ZARZĄDZENIE Nr 19
MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI

z dnia 7 lipca 2011 r.

w sprawie Polityki Bezpieczeństwa Elektronicznej Platformy Usług Administracji Publicznej

Na podstawie art. 34 ust. 1 i 2 ustawy z dnia 8 sierpnia 1996 r. o Radzie Ministrów (Dz. U. z 2003 r. Nr 24, poz. 199, z późn. zm.[1)]) zarządza się, co następuje:

§ 1.

1. W celu zapewnienia bezpieczeństwa informacji w Elektronicznej Platformie Usług Administracji Publicznej, zwanej dalej „ePUAP", w szczególności w celu wykonania obowiązków nałożonych na administratora danych osobowych przez ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.[2)]) w związku z art. 19a ust. 2 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. Nr 64, poz. 565, z późn. zm.[3)]) wprowadza się w Ministerstwie Spraw Wewnętrznych i Administracji Politykę Bezpieczeństwa ePUAP.

[1)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2003 r. Nr 80, poz. 717, z 2004 r. Nr 238, poz. 2390 i Nr 273, poz. 2703, z 2005 r. Nr 169, poz. 1414 i Nr 249, poz. 2104, z 2006 r. Nr 45, poz. 319, Nr 170, poz. 1217 i Nr 220, poz. 1600, z 2008 r. Nr 227, poz. 1505, z 2009 r. Nr 4, poz. 337, i Nr 98, poz. 817, Nr 157, poz. 1241, Nr 161, poz. 1277 oraz z 2010 r. Nr 57, poz. 354.

[2)] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2002 Nr 153, poz. 1271, z 2004 r. Nr 25, poz. 219 i Nr 33, poz. 285, z 2006 r. Nr 104, poz. 708 i 711, z 2007 r. Nr 165, poz. 1170 i Nr 176, poz. 1238 oraz z 2010 r. Nr 41, poz. 233, Nr 182, poz. 1228 i Nr 229, poz. 1497.

[3)] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2006 r. Nr 12, poz. 65 i Nr 73, poz. 501, z 2008 r. Nr 127, poz. 817, z 2009 r. Nr 157, poz. 1241, z 2010 r. Nr 40, poz. 230, Nr 167, poz. 1131 i Nr 182, poz. 1228 oraz z 2011 r. Nr 112, poz. 654.

2. Użyte w zarządzeniu pojęcia oznaczają:

1) Minister — Ministra Spraw Wewnętrznych i Administracji;

2) Ministerstwo — Ministerstwo Spraw Wewnętrznych i Administracji.

§ 2.

1. Na Politykę Bezpieczeństwa ePUAP, o której mowa w § 1 ust. 1, składają się:

1) Polityka bezpieczeństwa informacji ePUAP, określona w załączniku Nr 1 do zarządzenia;

2) Zakres systemu zarządzania bezpieczeństwem informacji ePUAP, określony w załączniku Nr 2 do zarządzenia;

3) Zasady zarządzania bezpieczeństwem informacji ePUAP, określone w załączniku Nr 3 do zarządzenia;

4) inne dokumenty, w szczególności instrukcje i procedury.

2. Dokumenty, o których mowa w ust. 1 pkt 4, są przedkładane do zatwierdzenia Ministrowi albo Dyrektorowi Generalnemu Ministerstwa, w zakresie ich kompetencji.

3. Do zatwierdzania, o którym mowa w ust. 2, Minister może upoważnić na piśmie właściwego Sekretarza lub Podsekretarza Stanu w Ministerstwie.

4. Dokumenty, o których mowa w ust. 1 pkt 4, są przedkładane do zatwierdzenia przez kierownika komórki organizacyjnej w Ministerstwie, w zakresie której są kompetencje związane z ePUAP; jeśli dokument związany jest z kompetencjami więcej niż jednej komórki organizacyjnej, wówczas dokument przedkładany jest wspólnie przez kierowników tych komórek.

5. Dokumenty, o których mowa w ust. 1 pkt 4, stają się obowiązujące z dniem ich zatwierdzenia przez Ministra, lub upoważnionego Sekretarza lub Podsekretarza Stanu w Ministerstwie, albo przez Dyrektora Generalnego Ministerstwa.

6. Za prawidłową realizację postanowień zawartych w dokumentach, o których mowa w ust. 1 pkt 4, odpowiedzialni są kierownicy komórek Ministerstwa, którzy przedłożyli ten dokument do zatwierdzenia, w zakresie kompetencji kierowanych przez nich komórek organizacyjnych.

§ 3.

Zarządzenie wchodzi w życie z dniem podpisania.

Minister Spraw Wewnętrznych i Administracji:
J. Miller

Załączniki do zarządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 7 lipca 2011 r. (poz. 45)

Załącznik nr 1

POLITYKA BEZPIECZEŃSTWA INFORMACJI ePUAP

1. Odbiorcy

Polityka Bezpieczeństwa Informacji odnosi się zarówno do pracowników Ministerstwa, jak i Podmiotów zewnętrznych współpracujących z Ministerstwem i uzyskujących dostęp do jego Zasobów w celu świadczenia usług na rzecz Ministerstwa na podstawie umów, porozumień lub innych stosunków prawnych.

2. Cel Polityki Bezpieczeństwa Informacji ePUAP

Celem Polityki Bezpieczeństwa Informacji ePUAP jest określenie zasad, zgodnie z którymi są zarządzane, zabezpieczane i eksploatowane Zasoby Ministerstwa związane z systemem ePUAP w celu zapewnienia poufności, integralności i dostępności informacji przetwarzanej w Ministerstwie.

3. Słownik terminów

Niniejszy dokument zawiera podstawowe definicje pojęć dotyczących polityki bezpieczeństwa informacji:

1. Autentyczność — właściwość zapewniająca, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana. Autentyczność dotyczy takich podmiotów jak użytkownicy, procesy, systemy i informacja;
2. Bezpieczeństwo informacji — zachowanie poufności, integralności i dostępności informacji; dodatkowo, mogą być brane pod uwagę inne właściwości informacji, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność (ISO/IEC 2007:2005);
3. Dostępność — właściwość bycia dostępnym i możliwym do wykorzystania na żądanie, w założonym czasie, przez autoryzowany podmiot. (ISO 7498-2:1989);
4. Incydent związany z bezpieczeństwem informacji — pojedyncze lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań i zagrażają bezpieczeństwu informacji (ISO/IEC TR 18044:2004);
5. Informacja wrażliwa — dane przetwarzane oraz przekazywane przez ePUAP oraz informacje związane z ochroną takich danych, a w szczególności zawartości baz danych oraz dane konfiguracyjne;

