta dotyczy np. wydruków z systemu centralnego wydruku tj. każda osoba odpowiada za sporządzony przez siebie wydruk;
3) niewygody uzasadnionej – bezpieczeństwo co do zasady opiera się na ograniczeniach oraz jest niewygodne. Środki ochrony nie mogą nadmiernie utrudniać realizacji celów i zadań GITD;
4) czystego biurka i czystego ekranu:
   a) 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.,
   b) 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;
5) separacji obowiązków – pojedyncze osoby nie mogą wykonywać krytycznych zadań w całości;
6) 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. Zasada ta ma ograniczone znaczenie dla pewnych grup informacji, np. informacji dostępnych publicznie;
7) obecności koniecznej – prawo 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. Szczegółowe zasady ochrony fizycznej obiektów i pomieszczeń użytkowanych przez GITD określają wewnętrzne dokumenty i instrukcje GITD oraz dokumenty, instrukcje i regulaminy udostępniane przez administratora / właściciela budynku, natomiast w odniesieniu do ochrony informacji niejawnych - Plan ochrony informacji niejawnych w Głównym Inspektoracie Transportu Drogowego, w tym w razie wprowadzenia stanu nadzwyczajnego. Ogólne zasady bezpieczeństwa fizycznego określa załącznik nr 2 do PBI;
8) zamykania pomieszczeń – niedopuszczalne jest pozostawienie pod nieobecność pracownika niezabezpieczonego pomieszczenia służbowego, zarówno w godzinach pracy, jak i po jej zakończeniu. Na zakończenie dnia pracy ostatnia wychodząca z pomieszczenia osoba jest

zobowiązana zamknąć wszystkie okna i drzwi oraz zabezpieczyć klucze do pomieszczenia. Szczegółowe zasady ochrony fizycznej obiektów i pomieszczeń użytkowanych przez GITD określają wewnętrzne dokumenty i instrukcje GITD oraz dokumenty, instrukcje i regulaminy udostępniane przez administratora / właściciela budynku, natomiast odniesieniu do ochrony informacji niejawnych - Plan ochrony informacji niejawnych w Głównym Inspektoracie Transportu Drogowego, w tym w razie wprowadzenia stanu nadzwyczajnego. Ogólne zasady bezpieczeństwa fizycznego określa załącznik nr 2 do PBI;

9) nadzorowania dokumentów – po godzinach pracy wszystkie dokumenty zawierające informacje podlegające ochronie należy przechowywać w miejscach zabezpieczonych przed dostępem osób nieuprawnionych;
10) stałej gotowości – niedopuszczalne jest tymczasowe wyłączanie mechanizmów zabezpieczających systemy funkcjonujące w GITD bez zastosowania alternatywnych mechanizmów. Systemy powinny być sprawne i przygotowane na zidentyfikowane zagrożenia;
11) zachowania prywatności kont w systemach – każdy użytkownik zobowiązany jest do pracy w systemach informatycznych na przypisanych lub udostępnionych mu kontach. Zabronione jest udostępnianie własnych kont osobom trzecim. Poufność ta obejmuje również karty wykorzystywane w systemach kontroli dostępu funkcjonujących w GITD;
12) poufności informacji uwierzytelniających – każdy użytkownik zobowiązany jest do zachowania poufności udostępnionych mu haseł, kodów dostępu, kodów PIN, w szczególności do systemów informatycznych;
13) legalnego oprogramowania – na stacjach roboczych zainstalowane jest wyłącznie legalne oprogramowanie. Oprogramowanie powinno posiadać możliwość automatycznej aktualizacji bez dodatkowych działań ze strony użytkownika;
14) zgłaszania incydentów oraz incydentów bezpieczeństwa informacji – każdy użytkownik ma obowiązek niezwłocznie zgłosić wystąpienie lub podejrzenie wystąpienia incydentu mającego lub mogącego mieć wpływ na cyberbezpieczeństwo lub bezpieczeństwo informacji w GITD;
15) automatyzacji kopii zapasowych – procesy tworzenia kopii zapasowych powinny być odpowiednio zaplanowane z uwzględnieniem wymogów prawnych i potrzeb GITD, jak również powinny być zautomatyzowane oraz niemożliwe do przerwania;
16) ochrony nośników danych – dane kopiowane na nośniki i wynoszone poza pomieszczenia użytkowane przez GITD powinny być odpowiednio zabezpieczone w czasie transportu i przechowywania, co najmniej poprzez szyfrowanie. W szczególności dotyczy to danych prawnie chronionych takich jak tajemnica przedsiębiorstwa, tajemnica skarbowa, dane osobowe oraz innych danych wrażliwych (np. tajemnica GITD);

17) adekwatności zabezpieczeń – używane mechanizmy zabezpieczeń powinny być adekwatne do zagrożeń, podatności, wartości aktywów oraz innych istotnych okoliczności;
18) kompleksowości ochrony – ochrona aktywów systemu przetwarzania informacji powinna opierać się na stosowaniu różnych mechanizmów ochrony, w tym ochrony prawnej, fizycznej, technicznej oraz organizacyjnej;
19) ochrony niezbędnej – minimalny wymagany poziom bezpieczeństwa informacji wynika z obowiązujących przepisów prawa. Zastosowanie wyższych poziomów bezpieczeństwa informacji uzasadniają szczególne potrzeby GITD i wyniki szacowania ryzyka;
20) bezpiecznej współpracy z podmiotami zewnętrznymi – dokumenty regulujące współpracę powinny zawierać stosowne klauzule bezpieczeństwa, w tym o zachowaniu poufności, zasadach postępowania z pozyskaną informacją, niszczenia lub zwrotu dokumentacji po ich wykorzystaniu, gdy wymaga tego przedmiot lub specyfika umowy;
21) doskonalenia – SZBI jest stale monitorowany i dostosowywany do zmieniających się warunków wewnętrznych i zewnętrznych;
22) podwyższonego poziomu ochrony zbiorów informacji – w szczególnie uzasadnionych przypadkach zbiór informacji powinien być bardziej chroniony niż poszczególne informacje, które się na niego składają;
23) czystej tablicy – po zakończonym spotkaniu należy uprzątnąć wszystkie materiały oraz wyczyścić tablice;
24) czystego kosza – dokumenty papierowe, z wyjątkiem materiałów zawierających informacje jawne, muszą być niszczone w sposób uniemożliwiający ich odczytanie. Niedopuszczalne jest wyrzucanie dokumentów zawierających informacje wrażliwe i prawnie chronione, o których mowa w § 11 ust. 1 pkt 2 i 3, do zwykłego kosza. W celu zniszczenia takich dokumentów należy korzystać z udostępnionych przez GITD niszczarek. Niszczenie nośników elektronicznych należy przeprowadzić zgodnie z zasadami określonymi w PBT lub odrębnej dokumentacji SZBI systemu informatycznego, jeżeli taką ustanowiono.

2. Katalog zasad, o których mowa w ust. 1 jest otwarty i może być rozszerzony lub uszczegółowiony w innych dokumentach stanowiących dokumentację SZBI.

3. Podstawowe zasady bezpieczeństwa informacji przy współpracy z podmiotami trzecimi zawiera załącznik nr 3 do PBI.

4. Podstawowe zasady bezpieczeństwa osobowego określa załącznik nr 4 do PBI.

5. Podstawowe zasady ochrony danych osobowych określa PODO.

6. Podstawowe zasady bezpieczeństwa informatycznego, w tym w odniesieniu do ochrony danych osobowych przetwarzanych w systemach informatycznych GITD, określa PBT.

7. PBT nie obejmuje systemów informatycznych, dla których ustanowiono odrębne SZBI, w tym SZBI certyfikowane za zgodność z normą PN-ISO/IEC 27001. Powyższe wyłączenie obejmuje również system informatyczny wykorzystywany do świadczenia usługi kluczowej w rozumieniu ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

Rozdział 3

Odpowiedzialność i uprawnienia w zakresie bezpieczeństwa informacji

§ 9. 1. Właściwe zarządzanie bezpieczeństwem informacji w GITD zapewnia wewnętrzna struktura organizacyjna, w której skład wchodzą, w szczególności:

1) Główny Inspektor;
2) Zastępcy Głównego Inspektora;
3) Dyrektor Generalny GITD;
4) kierujący komórkami organizacyjnymi GITD i ich zastępcy;
5) IOD;
6) koordynatorzy do spraw ochrony danych osobowych (delegatury terenowe);
7) Pełnomocnik do spraw bezpieczeństwa informacji;
8) Zespół do spraw Bezpieczeństwa Informacji;
9) Zespół Inspektora Ochrony Danych;
10) Pełnomocnik do spraw bezpieczeństwa cyberprzestrzeni;
11) Pełnomocnik do spraw Ochrony Informacji Niejawnych;
12) Zespół Zarządzania Kryzysowego;
13) Inspektor Bezpieczeństwa Teleinformatycznego systemów informatycznych przeznaczonych do przetwarzania informacji niejawnych, o którym mowa w ustawie z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych;
14) ASI;
15) AMS;
16) użytkownicy.

2. Dane kontaktowe osób pełniących funkcje, o których mowa w ust. 1 pkt 5-15, mogą być opublikowane w wewnętrznym zasobie sieciowym GITD.

3. Pełnomocnik do spraw bezpieczeństwa informacji jest osobą wyznaczoną przez Głównego Inspektora do zapewnienia koordynacji spraw z zakresu bezpieczeństwa informacji w GITD.

4. Pełnomocnik do spraw bezpieczeństwa cyberprzestrzeni jest jednocześnie osobą wyznaczoną przez Głównego Inspektora do utrzymywania kontaktów GITD z podmiotami krajowego systemu

cyberbezpieczeństwa, o którym mowa w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

5. Odpowiedzialność za bezpieczeństwo informacji w GITD ponoszą wszystkie osoby, o których mowa w § 5 ust. 1, w zakresie odpowiednim do nałożonych na nich obowiązków, posiadanych uprawnień lub postanowień określonych w umowach, porozumieniach i innych pisemnych formach współpracy regulujących obszar bezpieczeństwa informacji.

6. Niezależnie od zakresu, o którym mowa w ust. 5, pracownicy są zobowiązani do przestrzegania obowiązku zachowania tajemnicy pracodawcy zgodnie z przepisami prawa pracy.

§ 10. 1. Główny Inspektor:

1) zarządza bezpieczeństwem informacji w GITD oraz decyduje o celach i środkach przetwarzania informacji, w tym danych osobowych, jako ich administrator;
2) zatwierdza podstawowe dokumenty SZBI, w tym PBT, PODO;
3) wyznacza lub powołuje m.in.:
   a) IOD,
   b) Pełnomocnika do spraw Ochrony Informacji Niejawnych,
   c) Pełnomocnika do spraw bezpieczeństwa cyberprzestrzeni,
   d) Pełnomocnika do spraw bezpieczeństwa informacji,
   e) Zespół do spraw Bezpieczeństwa Informacji,
   f) Zespół Inspektora Ochrony Danych,
   g) Zespół Zarządzania Kryzysowego.

