Polityka Bezpieczeństwa Informacji

wersja 1.0

Sierpień 2012

Spis treści

1 Deklaracja Zarządu Głównego PTI

Zarząd Główny Polskiego Towarzystwa Informatycznego – PTI, mając na uwadze kluczową rolę informacji i jej ochrony dla właściwego funkcjonowania i dla realizacji celów statutowych PTI - ustanawia niniejszą Politykę Bezpieczeństwa Informacji.

Polityka Bezpieczeństwa Informacji jest podstawowym dokumentem zawierającym zasady i wymagania ochrony posiadanych informacji, zwłaszcza przechowywanych i przetwarzanych w ramach systemów teleinformatycznych.

Ustanowienie Polityki Bezpieczeństwa Informacji ma na celu podniesienie i utrzymanie wymaganego poziomu ochrony informacji związanych z funkcjonowaniem PTI.

Wdrożenie Polityki Bezpieczeństwa Informacji zapewnia:

- zachowanie zgodności z obowiązującymi przepisami prawa i regulacjami wewnętrznymi PTI w obszarze ochrony informacji, zwłaszcza przechowywanych i przetwarzanych przez systemy teleinformatyczne,
- ciągłość i efektywność procesów biznesowych PTI,
- zachowanie poufności gromadzonych i przetwarzanych informacji, ,
- zmniejszenie ryzyka utraty danych, kradzieży sprzętu i włamań do systemu teleinformatycznego,
- minimalizowanie negatywnych skutków naruszeń bezpieczeństwa,
- utrzymanie dobrego wizerunku PTI poprzez dbałość o bezpieczeństwo informacji.

Niniejsza Polityka Bezpieczeństwa została przedstawiona Zarządowi Głównemu, pracownikom oraz współpracownikom PTI i jest dostępna dla wszystkich zainteresowanych.

ZG PTI deklaruje pełne zaangażowanie w realizację niniejszej Polityki.

Imię i nazwisko

.....

Prezes PTI

data, podpis

05.08.2012

2 Słownik pojęć

Określenie	Definicja
1	*2*
Administrator Bezpieczeństwa Informacji (ABI)	Pracownik lub współpracownik PTI odpowiedzialny za wdrożenie zabezpieczeń i nadzorujący przestrzeganie zasad bezpieczeństwa informacji.
Administrator IT	Pracownik lub współpracownik PTI, który zarządza serwerami (systemami operacyjnymi), stacjami końcowymi lub innymi urządzeniami IT wchodzącymi w skład infrastruktury teleinformatycznej PTI. Administrator posiada dostęp techniczny do możliwości nadawania, modyfikowania i odbierania uprawnień użytkownikom danego systemu, w tym danego systemu operacyjnego.
Aktywa informacyjne	Dane, różnego rodzaju oprogramowanie i dokumentacja związana z opracowaniem, wdrożeniem, a następnie eksploatacją danego systemu IT.
Analiza ryzyka	Proces systematycznej identyfikacji ryzyk, określania ich wielkości i identyfikowania obszarów wymagających zabezpieczeń.
Autoryzacja	Proces, w którym sprawdzane jest czy dany podmiot ma prawo dostępu do zasobów, o które prosi. Odpowiednie uprawnienia są przypisane do konkretnego, zidentyfikowanego podmiotu. Autoryzacja jest zwykle poprzedzona uwierzytelnieniem (zidentyfikowaniem) podmiotu.
Bezpieczeństwo informacji	Zachowanie poufności, integralności i dostępności informacji; dodatkowo, mogą być brane pod uwagę inne własności, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.
Członek władz PTI	Członek towarzystwa wybrany na funkcję lub do jednego z jego organów statutowych, jak np. prezes PTI, Zarząd Główny, itd.
Dane osobowe	Informacje o osobach fizycznych, chronione zgodnie z uoodo.
Dostępność	Właściwość bycia dostępnym i możliwym do wykorzystania przez autoryzowany podmiot.
Incydent związany z bezpieczeństwem informacji	Pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji.
Informacje niejawne	Informacje wskazane w ustawie z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. z 2010 r., nr 182, poz. 1228)

