Polityka Bezpieczeństwa Informacji

Instytut Strat Wojennych im. Jana Karskiego

Warszawa 31-07-2022

WPROWADZENIE

Poniższy dokument określa założenia i jednolitą strategię ochrony informacji w Instytucie Strat Wojennych im. Jana Karskiego (ISW). Definiuje cele ochrony informacji, zakres tej ochrony, przypisuje odpowiedzialność i kompetencje oraz określa strukturę mającą za zadanie realizację programu ochrony informacji, a także określa zadania dla poszczególnych jednostek tej struktury.

Niniejsza Polityka jest dokumentem głównym ustanowionego Systemu Zarządzania Bezpieczeństwem Informacji.

DEFINICJE

Autentyczność – zapewnienie, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana (autentyczność dotyczy użytkowników, procesów, systemów i informacji).

Dane osobowe – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"), gdzie poprzez możliwą do zidentyfikowania osobę fizyczną rozumie się osobę, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

Deklaracja – dokument, w którym opisuje się cele stosowania zabezpieczeń oraz zabezpieczenia, które mają zastosowanie w SZBI w danej jednostce organizacyjnej.

Dostępność – zapewnienie bycia osiągalnym i możliwym do wykorzystania na żądanie, w założonym czasie, przez autoryzowany podmiot.

Integralność – zapewnienie, że dane nie zostały zmienione w sposób nieautoryzowany.

Niezaprzeczalność – zapewnienie braku możliwości wyparcia się swego uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie.

Poufność – zapewnienie, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom lub podmiotom.

Przetwarzanie danych osobowych - operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

RODO – Rozporządzenie Parlamentu Europejskiego i Rady 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).

Rozliczalność – właściwość systemu pozwalająca przypisać określone działanie w systemie do osoby fizycznej lub procesu oraz umiejscowić je w czasie.

Ryzyko – przyszłe, możliwe zdarzenie, które – w razie wystąpienia – może mieć negatywny wpływ na realizację zadań lub celów ISW.

SZBI lub System – System Zarządzania Bezpieczeństwem Informacji.

Zarządzanie ryzykiem – skoordynowane działania mające na celu identyfikację i analizę ryzyka, a także – poprzez zastosowanie odpowiednich zabezpieczeń – minimalizację zagrożeń wynikających z ryzyka do poziomu akceptowalnego.

I. DEKLARACJA STOSOWANIA

Dyrektor Instytutu Strat Wojennych im. Jana Karskiego (ISW), będąc jednocześnie Administratorem Danych Osobowych przetwarzanych w ISW, realizując obowiązki w zakresie zapewnienia bezpieczeństwa informacji ze szczególnym uwzględnieniem danych osobowych oraz z 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. 2017 poz. 2247 z pózn. zm.), promuje i aktywnie wspiera przyjęte w ISW zasady przetwarzania informacji. Wyrazem zaangażowania i wsparcia Dyrektora Instytutu Strat Wojennych im. Jana Karskiego (ISW) dla zagwarantowania bezpieczeństwa informacji jest podjęcie decyzji o wdrożeniu, utrzymaniu i doskonaleniu Systemu Zarządzania Bezpieczeństwem Informacji opracowanego na podstawie normy PN-ISO/IEC 27001:2017. Przyjęte reguły i zasady postępowania dotyczą wszystkich pracowników ISW, wykonawców usług i dostaw, jak również innych podmiotów współpracujących z ISW, które w ramach realizacji zawartych umów i na czas ich realizacji muszą uzyskać dostęp do danych. Przyjęte zasady obowiązują niezależnie od formy przetwarzania informacji. Odpowiedzialność za przygotowanie i utrzymanie Systemu Zarządzania Bezpieczeństwem Informacji oraz koordynację podejmowanych działań i ciągłe doskonalenie Systemu spoczywa na powołanym przez Dyrektora ISW, zespole do spraw wdrożenia i utrzymania SZBI.

II. CELE BEZPIECZEŃSTWA INFORMACJI

Celem Systemu Zarządzania Bezpieczeństwem Informacji jest zapewnienie ochrony danych osobowych oraz innych informacji przetwarzanych w Instytucie Strat Wojennych im. Jana Karskiego (ISW) przed wszelkiego rodzaju zagrożeniami, zarówno wewnętrznymi, jak i zewnętrznymi, w szczególności zagwarantowanie dostępności, integralności, poufności, rozliczalności oraz autentyczności i niezaprzeczalności danych. Zapewnienie, że przetwarzanie informacji odbywa się w zgodzie z obowiązującymi przepisami prawa oraz zawartymi umowami w sposób nie naruszający praw i wolności osób. Ustanowione cele bezpieczeństwa są zgodne i wspierają cele strategiczne i operacyjne realizowane przez ISW.