2. Zastępcy Głównego Inspektora oraz Dyrektor Generalny GITD odpowiadają, w zakresie swojej właściwości, za nadzorowanie bezpieczeństwa informacji w GITD.

3. Dyrektor Generalny GITD:

1) zapewnia okresowy audyt wewnętrzny w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok realizowany przez komórkę właściwą do spraw audytu wewnętrznego GITD lub uprawnione podmioty zewnętrzne;
2) akceptuje wyniki przeglądów SZBI oraz wyniki szacowania ryzyka;
3) określa kierującym komórkami organizacyjnymi GITD zadania mające na celu zapewnienie bezpieczeństwa informacji, w przypadku wystąpienia takiej potrzeby;
4) egzekwuje odpowiedzialność pracowników GITD za naruszenia związane z bezpieczeństwem informacji, w zakresie adekwatnym do nałożonych na nich obowiązków i posiadanych uprawnień.

4. Zadania Zespołu do spraw Bezpieczeństwa Informacji określają odrębne przepisy wewnętrzne.

5. Pełnomocnik do spraw bezpieczeństwa informacji:

1) zapewnia koordynację spraw z zakresu bezpieczeństwa informacji;
2) nadzoruje opracowanie dokumentacji SZBI;
3) współpracuje z kierującym komórką organizacyjną GITD właściwą do spraw szkoleń, o którym mowa w ust. 8, przy realizacji szkoleń z zakresu bezpieczeństwa informacji;
4) inicjuje oraz nadzoruje działania wdrożeniowe, korygujące i zapobiegawcze w zakresie bezpieczeństwa informacji;
5) nadzoruje działania związane z wykrytymi incydentami bezpieczeństwa informacji;
6) organizuje przeglądy SZBI, nie rzadziej niż raz na dwa lata, oraz nadzoruje realizację ustaleń wynikających z tych przeglądów;
7) jest zobowiązany do:
   a) wydawania zaleceń w zakresie związanym z funkcjonowaniem SZBI,
   b) wydawania zaleceń i wytycznych dla pracowników GITD związanych z bezpieczeństwem informacji i zagrożeniami tego bezpieczeństwa, w porozumieniu i we współpracy z pełnomocnikiem do spraw bezpieczeństwa cyberprzestrzeni oraz IOD,
   c) występowania do pracowników GITD o złożenie wyjaśnień, w szczególności w przypadku wystąpienia incydentów bezpieczeństwa informacji i nieprawidłowości w zakresie funkcjonowania SZBI,
   d) podejmowania działań w kwestiach bezpieczeństwa informacji, w zakresie niezastrzeżonym do kompetencji innych osób,
   e) rekomendowania rozwiązań organizacyjno-technicznych zwiększających skuteczność zarządzania w obszarze SZBI.

6. Zadania IOD[2)] określa art. 39 RODO oraz art. 47 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.

7. Uprawnienia i obowiązki:

1) Pełnomocnika do spraw bezpieczeństwa cyberprzestrzeni,
2) Pełnomocnika do spraw ochrony informacji niejawnych,
3) Inspektora Bezpieczeństwa Teleinformatycznego,
4) Zespołu Zarządzania Kryzysowego

– określają odrębne przepisy i upoważnienia.

8. Kierujący komórką organizacyjną GITD właściwą do spraw szkoleń działa na rzecz zapewnienia pracownikom GITD szkoleń w zakresie bezpieczeństwa informacji.

[2)] przepis ten określa również zadania osoby zastępującej IOD, o której mowa w art. 46 ust. 4 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.

9. Dyrektor Generalny GITD bądź osoba przez niego upoważniona zapewnia realizację audytu w zakresie bezpieczeństwa informacji, zgodnie z wynikami analizy ryzyka i przyjętego stopnia apetytu na ryzyko nie rzadziej jednak niż raz w roku, zgodnie z § 20 KRI ust. 2 pkt 14.

10. Kierujący komórką organizacyjną GITD właściwą do spraw prowadzenia polityki medialnej oraz realizacji zadań związanych z działalnością edukacyjną oraz promocyjną i informacyjną GITD działa na rzecz zapewnienia skutecznej komunikacji wewnętrznej i zewnętrznej w zakresie bezpieczeństwa informacji w GITD zgodnie z przepisami prawa i polityką medialną GITD.

11. Kierujący komórką organizacyjną GITD właściwą do spraw koordynowania udostępniania informacji publicznej działa na rzecz zapewnienia realizacji obowiązku udostępniania informacji publicznej zgodnie z przepisami prawa, z uwzględnieniem bezpieczeństwa informacji przetwarzanych w GITD.

12. Kierujący komórką organizacyjną GITD właściwą do spraw ochrony i monitoringu nieruchomości będących w trwałym zarządzie GITD oraz prawidłowego funkcjonowania zabezpieczeń przed nieuprawnionym dostępem do stref ograniczonego dostępu w GITD zapewnia niezbędne dla bezpieczeństwa informacji zabezpieczenia oraz prawidłowe funkcjonowanie tych zabezpieczeń.

13. Kierujący komórką organizacyjną GITD właściwą do spraw informatyki zapewnia bezpieczeństwo systemów informatycznych GITD i łączności telefonicznej w GITD, jak również wspiera Właścicieli Systemów w budowie, rozwoju i utrzymaniu systemów będących w ich właściwości merytorycznej, z zastrzeżeniem ust. 14.

14. Kierujący komórką organizacyjną GITD właściwą do spraw KSPO zapewnia realizację zadań związanych z wdrażaniem i utrzymaniem infrastruktury teleinformatycznej KSPO, w tym z zachowaniem optymalnego stanu zabezpieczeń teleinformatycznych, wdrażaniem i utrzymaniem infrastruktury przydrożnej KSPO, wdrażaniem i utrzymaniem procesów wsparcia czynności kontrolnych, w tym budową nowych narzędzi na potrzeby realizacji przez Głównego Inspektora czynności kontrolnych, wdrażaniem i utrzymaniem procesów obsługi użytkownika, wdrażaniem i utrzymaniem procesów obsługi transakcji finansowych w KSPO.

15. Właściciele Systemów zapewniają, w zakresie swojej właściwości, bezpieczeństwo systemów informatycznych GITD oraz merytoryczny nadzór nad ich działaniem.

16. Osoby reprezentujące GITD wskazane w umowach cywilnoprawnych, odpowiadają za prawidłowość ich realizacji.

17. Kierujący komórkami organizacyjnymi GITD, w zakresie swojej właściwości, odpowiadają za:

1) wdrożenie i przestrzeganie PBI, w tym przez osoby i podmioty określone w § 5 ust. 1 pkt 2 - 4;
2) ochronę aktywów;

3) szacowanie ryzyka bezpieczeństwa informacji;
4) realizację procedur zapewniających ciągłość funkcjonowania komórki w sytuacjach awaryjnych i kryzysowych, w szczególności przez:
   a) zarządzanie wiedzą i kompetencjami podległych pracowników w taki sposób, aby zapewnić ciągłość realizacji zadań (zastępowalność),
   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 urlopami i delegacjami podległych pracowników w taki sposób, aby dostępny był przynajmniej jeden pracownik posiadający kompetencje niezbędne do wykonania danego zadania;
5) umożliwienie pracownikom udziału w organizowanych szkoleniach z zakresu bezpieczeństwa informacji, teleinformatycznego, cyberbezpieczeństwa, ochrony danych osobowych oraz innych wydarzeniach podnoszących ich wiedzę i umiejętności z tego zakresu;
6) właściwy tryb zgłaszania i postępowania w sytuacji wystąpienia incydentów oraz incydentów bezpieczeństwa informacji, zgodnie z wewnętrznymi regulacjami w tym zakresie, w tym przez osoby i podmioty trzecie, z którymi GITD ma zawarte umowy lub inne formy współpracy, które są w zakresie właściwości danej komórki;
7) w przypadku Właścicieli Systemów:
   a) pisemne wyznaczenie pracowników w podległej komórce organizacyjnej odpowiedzialnych technicznie oraz merytorycznie za systemy informatyczne (ASI oraz AMS),
   b) zatwierdzenie odrębnych SZBI dla systemów informatycznych w przypadku ich ustanowienia,
   c) realizację zadań określonych w PBT;
8) bieżącą weryfikację zgodności regulacji wewnętrznych i przyjętych zasad bezpieczeństwa oraz ich stosowania z przepisami prawa. Weryfikacja ta dotyczy również zgodności z wymaganiami prawnymi, regulacyjnymi i umownymi, związanymi z prawami własności intelektualnej i użytkowaniem prawnie zastrzeżonego oprogramowania.

18. ASI odpowiada za techniczne utrzymanie ciągłości działania zasobów informatycznych, przede wszystkim systemów informatycznych GITD, m.in. utrzymanie infrastruktury i oprogramowania, wykonywanie kopii bezpieczeństwa, oraz innych zadań szczegółowo określonych i opisanych w PBT lub odrębnym SZBI systemu informatycznego.

19. AMS odpowiada za merytoryczne funkcjonowanie zasobu informatycznego, tj. weryfikację i potwierdzanie zgodności z wymaganiami funkcjonalnymi oraz proces zarządzania uprawnieniami

użytkowników obejmujący zakładanie / zmianę / blokowanie / usuwanie kont, nadawanie, odbieranie, modyfikację uprawnień, jak również okresowe przeglądy kont i uprawnień w systemie.

20. Użytkownicy odpowiadają w szczególności za:

1) przestrzeganie PBI oraz PODO i PBT w zakresie, jaki ich dotyczy;
2) ochronę aktywów, w zakresie swojej właściwości;
3) niezwłoczne reagowanie w przypadku wystąpienia lub podejrzenia wystąpienia incydentu oraz incydentu bezpieczeństwa informacji oraz postępowanie zgodnie z wewnętrznymi regulacjami w tym zakresie;
4) zabezpieczanie informacji przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów prawa oraz nieuprawnioną zmianą, utratą, uszkodzeniem lub zniszczeniem;
5) zachowanie w tajemnicy informacji pozyskanych w ramach wykonywania obowiązków służbowych w GITD oraz przestrzegania zasad bezpiecznego ich przetwarzania, w tym w systemach informatycznych, w zakresie nadanych uprawnień lub wskazanym w upoważnieniu do przetwarzania danych osobowych.

21. Odpowiedzialność i uprawnienia w odniesieniu do bezpieczeństwa informacji w systemach informatycznych, w których ustanowiono odrębny SZBI, w tym SZBI certyfikowany za zgodność z normą PN-ISO/IEC 27001, określa dokumentacja SZBI tych systemów.