6. Integralność danych — właściwość zapewniająca, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany (ISO 7498-2:1989);
7. Integralność systemu — właściwość polegająca na tym, że system realizuje swoją zamierzoną funkcję w nienaruszony sposób, wolny od nieautoryzowanej manipulacji, celowej lub przypadkowej;
8. Niezaprzeczalność — możliwość przeprowadzenia dowodu, że działanie lub zdarzenie miało miejsce, w taki sposób, że nie można temu działaniu lub zdarzeniu później zaprzeczyć (PN-ISO/IEC 13888-1);
9. Niezawodność — właściwość oznaczająca spójne, zamierzone zachowanie i skutki (PN-ISO-13335-1:1999);
10. Podatność — słabość aktywu lub grupy aktywów, która może być wykorzystana przez jedno lub więcej zagrożeń (PN ISO/IEC 17799:2007);
11. Poufność — właściwość zapewniająca, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom (ISO 7498-2:1989);
12. Rozliczalność — właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi (ISO 7498-2:1989);
13. Ryzyko związane z bezpieczeństwem informacji — potencjalna sytuacja, w której dane zagrożenie wykorzysta podatności aktywów lub grupy aktywów, co spowoduje szkodę dla organizacji. Ryzyko jest funkcją prawdopodobieństwa zdarzenia i jego konsekwencji (PN ISO/IEC 27005:2010);
14. System informacyjny — system, w którym w trakcie zachodzących w nim procesów gromadzi się, przetwarza, przechowuje i udostępnia informacje, niezależnie od formy realizacji tych procesów;
15. System teleinformatyczny — zespół współpracujących ze sobą według określonych reguł urządzeń i oprogramowania;
16. Zagrożenie — potencjalna przyczyna incydentu, który może spowodować stratę w systemie lub dla organizacji (PN ISO/IEC 17799:2007);
17. Zdarzenie związane z bezpieczeństwem informacji — określony stan systemu, usługi lub sieci, który wskazuje na możliwe przełamanie bezpieczeństwa informacji, błąd zabezpieczenia lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem (ISO/IEC TR 18044:2004);
18. Deklaracja stosowania — dokument, w którym opisano cele stosowania zabezpieczeń oraz zabezpieczenia, które odnoszą się i mają zastosowanie w Information Security Management System danej organizacji, oparte na rezultatach i wnioskach wynikających z procesów szacowania i postępowania z ryzykiem;
19. System Zarządzania Bezpieczeństwem Informacji (SZBI), lub Information Security Management System (ISMS) — ta część całościowego systemu zarządzania, oparta na podejściu wynikającym z ryzyka biznesowego, odnosząca się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji;
20. Zarządzanie ryzykiem — skoordynowane działania kierowania i kontrolowania organizacji z uwzględnieniem ryzyka (ISO/IEC Guide 73:2002);
21. Zasoby — wszystko to, co ma wartość dla Ministerstwa, w szczególności informacje przetwarzane w Ministerstwie oraz mienie wykorzystywane przez Ministerstwo (równoważnie — aktywa (informacyjne));
22. Ministerstwo — Ministerstwo Spraw Wewnętrznych i Administracji;
23. System — system informacyjny świadczący usługę Klientowi;
24. Klient — podmiot publiczny, osoba prawna, jednostka organizacyjna nie posiadająca osobowości prawnej lub osoba fizyczna korzystająca z usług systemu Ministerstwa;
25. Kierownictwo — Minister, Sekretarz Stanu, Podsekretarz Stanu, Dyrektor Generalny;
26. Pełnomocnik do spraw Zarządzania Systemem Bezpieczeństwa Informacji (Inspektor Bezpieczeństwa Informacji (IBI)) — osoba której Kierownictwo powierzyło koordynowanie rozwoju, wdrażania i utrzymywania Systemu Zarządzania Bezpieczeństwem Informacji (ISMS) oraz nadzór nad bezpieczeństwem informacji nie będącej w zakresie kompetencji Administrator Bezpieczeństwa Informacji;
27. Administrator Bezpieczeństwa Informacji (ABI) — osoba nadzorująca przestrzeganie stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych w sposób odpowiedni do zagrożeń oraz kategorii danych objętych ochroną wyznaczona przez administratora danych osobowych zgodnie z ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych;
28. Organizacja — w kontekście niniejszej Polityki oznacza Ministerstwo;
29. Podmiot zewnętrzny — osoba fizyczna, osoba prawna, jednostka organizacyjna nie posiadająca osobowości prawnej lub organ współpracujący z Ministerstwem bądź świadczący na jego rzecz usługi;
30. Zasób (Aktywa) — wszystko, co ma wartość dla Ministerstwa i składa się na Systemy, a w szczególności personel, budynki i budowle, sprzęt, oprogramowanie, informacja, prawa niematerialne, wizerunek;

31. Właściciel Zasobu (WZ) — kierownik komórki organizacyjnej Ministerstwa, nadzorującej eksploatację, rozwój, utrzymanie, korzystanie, bezpieczeństwo i dostęp do Zasobu;
32. Inspektor Bezpieczeństwa Informacji (IBI) — wyznaczony pracownik Ministerstwa realizujący zadania związane z kontrolą efektywności uzyskanego poziomu bezpieczeństwa do założonych celów w działalności właściwej komórki organizacyjnej;
33. Administrator — wyznaczony pracownik Ministerstwa realizujący zadania związane z utrzymaniem systemu teleinformatycznego, a w szczególności odpowiedzialny za utrzymywanie zabezpieczeń w tym systemie.

4. Postanowienia ogólne

1. Niniejszą Polityką Bezpieczeństwa nie jest objęta ochrona informacji niejawnych w rozumieniu ustawy o ochronie informacji niejawnych, których ochrona odbywa się na odrębnych zasadach.
2. Polityka Bezpieczeństwa Informacji jest zgodna z prawem Rzeczpospolitej Polskiej oraz prawem Unii Europejskiej, opiera się na Polskich Normach, standardach międzynarodowych,.
3. Ochronie podlegają Zasoby Ministerstwa.
4. Każdy pracownik Ministerstwa przyjmuje na siebie obowiązek ochrony Zasobów Ministerstwa w zakresie uzyskanych uprawnień. Obowiązek ochrony Zasobów nie kończy się z chwilą ustania stosunku pracy lub innego stosunku prawnego stanowiącego podstawę wykonywania pracy na rzecz Ministerstwa w takim zakresie, jaki ustanawiają przepisy prawa. Obowiązek ochrony Zasobów w przypadku współpracy z Podmiotami zewnętrznymi określany jest w ramach zawartych z nimi umów.

5. Wymagania bezpieczeństwa

Organizacja Ministerstwa oraz systemy teleinformatyczne służące do przetwarzania danych, muszą spełniać następujące wymagania bezpieczeństwa:

1) integralności, autentyczności i dostępności danych, na podstawie których jest prowadzona działalność statutowa Ministerstwa;
2) niezawodności, dostępności i integralności istotnych systemów informacyjnych Ministerstwa;
3) integralności i poufności informacji dotyczących Klientów Ministerstwa;
4) rozliczalności działań i zdarzeń zachodzących w systemach informacyjnych Ministerstwa;
5) poufności i ochrony dostępu do informacji wrażliwych, w szczególności wynikających z odnośnych przepisów prawa.

6. Podstawa prawna

1. Podstawę egzekwowania od pracowników oraz funkcjonariuszy Ministerstwa przestrzegania zasad niniejszej Polityki Bezpieczeństwa Informacji stanowią przepisy prawa oraz stosunek prawny będący podstawą wykonywania pracy oraz pełnienia służby na rzecz Ministerstwa.
2. Podstawą egzekwowania przestrzegania zasad ochrony informacji od Podmiotów zewnętrznych uczestniczących w procesach związanych z działalnością Ministerstwa są przepisy prawa lub stosowne zapisy umów, decyzji i porozumień.