Wśród głównych celów SZBI należy wymienić przede wszystkim:

● ustalenie najważniejszych zasad w zakresie bezpieczeństwa informacji,

● przygotowanie pracowników ISW do właściwych zachowań dotyczących bezpieczeństwa informacji,

● określenie zakresów odpowiedzialności w obrębie systemu bezpieczeństwa i poziomów dostępności do informacji poszczególnych grup pracowników ISW,

● wpływ na budowanie świadomości bezpieczeństwa informacji wśród pracowników ISW. Powyższe cele realizowane są poprzez:

- wyznaczenie osób odpowiedzialnych, zapewniających optymalny podział i koordynację zadań związanych z zapewnieniem bezpieczeństwa informacji,

- zobligowanie pracowników ISW, którzy przetwarzają informacje (bez względu na formę ich przetwarzania) do zapewnienia im optymalnego poziomu bezpieczeństwa,

- przyjęcie za obowiązujące, przez wszystkich pracowników ISW, zasad opisanych w omawianym dokumencie,

- ciągłe doskonalenie SZBI zgodnie z wymaganiami Polskiej Normy PN-ISO/IEC 27001:2017.

III. KONTEKST ORGANIZACJI

Instytut Strat Wojennych im. Jana Karskiego (ISW) jako państwowa jednostka budżetowa realizuje zadania wynikające z następujących przepisów prawa:

● Zarządzenie nr 321 Prezesa Rady Ministrów z dnia 2 grudnia 2021 r. w sprawie utworzenia Instytutu Strat Wojennych im. Jana Karskiego M.P. 2021 poz. 1126

IV. CZYNNIKI ZEWNĘTRZNE

W ramach uwarunkowań zewnętrznych, uwzględnia się w szczególności:

● obowiązujący porządek prawny i konieczność zapewnienie zgodności z obowiązującymi przepisami prawa,

● uwarunkowania ekonomiczne, technologiczne, naturalne, kulturowe, społeczne, polityczne,

● oczekiwania klientów i kontrahentów mające wpływ na sposób realizacji celów strategicznych

ISW,

● relacje i kontakty z zewnętrznymi podmiotami publicznymi i prywatnymi (w tym umowy z kontrahentami i dostawcami),

● wizerunek ISW.

V. CZYNNIKI WEWNĘTRZNE

W ramach uwarunkowań wewnętrznych, uwzględnia się w szczególności:

● strukturę organizacyjną ISW, podział kompetencji, ustanowione role i przypisane odpowiedzialności,

● przyjęte cele oraz kierunki działania i rozwoju,

● wewnętrzne zarządzenia, regulaminy i przyjęte standardy,

● charakter wykonywanych zadań i procesów,

● zasoby wykorzystywane do skutecznej realizacji powierzonych zadań i procesów (m.in. budżet,

wiedza, pracownicy, budynki i pomieszczenia ISW, systemy teleinformatyczne),

● relacje wewnętrzne i komunikację (m.in. przepływ informacji w formie tradycyjnej i za pośrednictwem systemu teleinformatycznego).

VI. ZAINTERESOWANE STRONY

Przyjęte reguły i zasady przetwarzania informacji dotyczą wszystkich pracowników ISW oraz

wykonawców usług i dostaw, jak również innych podmiotów współpracujących z ISW, które w ramach

realizacji zawartych z ISW umów i na czas ich realizacji muszą uzyskać dostęp do danych.

Przyjęte zasady obowiązują niezależnie od formy przetwarzania informacji. Interesariuszami

Systemu Zarządzania Bezpieczeństwem Informacji są w szczególności:

- Osoby fizyczne i prawne będące klientami ISW,
- Pracownicy ISW,
- Organy administracji rządowej i samorządowej,
- Podmioty realizujące zadania w imieniu i na rzecz ISW, dostawcy oraz kontrahenci.

VII. PODSTAWY PRAWNE

Podstawą do opracowania i wdrożenia niniejszej polityki jest:

● RODO

● Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (tekst jedn. Dz. U. z 2018 r., poz. 1000 ze zm.)

● Rozporządzenie Rady Ministrów w sprawie Krajowych Ramach Interoperacyjności minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej (Dz.U. 2017 poz. 2247),

● Krajowa Norma PN-ISO/IEC-27001:2017.