Określenie	Definicja
1	*2*
Integralność	Właściwość polegająca na zapewnieniu dokładności i kompletności aktywów informacyjnych.
Infrastruktura teleinformatyczna PTI	Całość urządzeń teleinformatycznych oraz oprogramowania zarządzanego przez PTI
Kopia zapasowa	Kopia danych lub oprogramowania. Celem jej wykonywania jest odtworzenie systemu po awarii.
Ocena ryzyka	Proces porównywania oszacowanego ryzyka z określonymi kryteriami w celu określenia znaczenia ryzyka.
Podatność	Wady lub luki w strukturze fizycznej, organizacji, procedurach, zarządzaniu, administrowaniu, sprzęcie, oprogramowaniu, a także zamierzone lub niezamierzone działania personelu lub działalności użytkownika, które mogą być wykorzystane do spowodowania szkód.
Postępowanie z ryzykiem	Proces wyboru i wdrażania środków zmieniających ryzyko.
Poufność	Właściwość zapewniająca, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom.
Pracownik PTI	Osoba fizyczna, która zawarła z PTI umowę o pracę.
Ryzyko	Wielkość prawdopodobieństwa, że określone zagrożenie wykorzysta podatność zasobu lub grupy zasobów, aby spowodować szkody, straty lub zniszczenie zasobów.
Serwer	Komputer, świadczący usługi, wchodzący w skład systemu teleinformatycznego.
Stacja robocza	Komputer, na którym w strukturach PTI pracują osoby obsługujące aplikacje biznesowe.
System IT/System	Synonim systemu teleinformatycznego. Każdy system teleinformatyczny PTI ma przypisane imiennie, co najmniej dwie osoby będące jego administratorami (główny i zastępca).
Szacowanie ryzyka	Całościowy proces analizy i oceny ryzyka.
Szkodliwe oprogramowanie	(*ang. malware*) - Oprogramowanie, którego celem jest niszczenie lub modyfikowanie zasobów systemu komputerowego (np. wirusy), umożliwianie wycieku informacji (np. spyware, trojany) lub jakiekolwiek inne wywierające negatywny skutek na stan systemu komputerowego (np. *rootkit*).

Określenie	Definicja
1	*2*
Tajemnica towarzystwa (PTI)	Nieujawnione do wiadomości publicznej informacje techniczne, technologiczne, handlowe i organizacyjne, co do których zostały podjęte przez PTI niezbędne działania w celu zachowania ich poufności.
Uoodo	Ustawa z dnia 29 sierpnia 1997 o ochronie danych osobowych (tekst jednolity Dz.U. z 2002 roku nr 101 poz. 926, z późn. zm.).
Uwierzytelnianie	Proces polegający na zweryfikowaniu zadeklarowanej tożsamości osoby, urządzenia lub usługi biorącej udział w wymianie danych.
Użytkownik Systemu IT	Pracownik PTI lub współpracownik PTI lub członek władz PTI, który w ramach swoich zadań wykonuje zadania związane z użytkowaniem aplikacji biznesowych.
Właściciel aktywów informacyjnych	Pracownik PTI lub współpracownik PTI lub członek władz PTI, który w ramach swoich kompetencji podejmuje decyzje odnośnie sposobu wykorzystania aktywów (zasobów), do których ma uprawnienia. W szczególności poprzez „decyzję o sposobie wykorzystania" rozumie się decyzję o nadaniu uprawnień innym użytkownikom.
Wrażliwość	Atrybut informacji wskazujący, że jej ujawnienie przyniesie straty dla PTI.
Współpracownik PTI	Osoba fizyczna, która wykonuje na rzecz PTI pracę na podstawie stosunku prawnego innego niż umowa o pracę, czyli np. umowa zlecenie, umowa o dzieło, praktyka, wynajęcie na czas określony z innej firmy, jednoosobowa działalność gospodarcza.
Wysoka dostępność	(*ang. High Availability)* zestaw standardów projektowania oraz odpowiedniej implementacji środowiska teleinformatycznego mający na celu minimalizację czasów nieplanowanych niedostępności czyli przerw w działaniu, braku świadczenia usług.
Zabezpieczenie	Środki (techniczne i fizyczne) oraz metody (proceduralno-organizacyjne) utrzymania – zgodnie z istniejącą polityką bezpieczeństwa informacji – pożądanych atrybutów informacji: jej poufności, integralności, dostępności, rozliczalności, autentyczności oraz pożądanych atrybutów systemu teleinformatycznego: integralności i niezawodności.
Zagrożenie	Potencjalna możliwość naruszenia bezpieczeństwa systemu informatycznego.