7. Zasady rozpowszechniania Polityki Bezpieczeństwa Informacji

1. Z treścią niniejszego dokumentu są zapoznani wszyscy pracownicy Ministerstwa, Klienci, organy regulacyjne oraz Podmioty zewnętrzne uczestniczące w realizacji działań statutowych Ministerstwa w zakresie ePUAP.
2. Z treścią polityk szczegółowych, instrukcji i regulaminów i procedur zawartych w dokumentach związanych są zapoznani pracownicy Ministerstwa lub Podmioty zewnętrzne po zaakceptowaniu ich treści przez Ministra i przekazaniu do stosowania w zakresie niezbędnym do wykonania swoich obowiązków związanych z systemem ePUAP.

8. Podstawowe zasady bezpieczeństwa informacji

1. W celu zapewnienia bezpieczeństwa informacji stosuje się następujące ogólne zasady:
   1) „przywilejów koniecznych" — każdy użytkownik systemów teleinformatycznych Ministerstwa ma prawa dostępu do Zasobów ograniczone wyłącznie do tych, które są niezbędne do wykonywania powierzonych mu obowiązków;
   2) rozliczalności — Ministerstwo dąży do zapewnienia jednoznacznej odpowiedzialności pracowników za Zasoby im powierzone; wszyscy użytkownicy Zasobów muszą być świadomi swej odpowiedzialności i konsekwencji, które poniosą, jeżeli zaniedbają swoje obowiązki; przekazywanie własnych praw dostępu do Zasobów innym osobom jest zabronione; odstępstwo od zasady rozliczalności musi być uzasadnione, odnotowane oraz zatwierdzone przez osoby odpowiedzialne za bezpieczeństwo;

3) „separacji obowiązków", polegającej na tym, że zadania krytyczne z punktu widzenia bezpieczeństwa systemu nie mogą być realizowane przez jedną osobę. Zadania krytyczne są wskazane w politykach szczegółowych i regulaminach;

4) „domniemanej odmowy", to jest przyjęcia jako standardowych najbardziej restrykcyjnych ustawień, które można zwolnić jedynie w określonych sytuacjach („to, co nie jest dozwolone, jest zabronione").

2. ePUAP jest zabezpieczony przed nieupoważnionym dostępem, modyfikacją lub zniszczeniem. Struktura wewnętrzna systemów jest zabezpieczona przed nieupoważnionym dostępem z zewnątrz.

3. Każdy użytkownik ePUAP dysponuje indywidualnym kontem umożliwiającym jego jednoznaczną identyfikację, za pośrednictwem którego może korzystać z udostępnianych Zasobów i usług. Mechanizmy uwierzytelniania, rejestrowania zdarzeń i monitorowania zdarzeń gwarantują rozliczalność użytkowników zarejestrowanych w tym systemie.

4. Wszyscy pracownicy Ministerstwa posiadający bezpośredni dostęp do ePUAP, związani z jego utrzymaniem oraz rozwojem lub z racji wykonywanych obowiązków służbowych posiadający dostęp do informacji wrażliwych związanych z ePUAP są zapoznawani z przyjętym dokumentem Polityki Bezpieczeństwa Informacji, a powyższy fakt potwierdzają podpisując oświadczenie. Okresowo są przeprowadzane szkolenia dotyczące bezpieczeństwa informacji w ePUAP oraz ochrony innych Zasobów Ministerstwa.

5. Każdy pracownik, funkcjonariusz Ministerstwa lub podmiotu zewnętrznego ma obowiązek informowania o wystąpieniu incydentu związanego z bezpieczeństwem informacji lub innych zasobów bezpośredniego przełożonego oraz Inspektora Bezpieczeństwa Informacji.

6. W przypadku wystąpienia incydentu związanego z bezpieczeństwem informacji lub innych Zasobów, kierownictwo Ministerstwa spowoduje podjęcie działań zaradczych w celu zmniejszenia potencjalnych strat.

7. Na wypadek katastrofy lub rozległej awarii technicznej są opracowane, oraz okresowo testowane plany ciągłości działania dla systemów i aplikacji istotnych z punktu widzenia działalności statutowej Ministerstwa.

9. Zasady dokonywania zmian w Polityce Bezpieczeństwa Informacji

Niniejszy dokument i inne dokumenty związane będą modyfikowane zgodnie z procedurami przyjętymi w systemie zarządzania bezpieczeństwem informacji w przypadku:

1) ogłoszenia nowych lub modyfikacji istniejących przepisów prawa;

2) przekazania uwag przez odbiorców Polityki Bezpieczeństwa Informacji;

3) powstania zaleceń poaudytowych;

4) w wyniku przeprowadzenia przez Ministra corocznych przeglądów Polityki Bezpieczeństwa Informacji;

5) zmian organizacyjnych w Ministerstwie.

10. Odpowiedzialność za Politykę Bezpieczeństwa Informacji

1. Osoby zajmujące stanowiska kierownicze oraz wytypowani pracownicy Ministerstwa mają obowiązki związane z utrzymaniem bezpieczeństwa informacji, kontrolą lub nadzorem nad przestrzeganiem polityki w tym zakresie. Od takich pracowników wymagana jest szczególna lojalność, staranność oraz wysoka etyka zawodowa.

2. Minister właściwy do spraw informatyzacji:

   1) zapewnia, że cele bezpieczeństwa informacji są zidentyfikowane, spełniają wymagania organizacji i są włączone do odpowiednich procesów;

   2) zapewnia jasne wskazania i widoczne wsparcie dla inicjatyw z zakresu bezpieczeństwa informacji;

   3) zapewnia środki potrzebne do zapewnienia bezpieczeństwa informacji;

   4) zatwierdza w Ministerstwie poszczególne role i zakresy odpowiedzialności związane z bezpieczeństwem informacji Systemu oraz dokumentację związaną z funkcjonowaniem ISMS;

   5) inicjuje plany i programy utrzymujące właściwą świadomość problematyki bezpieczeństwa informacji;

   6) zapewnia, że wdrożenie zabezpieczeń informacji jest skoordynowane w całym Ministerstwie poprzez powołanie Pełnomocnika do spraw Systemu Zarządzania Bezpieczeństwem Informacji — Administratora Bezpieczeństwa Informacji;

   7) zatwierdza plan postępowania z ryzykiem dla ryzyk, których wartość przekracza kompetencje dyrektora departamentu.