VIII. ZAKRES SYSTEMU

Zakres ustanowionego Systemu Zarządzania Bezpieczeństwem Informacji obejmuje:

- Informacje przetwarzane w ramach wszelkich realizowanych w ISW procesów i zadań (czynności przetwarzania), zarówno w postaci tradycyjnej (m.in. informacje wydrukowane lub zapisane na papierze), jak i elektronicznej oraz przekazywane werbalnie.

- Aktywa wspierające przetwarzanie informacji w ramach ww. procesów oraz realizowanych zadań, w tym: personel (wszyscy pracownicy ISW bez względu na podstawę zatrudnienia, praktykanci, stażyści, wolontariusze oraz inne osoby), podmioty zewnętrzne wykonujące czynności w imieniu i na rzecz ISW i/lub mające dostęp do aktywów informacyjnych ISW, budynki i pomieszczenia ISW, w których są przetwarzane informacje, sprzęt, w tym sprzęt komputerowy, urządzenia mobilne oraz inne nośniki danych, na których znajdują się informacje podlegające ochronie, oprogramowanie, infrastruktura sieciowa, systemy informatyczne, oprogramowanie narzędziowe stanowiące składowe systemów teleinformatycznych wykorzystywanych do przetwarzania informacji Niniejsza Polityka i opisane w niej zasady nie dotyczą informacji przetwarzanych na podstawie ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (t.j. Dz. U. z 2016 r. poz. 1167, 1948, z 2017 r. poz. 935.).

IX. CIĄGŁE DOSKONALENIE SYSTEMU

Wdrożony i utrzymywany w ISW, System Zarządzania Bezpieczeństwem Informacji podlega cyklicznym (nie rzadziej niż raz do roku) przeglądom i poddawany jest audytom nadzoru oraz audytom wewnętrznym. Oparty jest na ciągłym procesie zarządzania ryzykiem realizowanym zgodnie z wdrożoną Instrukcją Zarządzania Ryzykiem.

X. STRUKTURA KLASYFIKACJI DOKUMENTACJI SZBI

W ramach ustanowionego SZBI wprowadza się trójpoziomową klasyfikację dokumentacji bezpieczeństwa określającą zasady i tryb zarządzania bezpieczeństwem informacji oraz aktywów wspierających przedmiotowe przetwarzanie w ISW:

1. W ramach I poziomu SZBI (dokumenty o charakterze publicznym, ogólnodostępnym)

wyróżnia się:

a) „Politykę Bezpieczeństwa Informacji ISW" – dokument główny: dokument nadrzędny w stosunku do pozostałych wewnętrznych aktów prawnych dotyczących bezpieczeństwa informacji obowiązujących w ISW, tworzących wspólnie dokumentację bezpieczeństwa, określający ogólne ramy, kierunki, zasady i wymogi bezpieczeństwa informacji w ISW oraz zakres dokumentacji bezpieczeństwa na pozostałych poziomach, wprowadzony i aktualizowany w formie zarządzenia Dyrektora Instytutu Strat Wojennych im. Jana Karskiego

2. W ramach II poziomu SZBI (dokumenty udostępniane wszystkim pracownikom ISW, praktykantom, stażystom, wolontariuszom, w uzasadnionych przypadkach wybranym osobom i podmiotom zewnętrznym wykonującym czynności w imieniu i na rzecz ISW i/lub mającym dostęp do aktywów informacyjnych ISW) wyróżnia się polityki tematyczne:

a) zawierające uszczegółowienie zapisów polityki I poziomu SZBI,

b) określające specyficzne wymogi i zasady bezpieczeństwa w kluczowych obszarach bezpieczeństwa informacji,

c) określane i aktualizowane przez Dyrektora Instytutu Strat Wojennych im. Jana Karskiego.

3. W ramach III poziomu SZBI (dokumenty dedykowane i udostępniane wybranym osobom

i podmiotom na zasadzie „wiedzy uzasadnionej") wyróżnia się:

a) wybrane procedury i instrukcje wykonawcze:

- określające zasady i sposób realizacji wymogów w obszarach uregulowanych na II poziomie SZBI w danej komórce organizacyjnej/przez dany podmiot zewnętrzny wykonujący czynności w imieniu i na rzecz ISW,

b) wybrane umowy ze stronami trzecimi.