Określenie	Definicja
1	*2*
Zarządzanie ryzykiem	Skoordynowane działanie kierowania i zarządzania organizacją z uwzględnieniem ryzyka. Zarządzanie ryzykiem zawiera zwykle szacowanie ryzyka, postępowanie z ryzykiem, akceptowanie ryzyka i informowanie o ryzyku.
Zasada czystego biurka	Zasada stanowiąca, że osoba opuszczająca miejsce pracy nie pozostawia na biurku lub innym miejscu używanym przez niego do pracy, w sposób dostępny dla innych osób, dokumentów i nośników zawierających informacje wrażliwe.
Zasada czystego ekranu	Zasada stanowiąca, że osoba opuszczająca miejsce pracy nie pozostawia na swoim stanowisku pracy stacji roboczej (inne przenośne urządzenie IT) w stanie umożliwiającym innym osobom korzystanie z niej.
Zasada wiedzy uzasadnionej	Pracownik lub współpracownik powinien mieć dostęp tylko do tych informacji, które są mu niezbędne do pracy.
Zasoby informacyjne	Ogół informacji będących w posiadaniu PTI, niezależnie od klasyfikacji i stopnia wymaganej ochrony. Obejmuje zarówno informacje przechowywane i przetwarzane w systemie teleinformatycznym PTI, jaki i te, które występują poza systemem IT.
Zasoby materialne	Sprzęt, infrastruktura techniczna (zasilanie, media telekomunikacyjne, klimatyzacja, systemy ochrony fizycznej) oraz personel administrujący systemem IT.
Zdarzenie związane z bezpieczeństwem informacji	Zdarzenie związane z bezpieczeństwem informacji jest określonym stanem systemu, usługi lub sieci, który wskazuje na możliwe naruszenie polityki bezpieczeństwa informacji, błąd zabezpieczenia lub nieznaną dotychczas sytuację, która może być związana ze zmianą poziomu bezpieczeństwa.

3 Cel i zakres Polityki Bezpieczeństwa Informacji

Celem Polityki Bezpieczeństwa Informacji jest zapewnienie, że aktywa informacyjne, posiadane przez PTI, są zabezpieczone w stopniu właściwym dla ich wrażliwości i krytyczności. Niewłaściwa ochrona informacji, zwłaszcza przetwarzanych w ramach systemu teleinformatycznego PTI, może doprowadzić do braku dostępu do informacji, naruszenia ich integralności lub nieautoryzowanego ujawnienia, a w rezultacie, do naruszenia obowiązujących regulacji prawnych, strat finansowych lub pogorszenia wizerunku Polskiego Towarzystwa Informatycznego.

Polityka Bezpieczeństwa Informacji odnosi się do całości zasobów informacyjnych PTI.