22. Wzór pisemnego wyznaczenia pracownika, o którym mowa w ust. 17 pkt 7 lit. a zawiera załącznik nr 5 do PBI.

Rozdział 4

Klasyfikacja informacji i zasady postępowania z informacjami

§ 11. 1. W GITD przyjmuje się następującą klasyfikację informacji oraz ich oznaczenie:

1) informacja jawna, w tym udostępniana w trybie dostępu do informacji publicznej – informacje jawne powszechnie dostępne oraz informacje których obowiązek udostępniania wynika z przepisów prawa, w szczególności informacje publiczne w rozumieniu ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej z wyłączeniem informacji, do których dostęp podlega ograniczeniom w niej wskazanym. Informacje udostępniane w szczególności na stronach internetowych GITD;
2) informacja prawnie chroniona – informacje stanowiące dane osobowe podlegające ochronie na mocy przepisów o ochronie danych osobowych oraz informacje przekazane GITD przez przedsiębiorcę, co do których podjął on działania w celu zachowania ich w poufności, w szczególności nieujawnione do wiadomości publicznej informacje techniczne, technologiczne,

organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą (tajemnica przedsiębiorstwa) oraz informacje chronione na mocy ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (uregulowane odrębnymi przepisami), oraz inne informacje chronione z mocy prawa (np. tajemnica skarbowa). Dokumenty przychodzące do GITD zawierające informacje sklasyfikowane w szczególności jako „tajemnica przedsiębiorstwa" oraz „tajemnica skarbowa" powinny być oznaczone, np. na pierwszej stronie w przypadku dokumentów papierowych lub w nazwie pliku w przypadku dokumentów elektronicznych odpowiednio klauzulą: „TAJEMNICA PRZEDSIĘBIORSTWA". Dokumenty oznaczone klauzulą „TAJEMNICA SKARBOWA" nie powinny być przesyłane do GITD faksem oraz poprzez pocztę elektroniczną, w tym poprzez Elektroniczną Platformę Usług Administracji Publicznej – ePUAP. Sposób postępowania z informacjami klasyfikowanymi jako informacje niejawne określają właściwe przepisy oraz regulacje wewnętrzne, m.in. Plan ochrony informacji niejawnych, w tym w razie wprowadzenia stanu nadzwyczajnego. W tej kategorii informacji uwzględnia się dokumenty publiczne w rozumieniu ustawy z dnia 22 listopada 2018 r. o dokumentach publicznych, przy czym zasady postępowania i ochrony dokumentów publicznych określono szczegółowo we wskazanej ustawie oraz aktach wykonawczych wydanych na jej podstawie oraz innych wewnętrznych aktach normatywnych, zasady określone w dokumentacji SZBI w GITD należy stosować uzupełniająco;

3) informacja wrażliwa (tajemnica GITD) – informacje wewnętrzne GITD, wytworzone w GITD lub na jego rzecz, niewchodzące w zakres informacji zaklasyfikowanych do pozostałych grup. Są to informacje dostępne wewnątrz GITD i przeznaczone do użytku wewnętrznego. Informacje te mogą być udostępniane stronom trzecim (osobom lub podmiotom) na zasadzie „wiedzy uzasadnionej", w szczególności w związku z realizacją usług na podstawie zawartych umów, porozumień, itp. Dokumenty zawierające informacje sklasyfikowane jako tajemnica GITD, w szczególności te udostępniane stronom trzecim, powinno się oznaczać co najmniej na pierwszej stronie (np.: w nagłówku lub stopce dokumentu) w przypadku dokumentów papierowych, lub w nazwie pliku w przypadku dokumentów elektronicznych, informacją np.: „tajemnica GITD", „do użytku wewnętrznego";

4) informacja wymagająca klasyfikacji – informacje, których ewentualne udostępnienie poza GITD wymaga złożenia stosownego wniosku oraz analizy prawnej dotyczącej możliwości udostępnienia informacji wskazanej we wniosku oraz analizy ewentualnych konsekwencji związanych z jej udostępnieniem.

2. Wprowadzenie klasyfikacji informacji, o której mowa w ust. 1, nie powoduje konieczności fizycznego oznaczania informacji już udokumentowanych, dokonuje się w nich jedynie odwzorowania

literowo-cyfrowego zgodnie z instrukcją kancelaryjną lub oznaczenia identyfikującego dokument w systemie elektronicznego zarządzania dokumentacją.

§ 12. W GITD przyjmuje się następujące zasady postępowania z informacjami sklasyfikowanymi jako:

1) informacja jawna:
   a) przetwarzanie, przechowywanie, przekazywanie – w sposób gwarantujący zachowanie integralności i dostępności informacji,
   b) zmiana klasyfikacji i udostępnianie – na zasadach i w trybie przewidzianym przepisami prawa,
   c) niszczenie – zgodnie z wymogami określonymi w przepisach prawa lub zawartych przez GITD umowach, instrukcją kancelaryjną oraz niniejszą PBI;
2) informacja prawnie chroniona:
   a) przetwarzanie – w sposób gwarantujący zapewnienie bezpieczeństwa informacji, ze szczególnym uwzględnieniem atrybutów integralności, dostępności i poufności oraz innych atrybutów bezpieczeństwa, które są wymagane dla danej informacji chronionej na podstawie przepisów prawa,
   b) przechowywanie – w sposób gwarantujący zapewnienie bezpieczeństwa informacji,
   c) przekazywanie – wyłącznie osobom uprawnionym, w sposób gwarantujący zachowanie integralności i poufności oraz zgodnie z wymaganiami określonymi w przepisach prawa lub zawartych przez GITD umowach,
   d) zmiana klasyfikacji – zgodnie z wymaganiami określonymi w przepisach prawa lub zawartych przez GITD umowach,
   e) udostępnianie – wyłącznie uprawnionym osobom lub podmiotom po uzyskaniu zgody kierującego właściwą komórką organizacyjną GITD lub jego zastępcy,
   f) niszczenie – zgodnie z wymogami określonymi w przepisach prawa lub zawartych przez GITD umowach oraz instrukcją kancelaryjną;
3) informacja wrażliwa:
   a) przetwarzanie – w sposób gwarantujący zapewnienie bezpieczeństwa informacji, ze szczególnym uwzględnieniem atrybutów integralności, dostępności i poufności,
   b) przechowywanie – w sposób gwarantujący zapewnienie bezpieczeństwa informacji,
   c) przekazywanie – wyłącznie osobom uprawnionym (pracownikom GITD, osobom/pracownikom podmiotów, z którymi GITD zawarło umowy), w sposób

gwarantujący zachowanie integralności i dostępności informacji oraz zgodnie z wymaganiami określonymi w przepisach prawa lub zawartych przez GITD umowach,

d) zmiana klasyfikacji – możliwa po podjęciu decyzji przez uprawnione osoby oraz zgodnie z wymaganiami określonymi w przepisach prawa lub zawartych przez GITD umowach,

e) udostępnianie – wyłącznie po uzyskaniu zgody kierującego właściwą komórką organizacyjną GITD lub jego zastępcy,

f) niszczenie – zgodnie z wymogami określonymi w przepisach prawa lub zawartych przez GITD umowach oraz instrukcją kancelaryjną;

4) informacja wymagająca klasyfikacji:

a) przetwarzanie – w sposób gwarantujący zachowanie integralności, dostępności i poufności informacji,

b) przechowywanie – w sposób gwarantujący zapewnienie bezpieczeństwa informacji,

c) przekazywanie – możliwe wysyłanie adresatom zewnętrznym po dokonaniu analizy prawnej dotyczącej możliwości udostępnienia informacji oraz analizy ewentualnych konsekwencji z tym związanych. Przekazywanie wewnątrz GITD na zasadach określonych przez kierującego właściwą komórką organizacyjną GITD lub jego zastępcę,

d) zmiana klasyfikacji – po dokonaniu analizy w tym zakresie,

e) udostępnianie – wyłącznie po uzyskaniu zgody kierującego właściwą komórką organizacyjną GITD lub jego zastępcy,

f) niszczenie – zgodnie z instrukcją kancelaryjną.

4. Klasyfikacja informacji w systemach informatycznych, w których ustanowiono odrębny SZBI, w tym SZBI certyfikowany za zgodność z normą PN-ISO/IEC 27001, odbywa się w trybie przewidzianym w dokumentacji tych systemów.

5. Podstawowe zasady postępowania z dokumentami papierowymi określa załącznik nr 6 do PBI.

Rozdział 5

Naruszenia bezpieczeństwa informacji

§ 13. 1. Każde zdarzenie związane z naruszeniem lub możliwością naruszenia bezpieczeństwa informacji podlega obowiązkowemu zgłoszeniu.

2. Szczegółowe zasady zgłaszania, obsługi oraz odpowiedzialności za rozwiązywanie incydentów oraz incydentów bezpieczeństwa informacji określa załącznik nr 7 do PBI. Zasady te obowiązują podmioty, o których mowa w § 5 ust. 1.

3. Za przestrzeganie określonych w § 2 załącznika nr 7 do PBI zasad zgłaszania incydentów i naruszeń przez osoby i podmioty zewnętrzne, o których mowa w § 5 ust. 1 pkt 2 - 4, w tym za ustalenie

zasad współpracy zapewniających dochowanie obowiązku zgłoszenia naruszenia bezpieczeństwa informacji, odpowiadają właściwi kierujący komórkami organizacyjnymi GITD lub osoby wskazane w umowie lub porozumieniu odpowiedzialne za realizację tej umowy, czy porozumienia. Zasady współpracy mogą być określone w umowie lub porozumieniu lub w ramach bieżącej współpracy przy realizacji umowy, czy porozumienia.

Rozdział 6

Szacowanie ryzyka

§ 14. 1. W obszarze bezpieczeństwa informacji szacowanie ryzyka jest obligatoryjne i przeprowadza się je cykliczne, nie rzadziej niż raz w roku.

2. Szacowanie ryzyka powinno być dodatkowo realizowane zgodnie z potrzebami, w szczególności przed opracowaniem dokumentacji bezpieczeństwa dla danego obszaru lub systemu informatycznego oraz po wystąpieniu istotnych zmian w danym obszarze lub systemie informatycznym.

3. Szacowanie ryzyka przeprowadza się w oparciu o zasady określone w załącznikach nr 8 i 9 do PBI.

4. Szacowanie ryzyka należy udokumentować.

5. Szacowanie ryzyka w systemach informatycznych, w których ustanowiono odrębny SZBI, w tym SZBI certyfikowany za zgodność z Polską Normą PN-ISO/IEC 27001, odbywa się w trybie przewidzianym w dokumentacji tych systemów.

6. Szacowanie ryzyka obejmuje swoim zakresem ocenę skutków ochrony danych osobowych określoną w obowiązujących przepisach dotyczących ochrony tych danych i zawiera co najmniej zakres określony w art. 35 ust. 7 RODO. Do oceny skutków ochrony danych stosuje się również zalecenia, wytyczne i porady Prezesa Urzędu Ochrony Danych Osobowych.

7. Wyniki szacowania ryzyka podlegają akceptacji Dyrektora Generalnego GITD.

Rozdział 7

Postanowienia końcowe

§ 15. Działania audytowe, przeglądy, informacje o stwierdzonych niezgodnościach oraz działaniach korygujących podlegają obowiązkowemu dokumentowaniu.

§ 16. Dokumentacja z zakresu bezpieczeństwa informacji, o której mowa w § 3 ust. 3, jest wprowadzana odrębnymi regulacjami.