4. Dokumenty opracowywane na poszczególnych poziomach SZBI uzupełniają się wzajemnie, tworząc kompleksową dokumentację Systemu Zarządzania Bezpieczeństwem Informacji w ISW (dokumentację bezpieczeństwa):

1) dokumentacja I poziomu SZBI ma charakter ogólny, a jej zapisy odwołują się do dokumentów II poziomu, w których są uszczegółowione,

2) poszczególne dokumenty II poziomu odwołują się do siebie oraz do procedur i instrukcji III poziomu.

3) procedury i instrukcje III poziomu SZBI uszczegóławiają wybrane kwestie zidentyfikowane w ramach dokumentacji II poziomu.

5. Celem zapewnienia właściwości, adekwatności i skuteczności obowiązujących przepisów

wewnętrznych w zakresie bezpieczeństwa, prowadzone są okresowe przeglądy i aktualizacja ww. dokumentacji. Zasady oraz tryb prowadzenia przedmiotowych przeglądów dokumentacji SZBI uregulowano w Polityce monitorowania i nadzoru nad bezpieczeństwem informacji.

XI. ROLE I ODPOWIEDZIALNOŚCI W ZAKRESIE BEZPIECZEŃSTWA INFORMACJI

ADO - Administrator Danych Osobowych – Dyrektor Instytutu Strat Wojennych im. Jana Karskiego odpowiedzialny za wdrożenie i bieżący nadzór nad procesem przetwarzania danych osobowych, decydujący o celach i środkach przetwarzania danych osobowych. ADO zapewnia bezpieczeństwo przetwarzania informacji, ze szczególnym uwzględnieniem danych osobowych, poprzez zastosowanie środków technicznych i organizacyjnych adekwatnych do występujących ryzyk oraz kategorii danych objętych ochroną. W szczególności zapewnia środki i zasoby umożliwiające wdrożenie oraz utrzymanie Systemu Zarządzania Bezpieczeństwem Informacji, jak również zabezpieczeń danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, zmianą, utratą, uszkodzeniem i zniszczeniem.

IOD - Inspektor Ochrony Danych – osoba wyznaczona przez Dyrektora Instytutu Strat Wojennych im. Jana Karskiego do nadzorowania przestrzegania zasad ochrony danych osobowych.

Do obowiązków Inspektora Ochrony Danych należy:

1. Ustalanie standardów i zakresu dokumentowania SZBI;

2. Udział w przygotowaniu oraz opiniowanie poszczególnych polityk, procedur i standardów stanowiących składowe obowiązującej dokumentacji SZBI lub określanie odpowiedzialnych za ww. czynności Zarządzających właściwymi merytorycznie komórkami organizacyjnymi;

3. Zapoznanie pracowników z przepisami i obowiązującymi zasadami przetwarzania informacji, w szczególności danych osobowych.

4. Prowadzenie rejestru czynności przetwarzania i kategorii czynności przetwarzania danych osobowych.

5. Nadzorowanie prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych.

6. Bezzwłoczne podejmowanie działań w przypadku otrzymania informacji o:

a. nieprawidłowej pracy systemu przetwarzającego dane osobowe,

b. wystąpieniu sytuacji wskazującej na możliwość naruszenia bezpieczeństwa danych.

7. Opracowywanie i wdrażanie programu szkoleń pracowników zatrudnionych przy przetwarzaniu danych osobowych w zakresie przepisów o ochronie danych osobowych.

8. Udział w procesie oceny skutków przetwarzania.

KADRA ZARZĄDZAJĄCA - (dyrektor i zastępcy dyrektora ISW, kierownicy komórek organizacyjnych) odpowiedzialni są za zapewnienie i nadzorowanie zgodności realizowanych w podległych im komórkach organizacyjnych zadań z obowiązującymi zasadami przetwarzania informacji.

W szczególności odpowiedzialni są za:

1. aktualność informacji kadrowych i kontaktowych podległych pracowników,

2. aktualność i adekwatność upoważnień do przetwarzania danych osobowych posiadanych przez pracowników podległych im komórek organizacyjnych,

3. aktualność i adekwatność uprawnień do pracy w systemach informatycznych posiadanych przez pracowników podległych im komórek organizacyjnych,

4. aktualność rejestru czynności przetwarzania i kategorii czynności przetwarzania w zakresie przypisanym do komórki organizacyjnej,