Nieprawidłowe działanie systemu IT funkcjonującego na rzecz jednostek organizacyjnych PTI lub wręcz zaprzestanie jego funkcjonowania może uniemożliwić realizację zadań statutowych PTI. Stąd konieczność zapewnienia mechanizmów bezpieczeństwa dla całego Systemu, w oparciu o zapisy ustanowione przez Politykę Bezpieczeństwa Informacji.

3.1 Definicja bezpieczeństwa informacji

Bezpieczeństwo informacji oznacza zapewnienie następujących cech:

- **poufności** – właściwości zapewniającej, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom albo procesom;
- **integralności danych** – właściwości zapewniającej, że dane (forma reprezentacji informacji) nie zostały zmienione lub zniszczone w sposób nieautoryzowany, są dokładne i kompletne;
- **integralności systemu** – właściwości polegającej na tym, że system realizuje swoją zamierzoną funkcję w sposób nienaruszony, wolny od nieautoryzowanej manipulacji, celowej lub przypadkowej;
- **dostępności** – właściwości bycia dostępnym i możliwym do wykorzystania na żądanie, w założonym czasie, przez autoryzowany podmiot;
- **rozliczalności** – właściwości zapewniającej, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.

3.2 Chronione aktywa

W ramach zapewnienia bezpieczeństwa informacji w PTI ochronie podlegają aktywa, na które składają się:

- informacje zbierane, przetwarzane i przechowywane w ramach pracy Systemu, stanowiące dane osobowe lub inne dane wymagające ochrony;
- urządzenia i infrastruktura techniczno-systemowa Systemu;
- dokumentacja systemowa, eksploatacyjna i powykonawcza, zarówno w wersji elektronicznej jak i papierowej.

W zakres niniejszej Polityki Bezpieczeństwa Informacji nie wchodzi ochrona informacji niejawnych, ponieważ informacje niejawne nie są one obecnie gromadzone, przetwarzane i przechowywane w systemie teleinformatycznym PTI.

3.3 Dziedziny bezpieczeństwa

Zapewnienie bezpieczeństwa informacji w systemie IT działającym na potrzeby PTI oznacza zapewnienie bezpieczeństwa w następujących obszarach:

1. Organizacja bezpieczeństwa informacji.
2. Zarządzanie aktywami.
3. Bezpieczeństwo zasobów ludzkich.
4. Bezpieczeństwo fizyczne i środowiskowe.
5. Zarządzanie systemami i sieciami.
6. Kontrola dostępu.
7. Pozyskiwanie, rozwój i utrzymanie systemów informacyjnych.
8. Zarządzanie incydentami związanymi z bezpieczeństwem informacji.
9. Zarządzanie ciągłością działania.
10. Zgodność z prawem, standardami i regulacjami wewnętrznymi.

4 Postępowanie z ryzykiem bezpieczeństwa

W ramach zarządzania bezpieczeństwem informacji w PTI prowadzony jest systematyczny proces zarządzania ryzykiem. W trakcie tego procesu odbywa się okresowe szacowanie ryzyka. Jego wyniki są podstawą do dalszego postępowania ze zidentyfikowanymi zagrożeniami.

Proces zarządzania ryzykiem opiera się o udokumentowaną i formalnie zatwierdzoną procedurę.

5 Kompetencje i odpowiedzialność

Odpowiedzialność za ochronę informacji w PTI ponoszą wszyscy zajmujący się eksploatacją i rozwojem Systemu pracownicy i współpracownicy PTI oraz członkowie władz PTI odpowiednio w zakresie odpowiadającym ich obowiązkom służbowym, posiadanym kompetencjom i funkcjom w towarzystwie.