§ 17. 1. W terminie miesiąca od dnia wejścia w życie PBI osoby, o których mowa w § 5 ust. 1 pkt 1 i 3, mają obowiązek zapoznać się z jej treścią, zgodnie z trybem określonym w § 5 ust. 2 – 7.

2. Osoby wyznaczone do współpracy lub kierujący komórkami organizacyjnymi GITD, odpowiedzialni za realizację zawartych umów czy porozumień, o których mowa w § 5 ust. 1 pkt 2 - 4, są zobowiązani zapewnić zgłaszanie naruszeń bezpieczeństwa informacji w przypadku wystąpienia takich naruszeń w toku realizacji umowy czy porozumienia.

Załącznik nr 1 do Polityki Bezpieczeństwa Informacji
Głównego Inspektoratu Transportu Drogowego

Oświadczenie o zapoznaniu się z Polityką Bezpieczeństwa Informacji Głównego Inspektoratu Transportu Drogowego oraz o zachowaniu poufności

Niniejszym oświadczam, że zostałam/em* zapoznana/y* z Polityką Bezpieczeństwa Informacji Głównego Inspektoratu Transportu Drogowego oraz przepisami i podstawowymi zasadami dotyczącymi ochrony danych osobowych i zobowiązuję się do ich przestrzegania.

Zobowiązuję się do zachowania w tajemnicy informacji prawnie chronionych, w tym danych osobowych, do których mam lub będę miał/a* dostęp w związku z wykonywaniem przeze mnie obowiązków pracowniczych lub innych wykonywanych na rzecz Głównego Inspektoratu Transportu Drogowego na podstawie ……..

W szczególności zobowiązuję się do ochrony informacji prawnie chronionych 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 ze zbiorów prowadzonych przez Głównego Inspektora Transportu Drogowego, jak i zbiorów powierzonych do przetwarzania Głównemu Inspektorowi Transportu Drogowego przez inne podmioty.

Mam świadomość, że celem Polityki Bezpieczeństwa Informacji jest zapewnienie odpowiedniego poziomu bezpieczeństwa informacji, w tym danych osobowych, przetwarzanych w Głównym Inspektoracie Transportu Drogowego, a naruszenia związane z bezpieczeństwem informacji mogą skutkować odpowiedzialnością karną lub dyscyplinarną na zasadach i w trybie przewidzianym w przepisach prawa, w tym w ustawie z dnia 21 listopada 2008 r. o służbie cywilnej (Dz. U. z 2018 r. poz. 1559, z późn. zm.), ustawie z dnia 26 czerwca 1974 r. - Kodeks pracy (Dz. U. z 2019 r. poz. 1040, z późn. zm.), ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r. poz. 1000, z późn.zm.) oraz ustawie z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125).

*** niepotrzebne skreślić**

…….. ……..

miejsce i data złożenia oświadczenia czytelny podpis

Załącznik nr 2 do Polityki Bezpieczeństwa Informacji
Głównego Inspektoratu Transportu Drogowego

Ogólne zasady bezpieczeństwa fizycznego

§ 1. 1. Do przebywania na terenie GITD upoważnieni są pracownicy GITD.

2. Pracownicy GITD mogą przebywać w poszczególnych strefach zgodnie z uprawnieniami w systemie kontroli dostępu.

3. Pracownicy GITD znajdujący się w strefie, do której z uwagi na uprawnienia w systemie kontroli dostępu nie mają prawa samodzielnego wejścia, podlegają nadzorowi osób upoważnionych.

4. Byli pracownicy GITD traktowani są jak goście. Osoby te nie mogą się samodzielnie poruszać po terenie GITD i podlegają szczególnemu nadzorowi.

§ 2. 1. Osoby niebędące pracownikami GITD mają prawo wstępu do strefy publicznie dostępnej. W przypadku obiektów wyposażonych w oddzielną recepcję zarządzaną przez administrację budynku możliwość wejścia do strefy publicznie dostępnej GITD jest uzależniona od decyzji pracownika recepcji budynku mającej na uwadze ochronę osób i mienia w budynku.

2. Na terenie GITD goście mogą przebywać wyłącznie pod nadzorem pracownika GITD.

3. Obecność gościa na terenie GITD poza strefą publicznie dostępną jest dozwolona, jeżeli wynika to z celu związanego z działalnością GITD.

4. Tożsamość gościa oraz godzina wejścia do strefy ograniczonego dostępu i wyjścia z tej strefy mogą być odnotowywane w ewidencji gości prowadzonej przez administrację budynku.

5. Gość jest zobowiązany, podczas przebywania na terenie GITD poza strefą publicznie dostępną, do noszenia identyfikatora wskazującego, iż nie jest on pracownikiem GITD.

§ 3. 1. Zamówione towary i korespondencja są dostarczane do strefy publicznie dostępnej i tam są odbierane przez upoważnionego pracownika GITD.

2. W przypadku konieczności dostarczenia towarów do pomieszczeń znajdujących się w strefie ograniczonego dostępu, dostawcy traktowani są jak goście, zgodnie z zasadami określonymi w § 2.

3. Dostawa towarów w trybie określonym w ust. 2 jest w szczególności dopuszczalna, gdy gabaryty towaru uniemożliwiają jego przeniesienie przez pracowników GITD lub gdy dostawa łączy się z koniecznością przeprowadzenia specjalistycznych prac związanych np. z instalacją dostarczonego towaru.

Załącznik nr 3 do Polityki Bezpieczeństwa Informacji
Głównego Inspektoratu Transportu Drogowego

Współpraca ze stronami trzecimi

1. Umowa z podmiotem zewnętrznym, która wiąże się z możliwością dostępu do informacji, powinna regulować zagadnienia ochrony informacji i ochrony innych aktywów Głównego Inspektoratu Transportu Drogowego, zwanego dalej: GITD, przez ten podmiot oraz jego wszystkich podwykonawców uczestniczących w realizacji umowy.
2. Umowa z podmiotem zewnętrznym powinna w szczególności regulować następujące zagadnienia:
   1) wymagania prawne w zakresie świadczenia usługi w związku z ochroną informacji;
   2) określenie sposobu dostępu do informacji;
   3) określenie sposobu bezpiecznej wymiany informacji;
   4) określenie dopuszczalnego celu przetwarzania przekazanych informacji;
   5) określenie zasad bezpiecznego korzystania z infrastruktury informatycznej GITD oraz dostępu do tej infrastruktury, jeżeli wynika to ze specyfiki świadczenia usługi;
   6) ochronę poufności przekazanych informacji. Z obowiązku zachowania poufności zwolnione są informacje publicznie dostępne oraz informacje, których ujawnienie wymagane jest przepisami prawa;
   7) odpowiedzialność za naruszenie bezpieczeństwa informacji;
   8) obowiązkowo określać tryb postępowania w przypadku wystąpienia incydentu naruszenia bezpieczeństwa informacji. Tryb ten musi uwzględniać co najmniej powiadomienie GITD o wystąpieniu incydentu z uwzględnieniem wymogów prawnych, m.in. wynikających z przepisów o ochronie danych osobowych oraz cyberbezpieczeństwa;
   9) obowiązek zwrotu otrzymanych nośników informacji przed lub w momencie zakończenia obowiązywania umowy, usunięcia danych wytworzonych w związku z realizacją umowy lub otrzymanych od GITD w tym drogą elektroniczną oraz protokolarnego udokumentowania usunięcia danych;
   10) obowiązek informowania o wszelkich zmianach po stronie podmiotu zewnętrznego, mogących wpłynąć na realizację umowy;
   11) specyfikację warunków świadczenia usługi.
3. Zagadnienia, o których mowa w ust. 2, nie stanową katalogu zamkniętego i powinny być każdorazowo stosowane z uwzględnieniem specyfiki i przedmiotu zawieranej umowy.

4. Umowa, której przedmiot obejmuje prace rozwojowe w zakresie oprogramowania powinna również zawierać klauzule umożliwiające egzekwowanie wymagań określonych w Polityce Bezpieczeństwa Teleinformatycznego GITD.
5. Wymiana informacji wrażliwych i prawnie chronionych pomiędzy podmiotem zewnętrznym a GITD wymaga ich zabezpieczenia.
6. Wymiana informacji poprzez łącza informatyczne niebędące pod kontrolą GITD wymaga w szczególności:
    1) w przypadku wymiany informacji z wykorzystaniem poczty elektronicznej – zapewnienia szyfrowania przesyłanych informacji. Dopuszcza się szyfrowanie wyłącznie załączników, o ile treść wiadomości nie zawiera informacji wymagających ochrony;
    2) w przypadku połączenia pomiędzy systemami informatycznymi GITD, a systemem informatycznym dostawcy – zapewnienia przesyłania danych w postaci zaszyfrowanej, w szczególności z wykorzystaniem protokołów zapewniających transfer danych zaszyfrowanych lub poprzez przesyłanie zaszyfrowanych plików.
7. Wymiana informacji przy użyciu dokumentów papierowych odbywa się m.in. osobiście, za pośrednictwem poczty międzyresortowej, operatora pocztowego lub poprzez firmy kurierskie.
8. Sposób bezpiecznej wymiany danych może być określony w umowie głównej lub w oddzielnym porozumieniu pomiędzy GITD, a podmiotem zewnętrznym.
9. Kierujący komórkami organizacyjnymi GITD korzystającymi z usług podmiotów zewnętrznych są zobowiązani do monitorowania jakości usług świadczonych przez te podmioty z uwzględnieniem wymagań prawnych oraz zdefiniowanych parametrów świadczenia tych usług.
10. Częstotliwość monitorowania jakości usług i monitorowane parametry są określane indywidualnie, w zależności od charakteru usługi.
11. W przypadku stwierdzenia, iż jakość usługi nie spełnia wymagań określonych w umowie, kierujący komórką organizacyjną GITD podejmuje działania w celu wyegzekwowania warunków zawartej z podmiotem zewnętrznym. W przypadku, gdy egzekwowanie warunków świadczenia usługi nie przynosi oczekiwanych rezultatów powinny zostać podjęte, w ramach możliwych do podjęcia działań prawnych oraz zgodnie z postanowieniami zawartej umowy, działania w celu zakończenia współpracy z podmiotem zewnętrznym.

Załącznik nr 4 do Polityki Bezpieczeństwa Informacji
Głównego Inspektoratu Transportu Drogowego

Bezpieczeństwo osobowe

§ 1. Zatrudnienie

1. W przypadku podejmowania jakiejkolwiek formy zatrudnienia, kierujący komórką organizacyjną GITD (lub jego zastępca lub osoba wyznaczona), na rzecz której osoba wykonuje pracę, jest odpowiedzialny za nadzór nad prawidłowością realizacji zleconych zadań i zabezpieczenie interesów GITD.
2. Bezpośredni przełożony osoby jest zobowiązany do określenia wymagań w zakresie dostępu do informacji oraz uprawnień do zasobów (systemów informatycznych, stref dostępu, pomieszczeń itp.) niezbędnych do wykonania powierzonych osobie obowiązków i zadań.
3. Udostępnienie zasobów informacyjnych GITD (dokumentów, nośników z danymi, systemów informatycznych, stref dostępu, pomieszczeń itp.) w tym również urządzeń (komputerów, telefonów itp.), musi być poprzedzone podpisaniem przez osobę oświadczenia, o którym mowa w Polityce Bezpieczeństwa Informacji GITD, oraz otrzymania upoważnienia do przetwarzania danych.
4. Przed podjęciem zadań i obowiązków wymagających dostępu do informacji niejawnych, konieczne jest spełnienie wymagań prawnych związanych z dostępem do tych informacji wynikających z właściwych przepisów i regulacji wewnętrznych w zakresie ochrony informacji niejawnych.