5. Zarządzanie dostępem podległych pracowników do pomieszczeń,

6. Informowanie IOD z odpowiednim wyprzedzeniem o nowych planowanych czynnościach przetwarzania,

7. Określenie zakresu gromadzonych danych niezbędnych dla realizacji przydzielonych zadań,

8. Określenie wrażliwości i krytyczności gromadzonych danych ze względu na poufność, integralność i dostępność,

9. Poprawność merytoryczną gromadzonych danych tworzonych przez podległą komórkę organizacyjną,

10. Określenie rodzaju aplikacji oraz urządzeń komputerowych, które są niezbędne do gromadzenia danych,

11. Przygotowanie i przedkładanie zapotrzebowania w zakresie zakupu urządzeń komputerowych, peryferyjnych i oprogramowania,

12. Współpracę z IOD, ASI w sytuacji wystąpienia naruszenia bezpieczeństwa,

ASI - Administratorzy Systemów Informatycznych - wskazani pracownicy odpowiedzialni za wdrażanie i utrzymanie zabezpieczeń technicznych i organizacyjnych dotyczących systemów informatycznych.

Pracownicy ISW zobowiązani są do:

a. zapoznania się i stosowania zasad przyjętych w Polityce Bezpieczeństwa Informacji, oraz

innych politykach, standardach i regulaminach stanowiących dokumentację SZBI.

b. niezwłocznego informowanie IOD o incydentach lub zagrożeniach bezpieczeństwa danych

osobowych.

c. chronienia informacji przed dostępem do nich osób nieuprawnionych, przed przypadkowym

lub umyślnym zniszczeniem, utratą lub modyfikacją,

d. zachowania w tajemnicy informacji, z którymi zapoznali się w związku z pełnioną funkcją lub

wykonywaną pracą,

e. chronienia sprzętu, wydruków komputerowych i innych nośników zawierających informacje,

f. do regularnego podłączania sprzętu do sieci LAN, w celu pobierania m.in. aktualizacji

systemów AV,

g. utrzymywania w tajemnicy powierzonych haseł, informacji o częstotliwości ich zmiany oraz

szczegółach technicznych systemów, także po ustaniu zatrudnienia w ISW,

h. zgodnie z obowiązującą dokumentacją bezpieczeństwa dla danego zbioru danych,

powiadamiania IOD i bezpośredniego przełożonego o:

● ujawnieniu lub możliwości ujawnienia informacji osobom nieupoważnionym,

● nieautoryzowanej zmianie informacji chronionych lub możliwości wprowadzenia

nieautoryzowanych zmian,

● zniszczeniu lub możliwości zniszczenia informacji, zgodnie z obowiązującą dokumentacją bezpieczeństwa dla danego systemu, powiadamiania ASI i bezpośredniego przełożonego o:

● zablokowaniu lub możliwości zablokowania pracy systemu informatycznego przetwarzającego informacje lub uniemożliwienia innego dostępu do nich,

● możliwości wystąpienia awarii systemów,

● zakłóceniach w działaniu systemów informatycznych.

Zabrania się:

● ujawniania informacji osobom nieuprawnionym,

● ujawniania, przekazywania identyfikatorów i haseł lub wykorzystywania uprawnień,

identyfikatorów oraz haseł innych pracowników,

● wynoszenia dokumentów oraz składników majątkowych poza siedzibę ISW niezgodnie z regulacjami wewnętrznymi,

● kopiowania bazy danych lub ich części poza kopiami przewidzianymi dokumentacją

bezpieczeństwa,

● zakłócania pracy systemu informatycznego lub sieci teleinformatycznej,

● przetwarzania informacji w sposób mogący narażać na utratę bezpieczeństwa danych,

● przetwarzania na stacjach roboczych i publikowania w Internecie treści sprzecznych z prawem

lub normami współżycia społecznego,

● instalowania oprogramowania niezwiązanego z wykonywaniem obowiązków służbowych,

● ingerowania w konfigurację sprzętową urządzeń,

● wykorzystywania sprzętu służbowego niezgodnie z zasadami określonymi w odpowiednich

dokumentach SZBI.

XII. ZASADY PRZETWARZANIA INFORMACJI

Mając na celu jak najlepsze zabezpieczenie informacji i aktywów wspierających ich przetwarzanie wprowadza się do stosowania następujące zasady bezpieczeństwa informacji:

1. Zasada ograniczenia celu - dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami. Cel ten musi być określony w momencie ich pozyskiwania (art. 5 ust.1 lit. b RODO).

2. Zasada zgodności z prawem, rzetelności i przejrzystości - dane osobowe muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dotyczą. Wszelkie informacje i komunikaty związane z przetwarzaniem muszą być łatwo dostępne i zrozumiałe oraz sformułowane jasnym i prostym językiem (art. 5 ust. 1 lit. a i motyw 39 RODO).