3. Administrator Bezpieczeństwa Informacji:

   1) pełni rolę Administratora Bezpieczeństwa Informacji w rozumieniu art. 36 ust. 3 ustawy o ochronie danych osobowych;

   2) zapewnia, że zadania z zakresu bezpieczeństwa są realizowane zgodnie z Polityką Bezpieczeństwa Informacji;

3) określa postępowanie w przypadku niezgodności z obowiązującymi aktami normatywnymi oraz dokumentacją techniczną;

4) przedkłada do zatwierdzenia metodykę i procesy związane z bezpieczeństwem informacji, w tym dotyczącą klasyfikacji informacji, szacowania ryzyka, systemu mierników poziomu zabezpieczeń;

5) rozpoznaje znaczące zmiany zagrożeń i stopień narażenia informacji lub środków do przetwarzania informacji na zagrożenia;

6) szacuje adekwatność i koordynuje wdrożenie oraz okresowe testowanie zabezpieczeń;

7) skutecznie promuje w organizacji kształcenie, szkolenia i uświadamianie w zakresie bezpieczeństwa informacji;

8) ocenia informacje uzyskane z monitorowania i przeglądu incydentów związanych z bezpieczeństwem informacji oraz zaleca odpowiednie działania w stosunku do zidentyfikowanych incydentów związanych z bezpieczeństwem informacji.

4. Właściciel Zasobu (Aktywów) odpowiada za utrzymanie wyznaczonego poziomu bezpieczeństwa powierzonego mu poprzez regulacje wewnętrzne Ministerstwa Zasobu, w tym za szacowanie ryzyka, plan postępowania z ryzykiem, dobór zabezpieczeń oraz plan ciągłości działania, nawet w przypadku, gdy za bieżące utrzymywanie Zasobu odpowiada Podmiot zewnętrzny.

5. Audyt Wewnętrzny prowadzi wewnętrzne audyty ISMS w zaplanowanych odstępach czasu, a w razie konieczności doraźnie, w celu stwierdzenia, że cele stosowania zabezpieczeń, zabezpieczenia, procesy i procedury ISMS są:

1) zgodne z wymaganiami normy PN ISO/IEC 27001:2007, przepisami prawa oraz regulacjami wewnętrznymi;

2) zgodne ze zidentyfikowanymi wymaganiami bezpieczeństwa informacji;

3) efektywnie wdrożone i utrzymywane;

4) zgodne z oczekiwaniami.

6. Przełożeni pracowników wszystkich szczebli odpowiadają za nadzór nad realizacją zadań wynikających z Polityki Bezpieczeństwa Informacji w stosunku do swoich podwładnych.

Załącznik nr 2

ZAKRES SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI ePUAP

1. Słownik terminów:

1) Aplikacja — zestaw metadanych definiujących określone współpracujące ze sobą zasoby uruchomione na ePUAP, wspierające udostępnienie i realizację jakiejś usługi lub grupy usług publicznych;

2) Rejestr zdarzeń — zapis zajścia w ePUAP określonej sytuacji;

3) Zasób informatyczny — to w szczególności ludzie; zbiory informacyjne, procedury, oprogramowanie, sprzęt komputerowy, sieci telekomunikacyjne, nośniki danych;

4) Użytkownik — osoba fizyczna lub prawna, jednostka organizacyjna nieposiadająca osobowości prawnej bądź podmiot publiczny, które zarejestrowały się na ePUAP.

2. Założenia

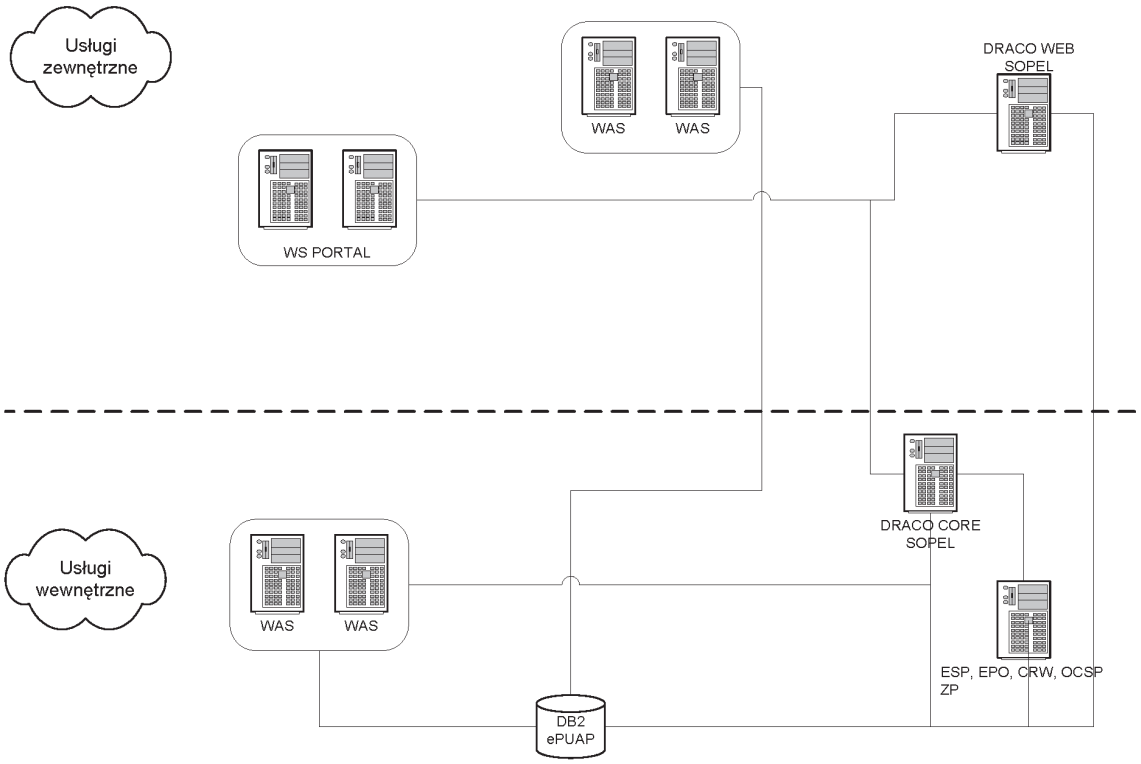
ePUAP jest systemem scentralizowanym. Dostęp do Systemu jest możliwy poprzez Internet. ePUAP jest publicznie dostępny: z portalu będącego częścią Systemu mogą korzystać wszyscy mający dostęp do Internetu za wyjątkiem operacji chronionych, które mogą być wykonywane jedynie przez uwierzytelnionych a w zakresie znacznej liczby operacji i dostępów — autoryzowanych użytkowników.

System korzysta z platformy sprzętowej zlokalizowanej w dwóch ośrodkach, pomiędzy którymi dokonywana jest bieżąca replikacja danych. W przypadku awarii lub z innych powodów (np. zniszczenie fizyczne działającego ośrodka) możliwe jest przełączenie Systemu, tak aby działał na drugim ośrodku bez utraty danych.