W szczególności:

- **prezes PTI** łącznie z Zarządem Głównym PTI są odpowiedzialni za zapewnienie zasobów niezbędnych dla opracowania, wdrożenia, funkcjonowania, utrzymania i doskonalenia bezpieczeństwa Systemu oraz poszczególnych zabezpieczeń;
- **prezes PTI** jest upoważniony do wydawania zgodę na użytkowanie urządzeń służących do przetwarzania informacji i zabezpieczeń rekomendowanych przez ABI, decyduje również o współpracy z innymi podmiotami w zakresie bezpieczeństwa;
- **prezes PTI** (lub osoba przez niego upoważniona) może wyrazić zgodę na udostępnienie stronom trzecim informacji stanowiących tajemnicę towarzystwa;
- **administrator bezpieczeństwa informacji** jest odpowiedzialny za wdrożenie wymaganych zabezpieczeń mających za zadanie zapewnienie bezpieczeństwa informacji oraz realizacji działań wynikających z procedur;
- **administrator IT** odpowiada za techniczne aspekty aktywów w ścisłej współpracy z właścicielami aktywów i administratorem bezpieczeństwa informacji;
- **właściciele aktywów** odpowiadają za bieżące nadzorowanie oraz zarządzanie aktywami.

6 Ogólne zasady bezpieczeństwa informacji przetwarzanych w ramach Systemu

1. ZG PTI jest odpowiedzialny za tworzenie, wdrożenie i utrzymanie polityki bezpieczeństwa informacji, oraz wynikających z niej standardów, zaleceń i procedur.

2. ZG PTI ma świadomość konieczności ponoszenia nakładów finansowych w celu zapewnienia właściwej ochrony informacji. Metody i środki zabezpieczeń są dobierane i wdrażane w sposób kompleksowy w oparciu o rezultaty szacowania ryzyka. Zapewni to osiągnięcie wymaganego poziomu bezpieczeństwa przy jednoczesnej optymalizacji kosztów.

3. Wszystkie aktywa informacyjne zostały zinwentaryzowane i wyznaczeni zostali ich właściciele. W celu osiągnięcia i utrzymania odpowiedniego poziomu ochrony aktywów zostanie wdrożony proces zarządzania aktywami informacyjnymi.

4. W celu zapewnienia prawidłowej i bezpiecznej eksploatacji systemu IT zostaną opracowane i ustanowione wszystkie wymagane procedury administracyjne.

5. Ochrona informacji przetwarzanych w ramach Systemu obowiązuje wszystkie osoby, które mają do nich dostęp, bez względu na zajmowane stanowisko oraz miejsce wykonywania, jak również charakter stosunku prawnego wiążącego daną osobę z PTI.

6. Osoby mające dostęp do informacji gromadzonych i przetwarzanych w systemie teleinformatycznym są zobowiązane do stosowania wymaganych zabezpieczeń chroniących przed ujawnieniem tych informacji osobom nieupoważnionym.

7. Zachowanie tajemnicy PTI obowiązuje zarówno podczas trwania stosunku prawnego, jak i po jego ustaniu przez okres dwóch lat.

8. Polecenia osób wyznaczonych przez ZG PTI do działań związanych z zapewnieniem ochrony informacji i bezpieczeństwa Systemu muszą być bezwzględnie wykonywane przez wszystkie osoby związane z Systemem PTI.

9. Informacje są chronione z należytą starannością i w sposób adekwatny do ich wartości. Do ochrony informacji są wykorzystywane, w zależności od potrzeb i możliwości, zabezpieczenia techniczne, organizacyjno-proceduralne i fizyczne.

10. Ochrona informacji w systemie teleinformatycznym PTI polega na kontroli dostępu do niej, który jest regulowany na podstawie analizy potrzeb biznesowych i wymagań bezpieczeństwa. Aktywa informacyjne oraz środki ich przetwarzania mogą być wykorzystywane wyłącznie do celów służbowych.

11. Mechanizmy kontroli dostępu w systemach, aplikacjach i urządzeniach IT są konfigurowane ze szczególną starannością. Dotyczy to w szczególności punktów dostępu do Internetu.