3. Zasada minimalizacji danych - pozyskiwane mogą być jedynie dane adekwatne i niezbędne dla osiągnięcia celów konkretnych, uzasadnionych i określonych w momencie zbierania danych. Nie można zbierać danych osobowych, które nie mają związku z celem przetwarzania, są nadmiarowe lub już nieprzydatne - np. ze względu na ich nieaktualność (art. 5 ust. 1 lit. C i motyw 39 RODO).

4. Zasada prawidłowości danych - dane osobowe muszą być prawidłowe i w razie potrzeby uaktualniane. Należy podejmować wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane (art. 5 ust. 1 lit. d RODO).

5. Zasada ograniczenia czasowego - dane osobowe muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, dla których dane te są przetwarzane. Przechowywanie danych zgromadzonych np. w celu realizacji umowy powinno być zakończone w momencie przedawnienia roszczeń czy innych praw i obowiązków wynikających z przepisów prawa (art. 5 ust. 1 lit. e RODO).

6. Zasada integralności i poufności - dane osobowe muszą być przetwarzane w sposób zapewniający im odpowiednie bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych (art. 5 ust.1 lit. f RODO).

7. Zasada ograniczonego przetwarzania - podmiot przetwarzający oraz każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego i mająca dostęp do danych osobowych przetwarzają je wyłącznie na polecenie administratora, przez co rozumie się przetwarzanie na podstawie i w zakresie udzielonego upoważnienia lub zawartej umowy powierzenia przetwarzania danych osobowych (art. 29 RODO).

8. Zasada rozliczalności - wszelkie czynności i decyzje związane z SZBI muszą być dokumentowane. Działania związane z przetwarzaniem danych (w szczególności decyzje dotyczące zarządzania dostępem do informacji lub zasobów służących do jej przetwarzania) muszą być dokumentowane lub powodować tworzenie zapisów pozwalających na ocenę zgodności podejmowanych działań z przyjętymi zasadami.

9. Zasada odpowiedzialności – odpowiedzialność za czynności przetwarzania, podejmowanie decyzji o dostępie do informacji, dokumentacja, procesy i środki przetwarzania musza być jednoznacznie przypisane do pracowników lub komórek organizacyjnych.

10. Zasada wiedzy koniecznej – możliwość uzyskania dostępu do informacji wyłącznie w zakresie i w ramach realizowanych obowiązków służbowych lub zapisów umowy.

11. Zasada identyfikowalności – osoby, procesy, urządzenia uzyskujące dostęp do informacji lub zasobów służących do jej przetwarzania muszą być w sposób jednoznaczny identyfikowalne.

12. Zasada uwierzytelnienia – mechanizmy kontroli dostępu osoby, procesu, urządzenia do informacji lub zasobów służących do jej przetwarzania muszą wykorzystywać właściwe środki uwierzytelniające oraz zapewniać bezpieczeństwo informacji uwierzytelniających.

13. Rozdzielenie obowiązków – rozdzielenie obowiązków związanych z podejmowaniem decyzji związanych z dostępem do informacji oraz zasobów wykorzystywanych do jej przetwarzania od obowiązków związanych z techniczną ich realizacją.

14. Zasada uwzględnienia ochrony danych w fazie projektowania – wdrożenie nowej czynności przetwarzania (w szczególności z wykorzystaniem narzędzi informatycznych) musi być poprzedzone fazą planowania obejmującą analizę związanych z nią ryzyk oraz uwzględnienie odpowiednich zabezpieczeń.

15. Zasada domyślnej ochrony - domyślnie przetwarzane mogą być wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności.

16. Zasada adekwatności zabezpieczeń – stosowane zabezpieczenia muszą być adekwatne do zidentyfikowanych zagrożeń.

17. Zasada uprawnionego dostępu – korzystanie z aktywów informacyjnych ISW odbywać się może tylko w oparciu o formalne uprawnienia do korzystania z wybranych aktywów.

18. Dodatkowe zasady bezpieczeństwa mogą zostać określone w pozostałych dokumentach wchodzących w skład dokumentacji bezpieczeństwa.

XIII. KONTROLA DOSTĘPU DO INFORMACJI

1. W ramach zapewnienia ograniczonego dostępu do aktywów informacyjnych ISW, w tym do budynków i pomieszczeń, sprzętu oraz systemów informatycznym tylko dla osób i podmiotów uprawnionych, prowadzona jest kontrola dostępu fizycznego i logicznego.