§ 2. Zmiana zadań i obowiązków

1. W przypadku zmiany powierzonych obowiązków i wykonywanych zadań, kierujący komórką organizacyjną GITD lub jego zastępca oraz bezpośredni przełożony osoby powinni zapewnić:
    1) przejęcie akt powierzonych spraw;
    2) złożenie wniosku o odebranie uprawnień do zasobów, do których nie jest wymagany dalszy dostęp;
    3) złożenie wniosku o nadanie uprawnień do nowych zasobów, do których dostęp będzie pracownikowi niezbędny w związku ze zmianą zadań i obowiązków.
2. W przypadku zmiany komórki organizacyjnej GITD uprawnienia do systemów informatycznych i pozostałych zasobów powinny zostać całkowicie odebrane i nadane ponownie w nowej komórce organizacyjnej GITD, zgodnie z wnioskiem skierowanym

z tej komórki. Nie obejmuje to podstawowych uprawnień takich jak dostęp do konta domenowego, poczty elektronicznej, zasobów wspólnych GITD, pomieszczeń wspólnych.

§ 3. Szkolenia

1. W celu utrwalania właściwych zachowań dotyczących bezpieczeństwa informacji w GITD organizowane są szkolenia i/lub warsztaty w tym obszarze. Szkolenia i/lub warsztaty prowadzone są w różnych formach m.in. wykładów, akcji informacyjnych, e -learning, newsletterów. Zadania i odpowiedzialność w tym zakresie określa Polityka Bezpieczeństwa Informacji GITD.
2. Obowiązkiem każdego pracownika jest uczestniczenie w szkoleniu lub warsztatach z zakresu bezpieczeństwa informacji przynajmniej raz na dwa lata.
3. Podczas realizacji szkoleń i warsztatów w obszarze bezpieczeństwa informacji, konieczne jest zapewnienie dowodu audytowego odbycia szkolenia (np.: certyfikat, pisemne potwierdzenie ukończenia itp.). W tym celu mogą być prowadzone listy obecności zawierające datę szkolenia, tytuł szkolenia oraz listę uczestników wraz z podpisami lub inne dowody audytowe adekwatne do wybranej formy szkolenia (np. certyfikat w formie elektronicznej).

§ 4. Ustanie zatrudnienia

1. W przypadku zakończenia lub przewidywanego zakończenia zatrudnienia/współpracy, kierujący właściwymi komórkami organizacyjnymi GITD zobowiązani są do zapewnienia w szczególności:
    1) odebrania uprawnień do poszczególnych zasobów informatycznych GITD (zasobów wspólnych, systemów informatycznych itp.);
    2) rozliczenia pracownika z udostępnionego wyposażenia związanego z przetwarzaniem informacji (komputerów, telefonów, nośników danych itp.).
2. Weryfikacja odbioru uprawnień realizowana jest w dowolny sposób np.: przy pomocy karty obiegowej, lub innego narzędzia lub dedykowanego systemu informatycznego, jeżeli taki zostanie uruchomiony.
3. Weryfikacja zwrotu udostępnionego wyposażenia odbywa się zgodnie z wewnętrznymi procedurami obowiązującymi w GITD.
4. Uprawnienia należy odbierać niezwłocznie z chwilą ustania stosunku pracy lub innej formy współpracy, chyba że osoba kończąca zatrudnienie nie świadczy pracy przed ustaniem zatrudnienia. W takim przypadku, uprawnienia powinny być odebrane w dniu ustania obowiązku świadczenia pracy (w tym również w przypadku rozpoczęcia urlopu).

Załącznik nr 5 do Polityki Bezpieczeństwa Informacji
Głównego Inspektoratu Transportu Drogowego

WZÓR WYZNACZENIA ASI / AMS

..... Warszawa, dnia …… 20 …. r.

Pan/i

…….

…….

Biuro ……...

/w miejscu/

Na podstawie § 10 ust. 17 pkt 7 lit. a Polityki Bezpieczeństwem Informacji Głównego Inspektoratu Transportu Drogowego, stanowiącej załącznik do zarządzenia nr ….. Głównego Inspektora Transportu Drogowego z dnia …….. w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji Głównego Inspektoratu Transportu Drogowego (Dz. Urz. GITD poz. …), wyznaczam Panią / Pana***** na Administratora Systemu Informatycznego / Administratora Merytorycznego Systemu***** …….

…….

podpis, pieczęć

Powierzone obowiązki przyjmuję: ……

data, podpis

*** niepotrzebne skreślić**

Załącznik nr 6 do Polityki Bezpieczeństwa Informacji
Głównego Inspektoratu Transportu Drogowego

Postępowanie z dokumentami papierowymi

1. Podczas pracy z dokumentami papierowymi wymagane jest zwrócenie szczególnej uwagi na ochronę informacji zawartych w tych dokumentach.
2. Praca z dokumentami odbywa się w pomieszczeniach Głównego Inspektoratu Transportu Drogowego, zwanego dalej: GITD, chyba, że charakter wytwarzanego lub przetwarzanego dokumentu wymusza pracę poza tymi pomieszczeniami.
3. Zabronione jest wynoszenie z terenu GITD dokumentów papierowych bez zgody kierującego komórką organizacyjną, chyba, że jest to jednoznacznie związane z wykonywanymi obowiązkami służbowymi i jest niezbędne do wykonania tych obowiązków.
4. Przepis pkt 3 nie dotyczy dokumentów zawierających informacje publicznie dostępne.
5. Podczas pracy z dokumentami należy zwrócić szczególną uwagę na zabezpieczenie przed możliwością zapoznania się z treścią dokumentu przez osoby nieupoważnione.
6. Pracownicy przetwarzający dokumenty papierowe poza pomieszczeniami GITD są zobowiązani do zabezpieczenia tych dokumentów przed ich utratą, w szczególności poprzez bezpośredni nadzór nad dokumentami oraz przechowywanie dokumentów w sposób uniemożliwiający dostęp do nich osobom niepowołanym.
7. Dokumenty papierowe mogą być udostępniane wyłącznie osobom upoważnionym, z racji pełnionych obowiązków służbowych, do zapoznania się z ich treścią.
8. Wytwarzając dokument należy zwrócić szczególną uwagę na poprawność jego treści. W przypadku stwierdzenia błędu w treści dokumentu należy niezwłocznie podjąć działania zapobiegające ewentualnym negatywnym skutkom błędu.
9. Podczas pracy z dokumentami należy zwrócić uwagę na ich zabezpieczenie przed uszkodzeniem lub zniszczeniem na skutek zabrudzenia lub zalania.
10. Drukując dokument należy zapewnić, że wydrukowany dokument nie będzie dostępny dla osoby nieuprawnionej tj. dokument musi być zabrany z drukarki przez osobę uprawnioną niezwłocznie po wydrukowaniu.
11. Kopiowanie lub skanowanie dokumentów odbywa przez pracownika upoważnionego do przetwarzania dokumentu. Po zakończeniu skanowania oryginał, a w przypadku kopiowania również wszystkie kopie dokumentu, muszą być niezwłocznie zabrane z urządzenia.

12. Wszelkie wadliwe wydruki lub kopie muszą być zabrane z urządzenia i zniszczone w przeznaczonych do tego celu niszczarkach dokumentów.
13. W przypadku zacięcia papieru, zadrukowany papier, po jego wyjęciu z urządzenia, podlega zniszczeniu w niszczarce. Papier powinien być wyjęty w sposób uniemożliwiający zapoznanie się przez osoby nieupoważnione z treścią wydruku.
14. Dokumenty papierowe przechowywane są:
    a. w zamykanych meblach biurowych lub w innych meblach zapewniających zwiększony poziom ochrony – w przypadku przechowywania dokumentów w pomieszczeniach biurowych,
    b. w pomieszczeniach przeznaczonych do przechowywania dokumentacji

- z zastrzeżeniem pkt 15. Powyższe nie obejmuje dokumentów zawierających informacje jawne, które mogą być przechowywane w zamykanych pomieszczeniach biurowych w meblach otwartych oraz nieposiadających zamka lub innego podobnego zabezpieczenia.

15. Przechowywanie dokumentów, co do których istnieją prawnie zdefiniowane wymagania w tym w zakresie, realizuje się zgodnie z właściwymi przepisami. Obejmuje to m.in. dokumenty publiczne, o których mowa w ustawie z dnia 22 listopada 2018 r. o dokumentach publicznych (Dz. U. z 2019 r. poz. 53, z późn. zm.).
16. Przepis pkt 14 nie dotyczy dokumentów zawierających wyłącznie informacje publicznie dostępne.
17. Zasady grupowania dokumentacji papierowej w miejscach przechowywania reguluje instrukcja kancelaryjna.
18. Zasady przechowywania dokumentacji archiwalnej reguluje instrukcja w sprawie organizacji i zakresu działania archiwum zakładowego w GITD.
19. Dokumenty papierowe niepodlegające archiwizacji są niszczone w niszczarkach. Nie dotyczy to dokumentów zawierających wyłącznie informacje przeznaczone do powszechnego udostępniania, chyba że taki dokument nie jest dalej potrzebny, w takiej sytuacji powinien być zniszczony w niszczarce.
20. Zasady brakowania dokumentacji archiwalnej określono w instrukcji w sprawie organizacji i zakresu działania archiwum zakładowego w GITD.
21. Przekazanie przez pracownika dokumentacji papierowej w związku z ustaniem stosunku pracy następuje w trybie określonym w obowiązującym w GITD regulaminie pracy.

22. Każdy pracownik jest zobowiązany do przestrzegania zasady czystego biurka. Zasada czystego biurka realizowana jest poprzez zapewnienie, że podczas dłuższej nieobecności pracownika na stanowisku pracy dokumenty i informatyczne nośniki danych przechowywane – w miarę możliwości organizacyjno-technicznych – należy przechowywać w odpowiednio zabezpieczonych meblach biurowych lub szafach metalowych, sejfach, itp.
23. Podstawowym narzędziem do niszczenia dokumentów w GITD jest niszczarka. Dokumenty przeznaczone do zniszczenia umieszczane są przez pracownika w niszczarce udostępnionej przez GITD, z zachowaniem podstawowych zasad BHP przy obsłudze takiego urządzenia.
24. W sytuacjach wyjątkowych, w szczególności potrzeby zniszczenia dużej ilości dokumentów, kierujący komórką organizacyjną może podjąć decyzję o przekazaniu dokumentów wyspecjalizowanemu podmiotowi zewnętrznemu celem ich zniszczenia. Zniszczenie dokumentacji przez podmiot zewnętrzny odbywa się za zgodą Dyrektora Generalnego GITD. Szczegółowe zasady określają wewnętrzne regulacje, m.in. instrukcja kancelaryjna.
25. Powyższe zasady należy stosować uzupełniająco do zasad i wymagań określonych w ustawie z dnia 22 listopada 2018 r. o dokumentach publicznych oraz aktach wykonawczych wydanych na jej podstawie, w odniesieniu do dokumentów publicznych w rozumieniu tej ustawy.