12. Wymagania bezpieczeństwa dla nowo pozyskiwanych składników systemu teleinformatycznego PTI (oprogramowanie, sprzęt, itp.) powinny być zidentyfikowane na etapie opracowania

wymagań projektowych oraz powinny być uzasadnione, uzgodnione i udokumentowane jako część ogólnego modelu systemu IT i jego architektury bezpieczeństwa.

13. Zdarzenia związane z bezpieczeństwem informacji oraz wykryte słabości systemów informacyjnych należy zgłaszać umocowanej osobie niezwłocznie po ich zaobserwowaniu. W razie wątpliwości kim jest osoba umocowana zgłoszenie należy przekazać prezesowi PTI lub jednemu z wiceprezesów PTI. W celu minimalizowania skutków zdarzeń związanych z bezpieczeństwem informacji zostaną wdrożone formalne procedury zgłaszania i eskalowania zdarzeń.

14. W celu przeciwdziałania przerwom w funkcjonowaniu Systemu konieczne jest wdrożenie procesu zarządzania ciągłością działania.

15. W ramach eksploatacji systemu IT używane jest tylko legalne oprogramowanie. Nie dopuszcza się stosowania oprogramowania z naruszeniem warunków ich licencji i prawa autorskiego.

16. Wszystkie systemy operacyjne funkcjonujące w infrastrukturze informatycznej PTI są chronione przed szkodliwymi programami przez oprogramowanie antywirusowe z ważną subskrypcją sygnatur.

17. Każda osoba związana z eksploatacją i rozwojem systemu IT jest zapoznawana z zasadami oraz z aktualnymi procedurami ochrony informacji.

18. Współpracownicy PTI biorący udział w eksploatacji i rozwoju Systemu są zapoznani z regułami oraz z aktualnymi procedurami ochrony informacji w zakresie niezbędnym do realizacji ich zadań.

19. Zasady bezpieczeństwa przedstawione w niniejszym dokumencie mają zastosowanie także wobec firm trzecich, współpracujących w eksploatacji i rozwoju Systemu. Znajduje to swoje odzwierciedlenie w umowach zawieranych pomiędzy PTI a tymi podmiotami.

20. Urządzenia i okablowanie wchodzące w skład sieci lokalnych PTI są zlokalizowane w obszarach chronionych fizycznie. Ich umieszczenie i eksploatacja poza obszarami chronionymi fizycznie jest możliwa po zastosowaniu odpowiednich zabezpieczeń gwarantujących poufność, integralność i dostępność danych, stosownie do ich wrażliwości i krytyczności.

21. Podstawę egzekwowania od osób związanych z Systemem IT zasad przestrzegania Polityki Bezpieczeństwa Informacji, w tym ochrony tajemnicy towarzystwa, stanowią odpowiednio kodeks pracy, regulamin pracy, porozumienia kontraktowe oraz statut PTI i właściwe uregulowania wewnętrzne. W relacjach kontraktowych, gdzie zastosowanie ma kodeks cywilny, należy stosować klauzule odpowiedzialności umownej za przestrzeganie zasad Polityki Bezpieczeństwa Informacji.

22. Naruszenie Polityki Bezpieczeństwa Informacji powoduje skutki prawne zgodne z Regulaminem Pracy lub porozumieniem kontraktowym, a w przypadkach zastrzeżonych przez ustawodawcę – karne wynikające z odpowiedzialności określonej przez prawo.

7 Szczegółowe zasady bezpieczeństwa

Szczegółowe zasady bezpieczeństwa informacji przetwarzanych w ramach Systemu IT PTI, dla każdej z dziedzin bezpieczeństwa, określają dokumenty polityk niższego rzędu, procedury i instrukcje (wymienione w rozdziale 9.1) oraz uchwały, zarządzenia i decyzje ZG PTI.

8 Audyty bezpieczeństwa

W celu weryfikacji przestrzegania Polityki Bezpieczeństwa Informacji należy przeprowadzać audyty bezpieczeństwa.