2. Szczegółowe zasady zarządzania dostępem do aktywów informacyjnych ISW zostały uregulowane w odpowiednich politykach odnoszących się do bezpieczeństwa fizycznego i środowiskowego oraz bezpieczeństwa teleinformatycznego.

XIV. ZARZĄDZANIE AKTYWAMI INFORMACYJNYMI

W celu zapewnienia adekwatnego poziomu bezpieczeństwa aktywów informacyjnych, przedmiotowe aktywa są inwentaryzowane, klasyfikowane i zarządzane zgodnie z obowiązującymi wymaganiami w zakresie ich ochrony.

XV. ZARZĄDZANIE RYZYKIEM

1. W celu skutecznego zarządzania bezpieczeństwem informacji wymagane jest podejmowanie okresowych działań w obszarze zarządzania ryzykiem, w szczególności w zakresie szacowania tj. identyfikowania, analizy i oceny ryzyka w bezpieczeństwie informacji, zmierzających do ograniczenia oraz eliminacji przedmiotowego ryzyka.

2. Działania związane z zarządzaniem ryzykiem mającym wpływ na bezpieczeństwo informacji obejmują w szczególności:

a) przygotowanie oraz okresową aktualizację dokumentów dot. zarządzania ryzykiem,

b) prowadzenie okresowego szacowania ryzyka,

c) postępowanie z ryzykiem,

d) podejmowanie działań korygujących.

3. Szczegółowe zasady dotyczące zarządzania ryzykiem w bezpieczeństwie informacji zostały uregulowane w Instrukcji zarządzania ryzykiem.

XVI. BEZPIECZEŃSTWO TELEINFORMATYCZNE

1. W ramach zarządzania bezpieczeństwem teleinformatycznym podejmowane są działania w zakresie szacowania i kontroli ryzyka utraty poufności, integralności, dostępności informacji w związku z korzystaniem z Systemów Informatycznych administrowanych przez ISW oraz aplikacji, komputerów i urządzeń mobilnych, sieci komputerowych i transmisji danych.

2. Przedmiotowe działania podejmowane są w szczególności w zakresie monitorowania, doskonalenia i rozwoju, infrastruktury teleinformatycznej.

3. Szczegółowe zasady i wymogi w zakresie bezpieczeństwa teleinformatycznego zostały uregulowane w odpowiedniej polityce bezpieczeństwa teleinformatycznego.

XVII. BEZPIECZEŃSTWO FIZYCZNE I ŚRODOWISKOWE

1. W celu zapobieżenia nieuprawnionemu fizycznemu dostępowi, szkodom i zakłóceniom w przetwarzaniu informacji i środkach przetwarzania informacji oraz utracie, zniszczeniu, uszkodzeniu, kradzieży aktywów informacyjnych ISW stosowane są mechanizmy ochrony w obszarze bezpieczeństwa fizycznego i środowiskowego.

2. Szczegółowe zasady dotyczące zarządzania bezpieczeństwem fizycznym i środowiskowym zostały uregulowane w odpowiedniej polityce bezpieczeństwa fizycznego i środowiskowego.

XVIII. ZAPEWNIENIE CIĄGŁOŚCI DZIAŁANIA

1. W ISW podejmowane są działania w zakresie planowania, weryfikowania, zapewnienia, przeglądu i oceny ciągłości działania i postępowania w przypadku wystąpienia sytuacji kryzysowych.

2. Szczegółowe zasady dotyczące zarządzania ciągłością działania zostały uregulowane w odpowiedniej polityce zarządzania ciągłością działania.

XIX. RELACJE Z PODMIOTAMI ZEWNĘTRZNYMI PODMIOTAMI ZEWNĘTRZNYMI

1. Celem zapewnienia ochrony aktywów informacyjnych udostępnianych usługodawcom, dostawcom i innym osobom i podmiotom zewnętrznym wykonującym czynności w imieniu i na rzecz ISW i/lub mającym dostęp do aktywów ISW, wprowadza się zasady postępowania w przypadku współpracy związanej z dostępem do aktywów informacyjnych ISW i korzystania z usług ww. osób i podmiotów.

2. W przypadku wykonywania zadań delegowanych i/lub korzystania z aktywów, w tym przetwarzania informacji powierzonych przez podmioty zewnętrzne w drodze stosownej umowy i/lub porozumienia, poza wymogami określonymi w obowiązującej w ISW dokumentacji bezpieczeństwa dopuszcza się stosowanie wymogów i zaleceń bezpieczeństwa określonych przez ww. podmioty zewnętrzne, o ile wskazane wymogi i zalecenia „zewnętrzne" nie obniżają poziomu bezpieczeństwa pozostałych informacji przetwarzanych w ISW.