Załącznik nr 7 do Polityki Bezpieczeństwa Informacji
Głównego Inspektoratu Transportu Drogowego

Procedura postępowania w sytuacji naruszenia bezpieczeństwa informacji, w tym ochrony danych osobowych (incydent)

§ 1. 1. Za zdarzenie powodujące naruszenie lub uzasadnione podejrzenie możliwości wystąpienia naruszenia bezpieczeństwa informacji, w tym ochrony danych osobowych, uznaje się:

1) świadome lub nieświadome ujawnienie informacji chronionych osobie nieupoważnionej;
2) sytuacje dotyczące systemu informatycznego:
   a) brak lub niedostępność spodziewanych informacji,
   b) pozostawione ślady włamania komputerowego, np. zmiany konfiguracji,
   c) zmiany sum kontrolnych plików,
   d) wszelkie zapisy w logach systemów świadczące o naruszeniu bezpieczeństwa, wykonywaniu niedozwolonych operacji itp.,
   e) samodzielne niezdefiniowane przez ASI lub użytkownika akcje podejmowane przez system (nawiązywanie połączeń, wysyłanie maili, itp.),
   f) intensywna praca dysku w czasie, gdy z komputera nikt nie korzysta,
   g) powtarzające się „zawieszenia" na ogół stabilnego systemu,
   h) spowolnienie pracy systemu lub sieci,
   i) inne niż zwykle lub dodatkowe okna powitalne i proszące o podanie hasła,
   j) odmowa przyjęcia hasła użytkownika,
   k) pojawianie się niestandardowych okien, napisów i innych elementów ekranu,
   l) znaczące zmiany w zajętości dysku,
   m) nienaturalne rozmiary zapisywanych na dysku plików,
   n) nietypowe nazwy plików lub katalogów,
   o) wykonujący nieuzasadnione połączenia lub odbierający nieuzasadnione połączenia modem podłączony do komputera,
   p) powtarzające się nagłe zrywanie połączeń sieciowych,
   q) ujawnienie indywidualnych haseł dostępu do informacji chronionych,
   r) otrzymanie niespodziewanej wiadomości e-mail z załącznikami (najczęściej typu .doc, .exe, .com lub innym plikiem wykonywalnym (aplikacja, skrypt, archiwum));

3) sytuacje dotyczące nośników informacji chronionych, w tym z danymi osobowymi (elektroniczne i papierowe):
   a) nieuprawnione wykonanie kopii nośników,
   b) zmiana lub usunięcie informacji zapisanych na kopiach bezpieczeństwa lub archiwalnych,
   c) zgubienie nośnika,
   d) wykrycie braku nośnika w jego miejscu przechowywania,
   e) odkrycie niezniszczonych nośników w koszu na śmieci,
   f) przekazanie nośnika osobie nieuprawnionej do ich otrzymania,
   g) znalezienie nośnika;
4) sytuacje dotyczące pomieszczeń:
   a) nieuprawniony dostęp lub próba dostępu do pomieszczeń przez osoby nieuprawnione,
   b) pozostawienie bez nadzoru osoby nieupoważnionej w pomieszczeniu;
   c) niewłaściwe działanie fizycznych zabezpieczeń pomieszczeń,
   d) niewłaściwe parametry środowiska takie jak temperatura i wilgotność w odniesieniu do pomieszczeń serwerowni i węzłów sieci;
5) sytuacje dotyczące naruszenia ochrony danych osobowych:
   a) dopuszczenie do przetwarzania danych osobowych pracowników bez odpowiednich upoważnień,
   b) udostępnianie danych osobowych osobom nieupoważnionym,
   c) udostępnianie danych osobowych nieuprawnionym podmiotom,
   d) powierzanie przetwarzania danych osobowych innym podmiotom bez pisemnej umowy,
   e) zbieranie danych osobowych bez wykonywania obowiązków informacyjnych,
   f) pozyskiwanie danych osobowych z nielegalnych źródeł,
   g) przetwarzanie danych osobowych jest niezgodne z prawnie uzasadnionym celem i zakresem,
   h) przetwarzanie danych osobowych w okresie dłuższym niż prawnie dopuszczalny,
   i) tworzenie nowych zbiorów danych osobowych lub modyfikacja istniejących bez konsultacji z IOD,
   j) przetwarzanie danych osobowych poza obszarem przetwarzania bez zgody,
   k) przetwarzanie danych osobowych w systemie, który nie spełnia wymogów określonych w przepisach prawa oraz dokumentacji tego systemu,
   l) wykonanie nieuprawnionych kopii danych osobowych,
   m) brak aktualnych kopii bezpieczeństwa danych osobowych,
   n) niewłaściwe niszczenie nośników z danymi osobowymi, pozwalające na ich ujawnienie osobom nieupoważnionym,

o) brak przeszkolenia pracowników w zakresie zasad przetwarzania danych osobowych,

p) brak oświadczenia pracownika o zachowaniu poufności.

2. Katalog zdarzeń, o których mowa w ust. 1 jest otwarty, jak również może być rozszerzony lub uszczegółowiony w innych dokumentach stanowiących dokumentację Systemu Zarządzania Bezpieczeństwem Informacji, zwaną dalej: SZBI, w szczególności w dokumentacji SZBI systemów informatycznych.

§ 2. 1. Osoba, która podejrzewa lub stwierdzi naruszenie bezpieczeństwa informacji, ma obowiązek niezwłocznie:

1) zgłosić zdarzenie na adres: incydent@gitd.gov.pl lub w przypadku braku dostępu do poczty elektronicznej – osobiście lub telefonicznie do Pełnomocnika do spraw bezpieczeństwa informacji, Pełnomocnika do spraw bezpieczeństwa cyberprzestrzeni lub sekretariatu BIŁ;
2) jeżeli sytuacja dotyczy systemu informatycznego, powiadomić również właściwego administratora tego systemu informatycznego, zwanego dalej: ASI;
3) jeżeli sytuacja dotyczy danych osobowych, w tym przetwarzanych w systemie informatycznym, powiadomić również inspektora ochrony danych, zwanego dalej „IOD”, (iod@gitd.gov.pl lub osobiście / telefonicznie); w przypadku delegatury terenowej Głównego Inspektoratu Transportu Drogowego, zwanego dalej: GITD, należy poinformować również koordynatora ds. ochrony danych osobowych w danej delegaturze;
4) nie podejmować dalszej pracy w systemie informatycznym bez decyzji ASI;
5) powiadomić o zaistniałym zdarzeniu swojego bezpośredniego przełożonego; w przypadku delegatury terenowej GITD należy poinformować koordynatora ds. ochrony danych osobowych w danej delegaturze;

2. Zgłoszenie, o którym mowa w ust. 1 pkt 1 powinno zawierać:

1) opis symptomów, w tym świadczących o możliwości naruszenia lub naruszeniu ochrony danych osobowych;
2) wskazanie sytuacji i czasu, w jakim zauważono zdarzenie, ewentualnie osób uczestniczących (jeżeli dotyczy), systemu informatycznego (jeżeli dotyczy), itp.;
3) wszelkie inne istotne informacje, mogące pomóc w ustaleniu przyczyny zdarzenia.

3. Po otrzymaniu zgłoszenia, Pełnomocnik do spraw bezpieczeństwa informacji, w określonych przypadkach Pełnomocnik do spraw bezpieczeństwa cyberprzestrzeni, IOD, koordynator do spraw ochrony danych osobowych, właściwy ASI:

1) weryfikują i kategoryzują zdarzenie;

2) oceniają wpływ zdarzenia, w tym możliwość wystąpienia strat w zasobach informacyjnych i systemowych w przypadku dalszego działania danego systemu z uwzględnieniem poziomu istotności:
   a) WYSOKI – jeżeli przewidywane skutki zdarzenia mogą uniemożliwić działanie procesów biznesowych GITD lub doprowadzić do utraty poufności, dostępności lub integralności danych (w szczególności danych osobowych),
   b) ŚREDNI – jeżeli przewidywane skutki zdarzenia mogą w istotny sposób utrudnić realizację procesów biznesowych GITD w związku z obniżoną jakością usług dostarczanych przez systemy informatyczne,
   c) NISKI – jeżeli przewidywane skutki zdarzenia są ograniczone w skali i zasięgu, oraz jest mało prawdopodobne, aby negatywnie wpływały na działalność GITD

   - oraz uwarunkowań prawnych w odniesieniu do incydentów cyberbezpieczeństwa (incydent w podmiocie publicznym, incydent poważny w odniesieniu do usługi kluczowej);
3) podejmują działania w celu zatrzymania negatywnych skutków zdarzenia, w tym we współpracy w właściwymi komórkami organizacyjnymi GITD odpowiedzialnymi za dane aktywa (zasoby), włączając w to zatrzymanie działania systemów informatycznych;
4) podejmują działania w celu wyjaśnienia przyczyn wystąpienia zdarzenia.

4. W przypadku stwierdzenia naruszenia ochrony danych osobowych (incydent) IOD powiadamia o tym Głównego Inspektora Transportu Drogowego oraz informuje Prezesa Urzędu Ochrony Danych Osobowych, zgodnie z trybem zgłaszania naruszeń do tego organu. IOD w tej sytuacji koordynuje i nadzoruje rozwiązanie incydentu. Główny Inspektor Transportu Drogowego w ramach działań naprawczych podejmuje również działania w celu wyeliminowania, bądź zminimalizowania wystąpienia podobnego zdarzenia w przyszłości.

5. W przypadku stwierdzenia incydentu w podmiocie publicznym w rozumieniu przepisów ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560), Pełnomocnik do spraw bezpieczeństwa cyberprzestrzeni informuje Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego, zwany dalej: CSIRT GOV, zgodnie z trybem zgłaszania incydentów określonym w wyżej wymienionej ustawie. Pełnomocnik do spraw bezpieczeństwa cyberprzestrzeni w tej sytuacji nadzoruje rozwiązanie incydentu. ASI rozwiązuje lub w określonych przypadkach koordynuje rozwiązanie incydentu (np.: wymagane są działania wykonawcy, któremu zlecono określone zadania w tym zakresie). W obsłudze incydentu mogą być stosowane wewnętrzne procedury właściwe dla danego systemu informatycznego określone w odrębnej dokumentacji SZBI tego systemu.