3. Aplikacje do słownika

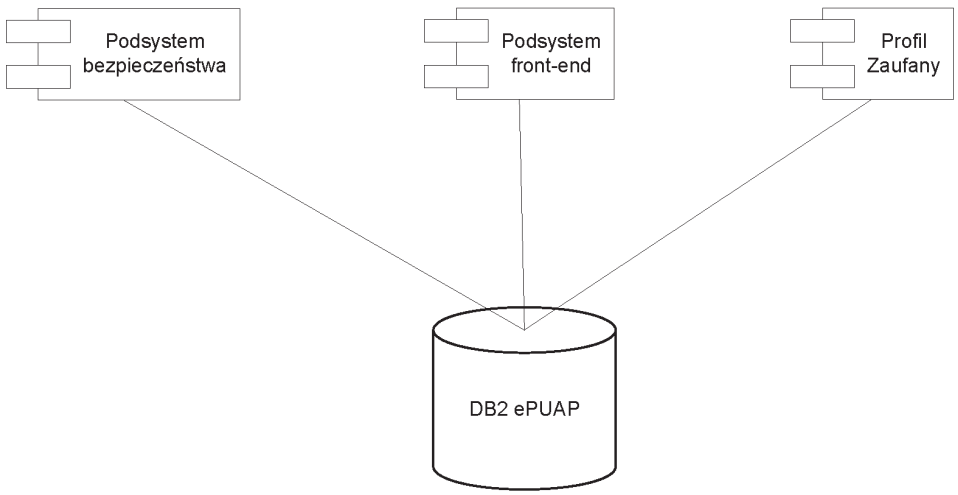
Zbiory danych

Ogólną architekturę logiczną i sprzętową przedstawiają rysunki 1—4.



Rysunek 1 Architektura fizyczna

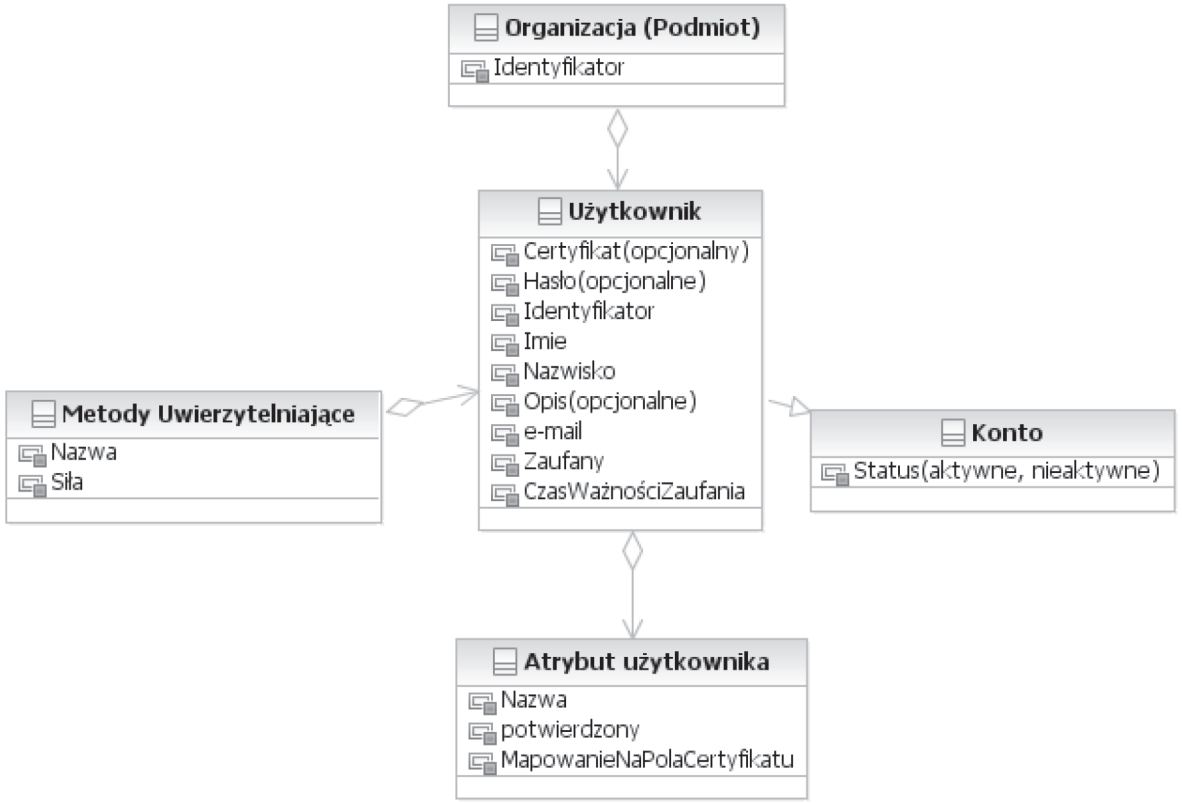
OPIS:
— WS PORTAL — serwery WebSphere Portal zawierające formatki aplikacji (portlety).
— WAS — serwery aplikacji WebSphere Application Server udostępniające logikę aplikacji (webserwisy).
— DB2 ePUAP — serwer bazodanowy DB2 z bazą danych na potrzeby aplikacji ePUAP.
— DRACO, SOPEL — serwery zawierające formatki i aplikacje realizujące usługi bezpieczeństwa.
— ESP, EPO, CRW — usługi podpisujące HSM.
— ZP — podpis cyfrowy dokonywany przez ePUAP zawierający informację o podmiocie zaufanym w imieniu, którego dokonano podpisu (podpis profilem zaufanym).



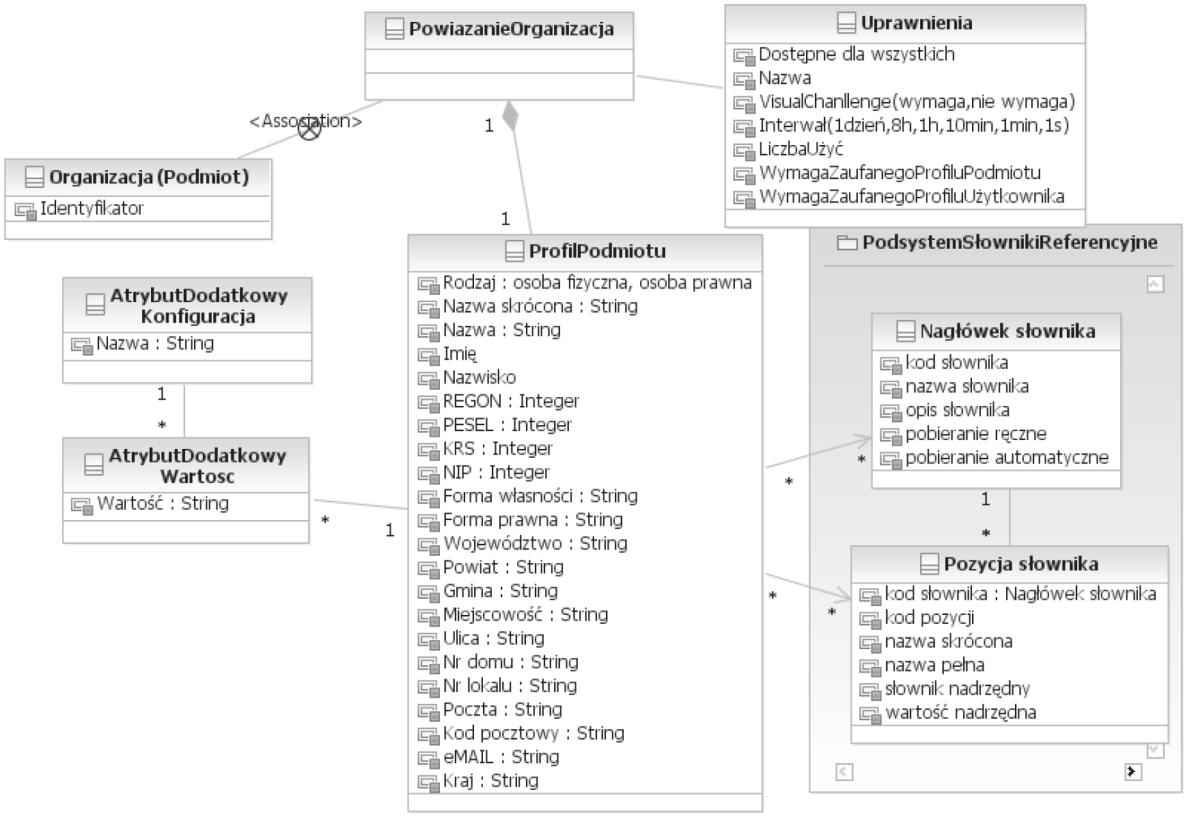
Rysunek 2 Podsystemy operujące na zbiorach danych osobowych