XX. ZGODNOŚĆ Z PRZEPISAMI PRAWA

1. W celu uniknięcia naruszenia obowiązujących przepisów prawa, zobowiązań ustawowych, zapisów zawartych umów i porozumień, w ISW prowadzona jest na bieżąco analiza zgodności regulacji wewnętrznych, przyjętych zasad bezpieczeństwa i ich stosowania z ww. przepisami, w tym identyfikowanie, dokumentowanie i aktualizowanie wszystkich istotnych wymagań prawnych, regulacyjnych, umownych oraz podejścia organizacji do ich przestrzegania.

2. Przedmiotowa analiza dotyczy również zgodności z wymaganiami prawnymi, regulacyjnymi i umownymi, związanymi z prawami własności intelektualnej i użytkowaniem prawnie zastrzeżonego oprogramowania.

3. Kierownicy komórek organizacyjnych, w zakresie zadań realizowanych zgodnie z obowiązującym Regulaminem Organizacyjnym, prowadzą bieżący nadzór w swoich komórkach w zakresie zgodności z przepisami prawa i zapisami umownymi.

4. Administrator Danych Osobowych w ISW odpowiedzialny jest za zapewnienia zgodności

przetwarzania danych osobowych z przepisami o ochronie danych osobowych.

5. Zespół ds. wdrożenia i utrzymania SZBI, we współpracy z kierownikami poszczególnych komórek organizacyjnych ISW dokonuje okresowych przeglądów regulacji wewnętrznych dotyczących bezpieczeństwa informacji w zakresie ich zgodności z przepisami prawa i zapisami umownymi, na zasadach i w trybie określonym w Polityce monitorowania i nadzoru nad bezpieczeństwem informacji i dedykowanych procedurach.

6. Koordynator ds. Audytów i Zarządzania Ryzykiem zapewnia okresowy audyt wewnętrzny w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.

XXI. NARUSZENIE BEZPIECZEŃSTWA INFORMACJI

1. Podstawową konsekwencją naruszenia bezpieczeństwa informacji jest obniżenie poziomu ochrony przetwarzanych informacji i aktywów wspierających ich przetwarzanie w ISW.

2. Każdy, kto posiada dostęp do informacji i aktywów wspierających ich przetwarzanie w ISW (pracownicy ISW, jak również praktykanci, stażyści, wolontariusze, zleceniobiorcy oraz inne osoby i podmioty zewnętrzne wykonujące czynności w imieniu i na rzecz ISW i/lub mające dostęp do aktywów informacyjnych ISW) ma obowiązek informowania podmiotów odpowiedzialnych za bezpieczeństwo ISW o podejrzeniu/każdym zidentyfikowanym przypadku naruszenia bezpieczeństwa.

3. Nieprzestrzeganie zasad zawartych w dokumentacji bezpieczeństwa stanowi naruszenie obowiązków pracowniczych i może skutkować sankcjami natury dyscyplinarnej.

4. Naruszenie postanowień PBI przez kontrahenta ISW lub jego pracowników stanowi podstawę do odstąpienia od umowy i żądania pokrycia powstałej szkody lub zapłaty kary umownej, jeżeli taki obowiązek wynika z zawartej umowy.

5. Z tytułu działań pracowników/kontrahentów ISW i innych osób i podmiotów, o których mowa w ust. 2, niezgodnych z przepisami prawa powszechnie obowiązującego (w szczególności dot. przetwarzania danych osobowych), grożą odrębne kary określone w szczególności w:

1) kodeksie pracy,

2) kodeksie cywilnym,

3) kodeksie karnym,

4) ustawie o ochronie danych osobowych.

6. W celu uzyskania możliwie pełnej informacji o naruszeniu bądź też podejrzeniu naruszenia bezpieczeństwa informacji w ISW, osoby bądź podmioty niezwiązane z ISW mogą zgłaszać przypadki bądź podejrzenie naruszenia bezpieczeństwa <kancelaria@instytutstratwojennych.pl>.

XXII. ODSTĘPSTWA

Podejmowanie jakichkolwiek działań stanowiących odstępstwo od zapisów niniejszej Polityki wymaga pisemnej zgody Dyrektora Instytutu Strat Wojennych im. Jana Karskiego.