6. W przypadku stwierdzenia incydentu poważnego w usłudze kluczowej w rozumieniu przepisów ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, osoba wyznaczona z Biura Krajowego Systemu Poboru Opłat, zwanego dalej: BKSPO, informuje CSIRT GOV, zgodnie z trybem zgłaszania incydentów określonym w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. BKSPO właściwe dla prowadzenia, utrzymania i rozwoju oraz nadzoru nad poprawnym i nieprzerwanym działaniem usługi kluczowej w rozumieniu ww. ustawy, której Główny Inspektor Transportu Drogowego jest operatorem, rozwiązuje lub w określonych przypadkach koordynuje rozwiązanie incydentu (np.: wymagane są działania wykonawcy, któremu zlecono określone zadania w tym zakresie). W obsłudze incydentu mogą być stosowane wewnętrzne procedury właściwe dla danego systemu informatycznego określone w odrębnej dokumentacji SZBI tego systemu.

7. W pozostałych przypadkach rozwiązanie incydentu nadzoruje Pełnomocnik do spraw bezpieczeństwa informacji. Incydent rozwiązują lub koordynują jego rozwiązanie właściwe komórki organizacyjne GITD odpowiedzialne za dane aktywa (zasoby), których dotyczy incydent.

8. Z każdego incydentu, którego wpływ został oceniony na poziomie „średni” i „wysoki”, oraz naruszeń ochrony danych osobowych, incydentów w podmiocie publicznym, które miały negatywny wpływ na realizację zadania publicznego, sporządzany jest raport.

9. W systemach informatycznych, w których ustanowiono odrębny SZBI, w tym SZBI certyfikowany za zgodność z normą PN-ISO/IEC 27001, obsługa incydentów może odbywać się w odrębny sposób, z zastrzeżeniem obowiązku informacyjnego określonego w ust. 1.

§ 3. 1. Pełnomocnik do spraw bezpieczeństwa informacji prowadzi rejestr wszystkich zdarzeń związanych z bezpieczeństwem informacji.

2. IOD prowadzi rejestr zdarzeń dotyczących naruszenia ochrony danych osobowych zgodnie z przepisami Polityki Ochrony Danych Osobowych Głównego Inspektoratu Transportu Drogowego i wymogami RODO oraz innych aktów prawnych w tym zakresie.

3. Pełnomocnik do spraw bezpieczeństwa cyberprzestrzeni prowadzi rejestr wszystkich incydentów cyberbezpieczeństwa (incydenty w podmiocie publicznym, incydenty poważne, incydenty krytyczne).

4. Rejestry, o których mowa w ust. 1 – 3, mogą być prowadzone elektronicznie.

5. Rejestr w zakresie, o którym mowa w ust. 1 – 3, może być wspólny dla wszystkich zdarzeń i incydentów w GITD, z zastrzeżeniem, że w przypadku prowadzenia rejestru, o którym mowa w ust. 2 w ramach wspólnego, rejestr wspólny musi spełniać wymagania określone w art. 33 RODO.

6. Dane o incydentach poważnych do rejestru, o którym mowa w ust. 3 przekazuje BKSPO.

Załącznik nr 8 do Polityki Bezpieczeństwa Informacji
Głównego Inspektoratu Transportu Drogowego

Zarządzanie Ryzykiem Informacyjnym

§ 1. 1. Dokument określa ramowe zasady zarządzania ryzykiem w obszarze bezpieczeństwa informacji w GITD.

2. Działania określone w niniejszym dokumencie mają na celu kontrolowanie ryzyka związanego z utratą poufności, integralności i dostępności informacji, a także przetwarzaniem informacji niezgodnie z regulacjami prawnymi.

§ 2. 1. Zarządzanie ryzykiem informacyjnym obejmuje:

1) analizę ryzyka, w skład której wchodzą:
   a) identyfikacja ryzyka mającego wpływ na bezpieczeństwo informacji przetwarzanych w GITD,
   b) szacowanie ryzyka, z uwzględnieniem konsekwencji jego materializacji i prawdopodobieństwa materializacji;
2) ewaluację ryzyka, w celu stwierdzenia, czy dane ryzyko jest akceptowalne;
3) określenie planu postępowania z ryzykiem i jego wdrożenie;
4) monitorowanie poziomu ryzyka.

2. Analiza ryzyka przeprowadzana jest zgodnie z niniejszym dokumentem oraz załącznikiem nr 9 do PBI.

3. Zarządzanie ryzykiem informacyjnym obejmuje:

1) informacje przetwarzane we wszystkich komórkach organizacyjnych GITD;
2) informacje przetwarzane w dowolnej postaci, w tym z wykorzystaniem systemów informatycznych, w postaci papierowej oraz przekazywane podczas rozmowy telefonicznej lub osobiście.

4. Niniejszy dokument nie obejmuje zarządzania ryzykiem w związku z przetwarzaniem informacji niejawnych w rozumieniu ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych.

§ 3. 1. Plan postępowania z ryzykiem określa sposób postępowania z ryzykiem.

2. Dopuszcza się następujący sposób postępowania z ryzykiem informacyjnym:

1) tolerowanie ryzyka;
2) monitorowanie ryzyka wraz ze wskazaniem częstotliwości monitorowania;
3) unikanie ryzyka poprzez zaprzestanie działalności, która generuje dane ryzyko;

4) ograniczenie ryzyka poprzez wdrożenie mechanizmów zabezpieczających;
5) dzielenie się ryzykiem, poprzez przerzucenie, całkowite lub częściowe, skutków materializacji ryzyka na podmiot zewnętrzny.

3. W przypadku, gdy plan postępowania z ryzykiem określa działania, które muszą być podjęte w celu zarządzania ryzykiem, plan postępowania z ryzykiem wskazuje:

1) osoby odpowiedzialne za realizację czynności związanych z postępowaniem z ryzykiem;
2) terminy czynności związanych z postępowaniem z ryzykiem, w tym, w zależności od rodzaju czynności, terminy jednorazowe lub częstotliwość realizowanych czynności.

§ 4. 1. Właściciele ryzyka odpowiadają za zarządzanie ryzykiem w podległych sobie obszarach, w tym za realizację czynności związanych z analizą i ewaluacją ryzyka oraz przygotowaniem planu postępowania z ryzykiem.

2. Właścicielami ryzyka są kierujący komórkami organizacyjnymi w zakresie przetwarzania informacji w podległych komórkach organizacyjnych, w postaci papierowej oraz cyfrowej w tym w systemach informatycznych.

3. Właściciele ryzyka są odpowiedzialni za oszacowanie konsekwencji naruszenia bezpieczeństwa informacji przetwarzanych przez ich komórki organizacyjne, w tym również z wykorzystaniem systemów informatycznych.

4. Kierujący komórką organizacyjną GITD właściwą do spraw ochrony i monitoringu nieruchomości będących w trwałym zarządzie GITD oraz prawidłowego funkcjonowania zabezpieczeń przed nieuprawnionym dostępem do stref ograniczonego dostępu w GITD odpowiada za dostarczenie, na wniosek kierujących komórkami organizacyjnymi, informacji na temat oceny zabezpieczeń, podatności i prawdopodobieństw materializacji ryzyka związanego z bezpieczeństwem fizycznym i środowiskowym obiektów GITD.

5. Sposób postępowania z ryzykiem określa właściciel ryzyka.

6. Za koordynację procesu zarządzania ryzykiem informacyjnym odpowiada Pełnomocnik do spraw bezpieczeństwa informacji.

§ 5. 1. Analiza i ewaluacja ryzyka oraz opracowanie planu postępowania z ryzykiem przeprowadzane są co najmniej raz w roku.

2. Właściciel ryzyka przeprowadza dodatkową analizę ryzyka w przypadku, gdy:

1) w obszarze jego odpowiedzialności planowane jest wprowadzenie zmian mogących mieć wpływ na poziom zidentyfikowanego ryzyka;

2) w obszarze jego odpowiedzialności zidentyfikowano podatności lub wystąpiły incydenty naruszenia bezpieczeństwa, świadczące o niedoskonałości mechanizmów zabezpieczających wdrożonych na podstawie planu postępowania z ryzykiem.

§ 6. Wyniki szacowania ryzyka podlegają akceptacji Dyrektora Generalnego GITD.

§ 7. 1. Monitorowanie ryzyka odbywa się w terminach, z częstotliwością i w zakresie określonym w planie postępowania z ryzykiem.

2. Za monitorowanie ryzyka odpowiadają osoby przypisane do tego zadania w planie postępowania z ryzykiem.

3. Sposób raportowania wyników monitorowania ryzyka określa się w planie postępowania z ryzykiem.

§ 8. 1. Realizacja planu postępowania z ryzykiem podlega weryfikacji podczas audytów wewnętrznych.

2. Efektywność działań określonych w planie postępowania z ryzykiem podlega weryfikacji podczas analizy ryzyka przeprowadzanej po realizacji działań określonych w przedmiotowym planie i obejmującej swoim zakresem ryzyka określone w tym planie.

§ 9. Efektywność zarządzania ryzykiem informacyjnym podlega weryfikacji w ramach przeprowadzanych audytów wewnętrznych. W wyniku audytu wewnętrznego mogą zostać określone działania korygujące lub zapobiegawcze, prowadzące do modyfikacji zasad zarządzania ryzykiem w GITD.

§ 10. Zasady przeprowadzania identyfikacji i oceny aktywów informacyjnych oraz analizy ryzyka informacyjnego w GITD określa załącznik nr 9 do PBI.

Załącznik nr 9 do Polityki Bezpieczeństwa Informacji
Głównego Inspektoratu Transportu Drogowego

Procedura analizy ryzyka informacyjnego

Rozdział 1

Postanowienia ogólne

§ 1. 1. Procedura Analizy Ryzyka Informacyjnego w GITD, zwana dalej: Procedurą, określa zasady przeprowadzania identyfikacji i oceny aktywów informacyjnych oraz analizy ryzyka informacyjnego w GITD.

2. Procedura stanowi uszczegółowienie zasad określonych w załączniku nr 8 do PBI.

3. Analiza ryzyka obejmuje identyfikację, szacowanie, ewaluację i postępowanie z ryzykiem.

Rozdział 2

Przeprowadzenie analizy ryzyka

§ 2. W ramach procesu analizy ryzyka informacyjnego przeprowadzana jest:

1) identyfikacja i ocena aktywów informacyjnych GITD;
2) identyfikacja zagrożeń mogących spowodować naruszenia poufności, integralności i/lub dostępności informacji przetwarzanych w GITD;
3) identyfikacja zabezpieczeń chroniących aktywa informacyjne przed zagrożeniami;
4) identyfikacja i ocena podatności stopnia zabezpieczenia aktywów informacyjnych przed poszczególnymi zagrożeniami;
5) określanie planów postępowania z ryzykiem.

Rozdział 3

Identyfikacja i ocena aktywów informacyjnych

§ 3. 1. Identyfikacja aktywów informacyjnych obejmuje:

1) identyfikację grup informacji;
2) identyfikację aktywów służących do przetwarzania poszczególnych grup informacji.