Podsystemami operującymi na danych osobowych są:
○ Podsystem bezpieczeństwa (w ramach tego podsystemu gromadzone są dane osobowe: dane użytkownika i podmiotu w kontekście, którego użytkownik pracuje).
○ Podsystem Front-End (w ramach tego podsystemu dokonywane są operacje na danych osobowych pochodzących z danych gromadzonych w podsystemie bezpieczeństwa — pobranie danych użytkownika i podmiotu oraz przechowywane dokumenty xml z danymi osobowymi, np. dane adresata, dane odbiorcy).
○ Profil Zaufany (w ramach tego podsystemu gromadzone są potwierdzone podpisem kwalifikowanym dane osobowe użytkownika, wykorzystywane do generowania podpisów cyfrowych).

ePUAP przekazuje dane osobowe w postaci dokumentów xml zgodnie z modelami zaprezentowanymi poniżej:



Rysunek 3 Model danych dla użytkownika



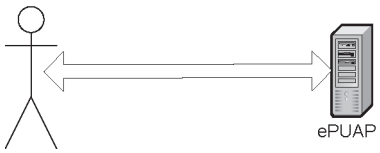
Rysunek 4 Model danych dla podmiotu

Dane osobowe w podsystemie Front-End przechowywane są w ramach danych na dokumentach — pliki xml. Dane te nie podlegają ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

Przepływy danych

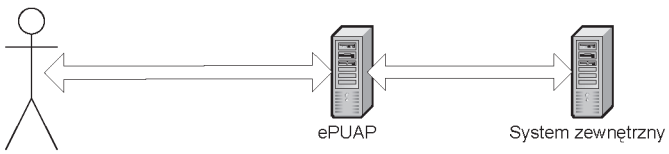
Przepływ danych przedstawiają rysunki 5—8

ePUAP przekazuje dane osobowe w postaci dokumentów xml zgodnie z modelami zaprezentowanymi poniżej:



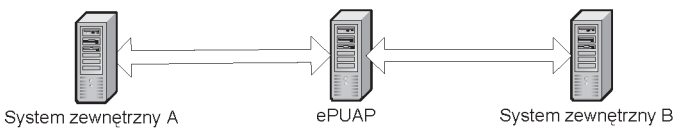
Rysunek 5 Dane w ramach ePUAP

W modelu tym użytkownik wykorzystujący mechanizmy operacji na dokumentach ePUAP wprowadza dane osobowe, które gromadzone są i przechowywane w ePUAP. Dla danych tych ewentualny ich przepływ to operacje przekazywania dokumentów (xml) w ramach ePUAP (przekazywanie dokumentów pomiędzy składami dokumentów różnych podmiotów w podsystemie Front-End).



Rysunek 6 Dane wprowadzone do ePUAP i przesyłane do Systemu Zewnętrznego

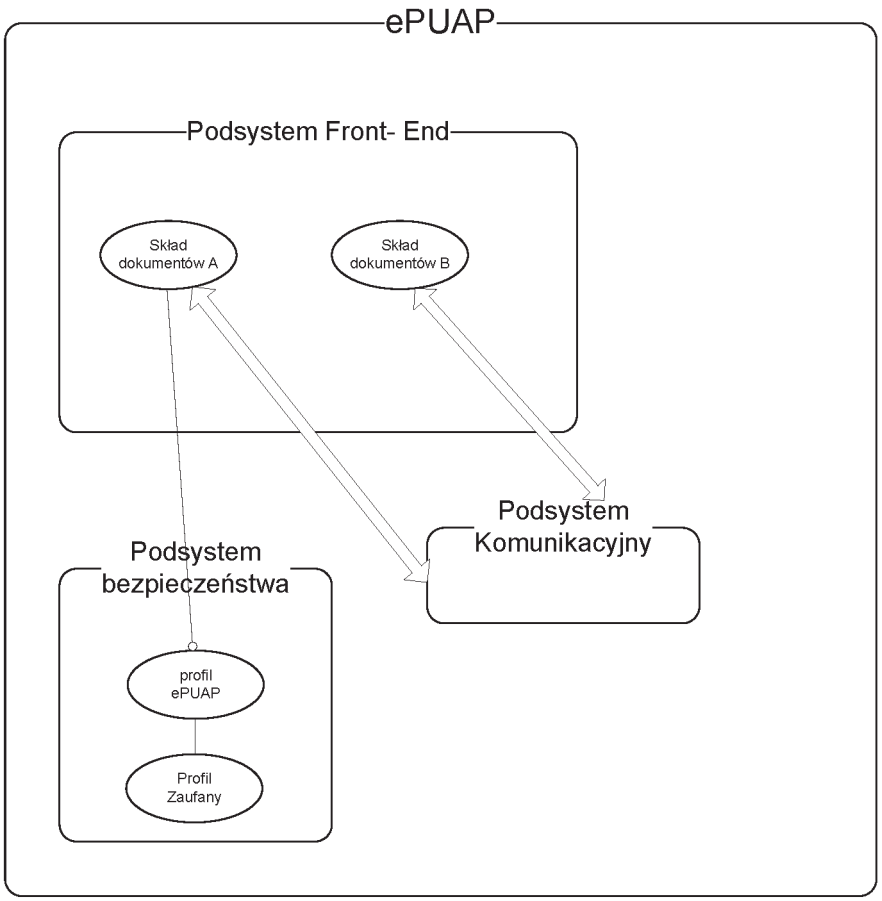
W modelu tym użytkownik wykorzystujący mechanizmy operacji na dokumentach ePUAP wprowadza dane osobowe, które gromadzone są i przechowywane w ePUAP. Dane te są przesyłane do i z Systemu Zewnętrznego.



Rysunek 7 Dane przesyłane przez ePUAP z jednego Systemu Zewnętrznego do drugiego

W modelu tym ePUAP jest jedynie „przekaźnikiem" dane są jedynie przesyłane z wykorzystaniem mechanizmów platformy bez ingerencji w dane.