Audyty okresowe powinny być przeprowadzane nie rzadziej niż jeden raz w roku. Dodatkowe audyty bezpieczeństwa powinny być przeprowadzane w przypadku wystąpienia poważnych incydentów bezpieczeństwa lub dokonaniu istotnych modyfikacji systemu teleinformatycznego.

Przeprowadzany audyt powinien być oparty o analizę ryzyka.

W zależności od potrzeb, część prac w ramach audytu można zlecić kompetentnemu i zaufanemu podmiotowi zewnętrznemu.

9 Dokumentacja Polityki

9.1 Dokumenty uzupełniające

Dokumentami uzupełniającymi Politykę Bezpieczeństwa Informacji są:

1. Regulamin użytkowania sieci komputerowej i systemów informatycznych
2. Polityka bezpieczeństwa danych osobowych
3. Procedura zarządzania ryzykiem bezpieczeństwa informacji
4. Procedura postępowania z incydentami bezpieczeństwa

9.2 Dostępność

Charakter i przesłanie informacji zawartych w Polityce Bezpieczeństwa Informacji determinuje konieczność udostępnienia tego dokumentu wszystkim pracownikom PTI, którzy w ramach swoich obowiązków wykonują zadania związane z gromadzeniem i przetwarzaniem informacji. Dokument ten powinien zostać udostępniony również współpracownikom PTI, jeżeli charakter ich pracy ma wpływ na bezpieczeństwo informacji.

9.3 Zasady wprowadzania zmian

Dokumentacja Polityki Bezpieczeństwa Informacji powinna być przeglądana i weryfikowana:

- na polecenie prezesa PTI,
- w przypadku wystąpienia poważnych incydentów naruszenia bezpieczeństwa,
- w celu realizacji rekomendacji i zaleceń wynikających z przeprowadzonych audytów,
- w przypadku ogłoszenia nowych lub modyfikacji istniejących przepisów odnoszących się do zasad ochrony aktywów informacyjnych PTI, ze szczególnym uwzględnieniem informacji gromadzonych i przetwarzanych w ramach Systemu,
- w przypadku poważnych modyfikacji Systemu,
- w przypadku zawarcia umów, z których wynikają zobowiązania związane z bezpieczeństwem informacji,
- okresowo, nie rzadziej niż 1 raz w roku.

10 Zgodność z prawem

Polityka Bezpieczeństwa Informacji jest zgodna z następującymi aktami prawnymi, normami i standardami:

- [UODO] Ustawa z dnia 29 sierpnia 1997 o ochronie danych osobowych (Dz.U. nr 133/97 poz. 883).
- [UPA] Ustawa z dnia 4 lutego 1994 o prawie autorskim i prawach pokrewnych (Dz.U. z 1994 nr 24, poz. 83, z późn. zm.).
- [13335-1] PN-I-13335-1 Technika informatyczna – Wytyczne do zarządzania bezpieczeństwem systemów informatycznych – Model ogólny.
- [13335-2] TR ISO/IEC 13335-2 Technika informatyczna – Wytyczne do zarządzania bezpieczeństwem systemów informatycznych – Zarządzanie i planowanie bezpieczeństwa informatycznego.
- [13335-3] TR ISO/IEC 13335-3 Technika informatyczna - Wytyczne do zarządzania bezpieczeństwem systemów informatycznych – Techniki zarządzania bezpieczeństwem systemów informatycznych.
- [17799] PN-ISO/IEC 17799 Technika informatyczna – Praktyczne zasady zarządzania bezpieczeństwem informacji.
- [7799-2] PN-I-07799-2 Systemy zarządzania bezpieczeństwem informacji – Specyfikacja i wytyczne do stosowania.

11 Podstawa wewnętrzna

Niniejsza Polityka Bezpieczeństwa Informacji została wprowadzona uchwałą Zarządu Głównego PTI nr 075e/XI/12 z dnia 11 sierpnia 2012 r.