2. Grupy informacji są identyfikowane i oceniane przez kierujących komórkami organizacyjnymi, w których informacje są przetwarzane.

3. Grupę informacji tworzą informacje:

1) przetwarzane w tym samym celu;

2) zbliżone zawartością merytoryczną;

3) podlegające tym samym wymaganiom w zakresie ochrony (w tym prawnym).

4. Dla każdej grupy informacji określane są konsekwencje utraty ich poufności, integralności i dostępności. W tym celu wykorzystuje się poniższą skalę:

Atrybut	Wartość	Opis wartości
Poufność	1	**Jawne.** Informacje, które są jawne, mogą być dostępne dla pracowników oraz osób niebędących pracownikami GITD.
	2	**Wewnętrzne.** Informacje dostępne dla wszystkich pracowników GITD. Informacje te, mogą być udostępniane uprawnionym podmiotom zewnętrznym.
	3	**Limitowane.** Informacje są dostępne dla ograniczonej grupy pracowników GITD w ramach realizowanych zadań. Informacje te mogą być udostępniane uprawnionym podmiotom zewnętrznym.
Integralność	1	**Niska.** Nieuprawniona zmiana informacji lub w wyniku błędu systemu może pociągnąć za sobą zauważalne, ale niezbyt dotkliwe konsekwencje.
	2	**Średnia.** Nieuprawniona zmiana informacji lub w wyniku błędu systemu może pociągnąć za sobą zauważalne, dotkliwe konsekwencje.
	3	**Bezwzględna.** Nieuprawniona zmiana informacji lub w wyniku błędu systemu spowoduje bardzo istotne konsekwencje.
Dostępność	1	Brak dostępu do informacji powyżej 24 godzin nie wiąże się z konsekwencjami dla GITD.
	2	Brak dostępu do informacji do 24 godzin wiąże się z konsekwencjami dla GITD.
	3	Brak bieżącego dostępu do informacji wiąże się z konsekwencjami dla funkcjonowania GITD.

Tabela nr 1. Skala ocen atrybutów bezpieczeństwa informacji

5. Oceny poszczególnych atrybutów informacji służą określeniu wartości informacji wykorzystywanej w analizie ryzyka informacyjnego. W zależności od sumy ocen poufności, integralności i dostępności, grupa informacji przyjmuje wartość zgodnie z poniższą tabelą:

Wartość min.	Wartość max.	Wartość grupy informacji

3,0	5,0	Nieznacząca
Powyżej 5,0	7,0	Średnia
Powyżej 7,0	9,0	Bardzo duża

Tabela nr 2. Określanie wartości grup informacji na podstawie atrybutów

6. W przypadku oceny grupy informacji przez więcej niż jednego kierującego komórką organizacyjną, za wartość przyjmuje się najwyższą ocenę. W sprawach spornych, ocena wyjaśniana jest z Pełnomocnikiem do spraw bezpieczeństwa informacji.

7. W ramach identyfikacji aktywów informacyjnych, dla każdej z grup informacji przypisywane są miejsca ich przetwarzania, w tym systemy informatyczne, w których przetwarzane są informacje w wersji elektronicznej oraz pomieszczenia, w których przetwarzane są informacje w wersji papierowej.

8. Identyfikacja aktywów obejmuje w szczególności:

1) systemy informatyczne, w tym:
   a) systemy informatyczne dedykowane do przetwarzania informacji,
   b) systemy wspomagające;
2) pomieszczenia biurowe, w których informacje są przetwarzane wraz z ich wyposażeniem (meble i urządzenia służące do przechowywania dokumentów);
3) pomieszczenia specjalne stanowiące pomieszczenia o podwyższonym rygorze bezpieczeństwa wraz z ich wyposażeniem (np. serwerownie);
4) nośniki informacji;
5) zasoby ludzkie.

9. Dla aktywów wskazuje się właścicieli. Właścicielem aktywa jest kierujący komórką organizacyjną odpowiedzialną za dane aktywa.

10. Aktywa są identyfikowane w celu przeprowadzenia analizy zagrożeń prowadzących do utraty poufności, integralności i dostępności informacji. Z tego względu stopień szczegółowości identyfikacji aktywów powinien odpowiadać temu celowi.

11. Każdy z aktywów otrzymuje wartość wynikającą z przeprowadzonej identyfikacji i oceny grup informacji, które są w nim przetwarzane. W przypadku, gdy w danym aktywie przetwarzanych jest więcej niż jedna grupa informacji, wartość aktywa jest równoznaczna z najwyżej ocenioną grupą informacji.

12. Aktywa otrzymują wartości w 3-stopniowej skali, zgodnie z Tabelą nr 2 zawartą w niniejszej Procedurze.

13. Wartość aktywa stanowi stopień skutków w przeprowadzanej analizie ryzyka informacyjnego.

Rozdział 4

Ocena ryzyka i postępowanie z ryzykiem

§ 4. 1. Zagrożenia są identyfikowane w odniesieniu do aktywów, w których przetwarzane są zidentyfikowane grupy informacji.

2. Zagrożenia są identyfikowane m.in. na podstawie wykazu zagrożeń generycznych prowadzonego przez Pełnomocnika do spraw bezpieczeństwa informacji.

3. Dla każdej z kategorii aktywów przedstawionej w § 3 pkt 8 niniejszej Procedury może być opracowana lista specyficznych zagrożeń wraz z listą pytań pomocniczych umożliwiającą przeprowadzenie oceny.

4. Stopień szczegółowości identyfikacji zagrożeń musi uwzględniać możliwość efektywnej analizy zabezpieczeń, podatności i możliwości materializacji ryzyka. Z tego względu:

1) zagrożenia, dla których występują różne podatności i różne środki zabezpieczające nie powinny być łączone;
2) zagrożenia o tej samej naturze oraz dotyczące tych samych aktywów lub grup aktywów powinny podlegać konsolidacji.

§ 5. 1. Dla każdego ze zidentyfikowanych zagrożeń przeprowadzana jest identyfikacja zastosowanych zabezpieczeń chroniących przed tym zagrożeniem oraz podatności na to zagrożenie.

2. Dla każdego z zagrożeń wykaz zastosowanych zabezpieczeń i zidentyfikowanych podatności podlega udokumentowaniu.

3. Stopień zabezpieczenia aktywów przed danym zagrożeniem oceniany jest w stosunku do skutków i prawdopodobieństwa wystąpienia przy użyciu poniższej skali:

1) zabezpieczenie pełne – aktywa są w pełni zabezpieczone przed zagrożeniem. Wystąpienie zagrożenia nie spowoduje naruszenia bezpieczeństwa informacji;
2) zabezpieczenie częściowe – w przypadku wystąpienia zagrożenia może nastąpić naruszenie bezpieczeństwa informacji;
3) brak zabezpieczeń – wystąpienie zagrożenia spowoduje naruszenie bezpieczeństwa informacji.

4. Stopień zabezpieczenia aktywów jest określany dla każdego zagrożenia.

§ 6. 1. Dla każdego zagrożenia analizowana jest możliwość wystąpienia strat spowodowanych materializacją zagrożenia i na tej podstawie określany jest stopień prawdopodobieństwa.

2. Prawdopodobieństwo wystąpienia zdarzenia oceniane jest w oparciu o poniższą skalę:

1) prawdopodobieństwo wysokie – 3 punkty. Przesłanki stosowania: zdarzenie objęte ryzykiem może zdarzyć się wielokrotnie w ciągu roku;

2) prawdopodobieństwo średnie – 2 punkty. Przesłanki stosowania: zdarzenie objęte ryzykiem może zdarzyć się kilkukrotnie w ciągu roku;

3) prawdopodobieństwo niskie – 1 punkt. Przesłanki stosowania: zdarzenie objęte ryzykiem może zdarzyć się raz w roku lub nie zdarzyć się wcale w ciągu roku.

§ 7. 1. Dla każdego zagrożenia przypisanego do aktywa informacyjnego określana jest wartość ryzyka pierwotnego i szczątkowego.

2. Wartość ryzyka pierwotnego jest obliczana jako iloczyn prawdopodobieństwa i skutków materializacji ryzyka według poniższego wzoru:

$$\mathbf{WR_P = P \times S,}$$

gdzie:

WR_P – to wartość ryzyka pierwotnego

P – to prawdopodobieństwo materializacji ryzyka

S – to skutki materializacji ryzyka

3. Wartość ryzyka szczątkowego obliczana jest jako iloczyn prawdopodobieństwa i skutków materializacji ryzyka pomniejszonych o stopień zabezpieczenia aktywów według poniższego wzoru:

$$\mathbf{WR_S = (P - Z_P) \times (S = Z_S),}$$

gdzie:

WR_S – to wartość ryzyka szczątkowego

Z_P – to stopień zabezpieczenia aktywów przed prawdopodobieństwem wystąpienia ryzyka

Z_S – to stopień zabezpieczenia aktywów przed skutkami wystąpienia ryzyka

4. Istotność ryzyka szczątkowego określana jest według następującej skali:

Rysunek nr 1. Macierz ryzyka

1) ryzyko szczątkowe poważne, oznaczone kolorem czerwonym, tj. ryzyko, którego iloczyn prawdopodobieństwa wystąpienia danego zdarzenia oraz jego konsekwencji wynosi 6 lub 9 punktów;
2) ryzyko szczątkowe umiarkowane, oznaczone kolorem żółtym, tj. ryzyko, którego iloczyn prawdopodobieństwa wystąpienia danego zdarzenia oraz jego konsekwencji wynosi 3 lub 4 punkty;
3) ryzyko szczątkowe nieznaczne, oznaczone kolorem zielonym, tj. ryzyko, którego iloczyn prawdopodobieństwa wystąpienia danego zdarzenia oraz jego konsekwencji wynosi 1 lub 2 punkty.

§ 8. 1. Ryzykiem akceptowalnym jest ryzyko nieznaczne. W stosunku do pozostałego ryzyka podejmowane są działania przeciwdziałające ryzyku polegające na zaproponowaniu przez właściciela ryzyka planu postępowania z ryzykiem.

2. Plan postępowania z ryzykiem musi zawierać przynajmniej:
1) opis działań, które należy podjąć w celu przeciwdziałania ryzyku;
2) osobę odpowiedzialną za ich wykonanie;
3) termin zakończenia działań;
4) zasoby niezbędne do wykonania działania;
5) częstotliwość monitorowania planu postępowania z ryzykiem.

Rozdział 5

Ocena ryzyka dla systemów informatycznych

§ 9. 1 Analiza ryzyka dla nowych systemów informatycznych powinna stanowić element cyklu projektowego i prowadzić do określenia wymagań bezpieczeństwa dla nowego systemu oraz planowanych zabezpieczeń na poziomie technologicznym i organizacyjnym.

2. Analiza ryzyka dla istniejących systemów informatycznych powinna prowadzić do potwierdzenia lub zaprzeczenia skuteczności istniejących zabezpieczeń oraz ewentualnego przedstawienia rekomendacji dla podniesienia poziomu bezpieczeństwa.