Poniżej przedstawiony jest schemat przepływu danych w ramach ePUAP:



Rysunek 8 Przepływy danych w ePUAP

Dane osobowe wprowadzane i przechowywane w ramach struktur profilu podmiotu mogą być pobierane automatycznie do dokumentów (xml) tworzonych przez użytkowników uprawnionych do danego podmiotu. Dokumenty z danymi osobowymi przesyłane są za pośrednictwem podsystemu komunikacyjnego pomiędzy składami dokumentów (podsystem Front— End) poszczególnych podmiotów.

4. Infrastruktura Teleinformatyczna

Baza danych

Za dostęp do bazy danych z danymi osobowymi odpowiadają mechanizmy autentykacji i autoryzacji bazy danych. Operacje bezpośrednio na bazie danych dostępne są jedynie dla uprawnionych administratorów z imiennymi kontami i bezpiecznymi hasłami. Dostęp do bazy danych ograniczony jest również poprzez zapory sieciowe. Zdalny dostęp możliwy jest jedynie przez połączenie VPN dla adresów dodanych zgodnie z procedurą przydzielania dostępu zdalnego.

Rejestr Zdarzeń

W aplikacji rejestrowane są wszystkie zdarzenia dotyczące operacji na danych osobowych. Mechanizmy zabezpieczające Rejestru Zdarzeń zapewniają jego integralność i bezpieczeństwo.

Autentykacja i Autoryzacja w Systemie

— Dostęp do systemów ePUAP wykorzystuje proces bezpiecznego logowania,
— Wszyscy użytkownicy posiadają niepowtarzalne identyfikatory dla swojego osobistego i wyłącznego użytku tak, aby można było powiązać działania z odpowiedzialnymi za nie osobami. Właściciel identyfikatora jest odpowiedzialny za wszystkie działania wykonane z wykorzystaniem tego identyfikatora,
— Istnieje system zarządzania hasłami,
— Wykorzystanie systemowych programów narzędziowych jest ograniczone i ściśle kontrolowane,

— Nieaktywne terminale obsługujące systemy ePUAP są odłączane po zadanym czasie bezczynności, aby zapobiec dostępowi osób nieupoważnionych,

— Żaden zasób informatyczny ePUAP nie może być używany bez wcześniejszego określenia osoby odpowiedzialnej za ten zasób,

— Każdy dostęp do systemu jest monitorowany.

Za uwierzytelnianie w ePUAP odpowiedzialny jest system DRACO.

Dla PUAP możliwe są dwa scenariusze uwierzytelniania:

— z wykorzystaniem hasła — uwierzytelnianie odbywa się z wykorzystaniem losowego identyfikatora użytkownika (generowanego podczas zakładania konta użytkownika) oraz statycznego hasła,

— z wykorzystaniem certyfikatów kwalifikowanych — uwierzytelnianie odbywa się z wykorzystaniem losowego identyfikatora użytkownika oraz certyfikatu kwalifikowanego, który posiada użytkownik. W przypadku tej metody użytkownik zamiast hasła podaje PIN do karty mikroprocesorowej, na której znajduje się certyfikat.

Dla systemu ePUAP zdefiniowana jest następująca polityka haseł:

— Minimalna ilość znaków: 8

— Maksymalna ilość znaków: 32

— Minimalna ilość znaków specjalnych: 1

— Minimalna ilość cyfr: 1

Dodatkowo zdefiniowane są nastepujące:

— Ilość prób niepoprawnego wprowadzania hasła: 3

— Okres blokady konta (po wykorzystaniu maksymalnej ilości prób wprowadzenia niepoprawnego hasła): 10 minut

Autoryzacja użytkowników w systemie ePUAP realizowana jest przez system DRACO.

W ePUAP użytkownicy są autoryzowani w poszczególnych aplikacjach systemu na podstawie przynależności do ról grupujących określone uprawnienia.

Dane zgromadzone na nośnikach umieszczonych w zabezpieczonym centrum przetwarzania (centrum podstawowe i centrum zapasowe).

Ośrodki przetwarzania danych znajdują się w silnie strzeżonych budynkach kontrolowanych przez Straż Graniczną oraz Państwową Wytwórnię Papierów Wartościowych S.A. Procedura dostępu do serwerowni wymaga uzyskania przepustki i przejścia przez kilka punktów kontrolnych. Budynki są monitorowane przez kamery (w szczególności korytarz przed serwerownią). Pracownicy Straży Granicznej oraz PWPW S.A. 24 godziny na dobę, przez 7 dni w tygodniu pełnią dyżur i kontrolują dostęp do serwerowni.

Obszary przetwarzania

Dane osobowe przetwarzane są w lokalizacjach, których wykaz aktualizowany przez. Administratora Bezpieczeństwa Informacji.

Załącznik nr 3

ZASADY ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI ePUAP

1. SŁOWNIK TERMINÓW

Występujące w Zasadach Zarządzania Bezpieczeństwem Informacji zwroty i skróty oznaczają:

1) **DSI** — Departament Społeczeństwa Informacyjnego;

2) **DEPiT** — Departament Ewidencji Państwowych i Teleinformatyki;

3) **AS** — Administrator ePUAP;

4) **ABI** — Administrator Bezpieczeństwa Informacji w rozumieniu Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r.;

5) **IBI** — Inspektor Bezpieczeństwa Informacji;

6) **ZKBI** — Zespół Koordynacji Bezpieczeństwa Informacji ePUAP;

7) **WZ** — właściciel zasobu — Minister właściwy ds. Informatyzacji;

8) **ServiceDesk** — dział wsparcia technicznego użytkowników ePUAP;

9) **gwarantowane źródło zasilania** — źródło zasilania zapewniające jakość zasilania niezależnie od stanu źródeł zewnętrznych;
10) **koperta bezpieczna** — koperta, której nie można otworzyć bez naruszenia jej struktury;
11) **kopia zapasowa (backup)** — kopia oprogramowania lub danych pozwalająca na ich dokładne odtworzenie w wypadku utraty oryginału;
12) **logowanie** — proces uwierzytelniania użytkownika w ePUAP;
13) **nośnik informacji** — medium magnetyczne, optyczne, półprzewodnikowe lub papierowe, na którym zapisuje się i przechowuje informacje;
14) **pracownik** — należy przez to rozumieć funkcjonariusza lub osobę zatrudnioną w Ministerstwie bez względu na podstawę nawiązania stosunku pracy;
15) **współpracownik** — osoba wykonująca zadania na rzecz Ministerstwa zatrudniona przez podmiot zewnętrzny;
16) **osoba trzecia** — podmiot publiczny, osoba fizyczna, osoba prawna lub instytucja nie posiadająca osobowości prawnej, usytuowana poza Ministerstwem;
17) **środowisko produkcyjne** — zasoby ePUAP wykorzystywane do pracy z aplikacjami korzystającymi z danych rzeczywistych;
18) **środowisko testowe** — zasoby ePUAP wykorzystywane do testowania środowiska ePUAP;
19) **środowisko rozwojowe (deweloperskie)** — zasoby systemu teleinformatycznego wykorzystywane do tworzenia, rozwijania i testowania aplikacji ePUAP;
20) **wirtualna sieć lokalna (VLAN)** — logicznie wydzielona grupa urządzeń lub użytkowników, dobranych pod względem funkcji, przyporządkowania lub aplikacji, niezależnie od ich fizycznej lokalizacji w sieci lokalnej;
21) **wirtualna siec prywatna (VPN)** — sieć stosująca szyfrowanie pakietów pomiędzy ruterami brzegowymi;
22) **zapora sieciowa (firewall)** — urządzenie bądź system ochrony sieci teleinformatycznych przed nieuprawnionym dostępem z zewnątrz;
23) **zasoby kluczowe** — zasoby niezbędne do funkcjonowania ePUAP.

2. ORGANIZACJA BEZPIECZEŃSTWA

Infrastruktura bezpieczeństwa informacji

I. Na infrastrukturę bezpieczeństwa informacji składają się:
1) działający pod przewodnictwem Ministra lub osoby przez niego upoważnionej Zespół Koordynacji Bezpieczeństwa Informacji (ZKBI), który tworzą:
a) Dyrektor DSI jako zastępca przewodniczącego,
b) Dyrektor DEPiT,
c) ABI,
d) Naczelnik Wydziału Polityki Informatyzacji Państwa DSI,
e) Naczelnik Wydziału Bezpieczeństwa Systemów Infrastruktury Teleinformatycznej;
2) koordynowanie bezpieczeństwa sprawowane przez Dyrektora DSI i Dyrektora DEPiT Ministerstwa we współpracy z osobami odpowiedzialnymi za bezpieczeństwo systemu;
3) autoryzacja urządzeń do przetwarzania informacji realizowana przez DEPiT;
4) doradztwo w dziedzinie bezpieczeństwa informacji uzyskiwane w miarę potrzeb i świadczone przez konsultantów wewnętrznych, jak i zewnętrznych;
5) niezależne przeglądy wdrożonej polityki bezpieczeństwa informacyjnego realizowane w miarę potrzeb przez zewnętrzną organizację specjalizującą się w dokonywaniu takich przeglądów, nie rzadziej jak raz w roku.

II. Przed uzyskaniem dostępu do zasobów ePUAP osoba trzecia musi podpisać na piśmie lub elektronicznie musi zapoznać się i zaakceptować postanowienia stanowiące załącznik do niniejszych zasad.

Zlecanie przetwarzania informacji podmiotom zewnętrznym

1. Powierzenie przetwarzania informacji prawnie chronionej jest dozwolone tylko w przypadkach opisanych w powszechnie obowiązujących aktach pranych.
2. Zlecanie przetwarzania innych informacji znajdujących się w ePUAP możliwe jest po spełnieniu przez stronę świadczącą taką usługę zasad zawartych w „Polityce Bezpieczeństwa ePUAP" i innych wewnętrznych aktach dotyczących bezpieczeństwa informacji w ePUAP.

3. KLASYFIKACJA ZASOBÓW

Rozliczalność zasobów

1. Za zasoby ePUAP odpowiada Dyrektor DSI lub Dyrektor DEPiT stosownie do swoich kompetencji wynikających z Regulaminu Organizacyjnego Ministerstwa.

2. Wszystkie zasoby ePUAP podlegają inwentaryzacji i klasyfikacji ze względu na ich kluczowość w procesie funkcjonowania systemu. Zinwentaryzowane zasoby fizyczne podlegają oznakowaniu.
3. Inwentaryzacja zasobów fizycznych systemu teleinformatycznego obejmuje konfigurację tych zasobów uwzględniającą aktualnych użytkowników. Za każdy środek należący do tego zasobu odpowiedzialny jest jednoznacznie określony pracownik Ministerstwa.

Klasyfikacja informacji

1. Oznaczenia klasyfikacji umieszcza się zarówno na dokumentach w postaci papierowej, jak i na wymiennych komputerowych nośnikach danych. Oznaczenia klasyfikacji informacji przechowywanej na komputerowych nośnikach niewymiennych realizuje się w miarę potrzeb i możliwości.
2. W ePUAP nie przetwarza się dokumentów niejawnych.
3. Dokumenty lub komputerowe nośniki danych zawierające dane osobowe posiadają oznaczenie „DANE OSOBOWE";
4. Oznaczenia innych klas dokumentów niż wynikające z przepisów powszechnie obowiązujących i aktów wewnętrznych tworzone są w miarę potrzeb przez osoby odpowiedzialne w uzgodnieniu z Dyrektorem DSI.

4. BEZPIECZEŃSTWO OSOBOWE

Bezpieczeństwo przy określaniu zakresów czynności i zarządzaniu zasobami ludzkimi

1. Każdy pracownik/współpracownik Ministerstwa mający dostęp do zasobów ePUAP odpowiada za bezpieczeństwo informacyjne w takim zakresie, jaki wynika posiadanej przez niego roli w ePUAP.
2. Zakres czynności pracownika/współpracownika uwzględnia obowiązek przestrzegania zasad bezpieczeństwa informacyjnego.
3. Pracownik/współpracownik wykonujący czynności w ePUAP, które są objęte niniejszymi zasadami podpisuje oświadczenie o którym mowa w ust. 2, stanowiące załącznik do niniejszych zasad.

Szkolenia

1. Każdy pracownik zaangażowany w ePUAP podlega szkoleniu z zakresu zasad zarządzania bezpieczeństwem informacyjnym.
2. Pracownik dopuszczony do pracy w ePUAP potwierdza fakt przeszkolenia w zakresie zasad bezpieczeństwa użytkowania ePUAP na formularzu wniosku o przyznanie dostępu do ePUAP.
3. Dodatkowe szkolenie pracowników przeprowadza się po każdorazowej zmianie zasad dotyczących zapewnienia bezpieczeństwa informacji, w zakresie stosownym do roli, jaką spełnia dany pracownik w ePUAP.
4. Za opracowanie metodyki szkolenia, materiałów szkoleniowych oraz przeszkolenie instruktorów z zakresu zasad zarządzania bezpieczeństwem informacyjnym, odpowiada Dyrektor DSI.
5. Szkolenia w zakresie dostępu do danych osobowych, normują odrębne przepisy.

Reagowanie na naruszenie bezpieczeństwa i niewłaściwe funkcjonowanie systemu

1. Każdy pracownik, który stwierdzi niewłaściwe funkcjonowania ePUAP ma obowiązek zgłosić ten fakt do ServiceDesku. Jeśli nieprawidłowe funkcjonowanie systemu ma związek z naruszeniem zasad bezpieczeństwa, ServiceDesk ma obowiązek natychmiastowego powiadomienia o takim zdarzeniu odpowiednio ABI, AS, IBI.
2. Każdy pracownik, który powziął wiadomość o naruszeniu zasad bezpieczeństwa jest zobowiązany do złożenia notatki służbowej swojemu bezpośredniemu przełożonemu.
3. Informacje o naruszeniu zasad bezpieczeństwa przekazywane są do ABI w zakresie naruszenia zasad ochrony danych osobowych, AS i IBI w zakresie naruszenia zasad bezpieczeństwa systemu. Po przyjęciu zgłoszenia, osoby funkcyjne wszczynają postępowanie mające na celu ustalenie okoliczności incydentu, ustalenie osobistej odpowiedzialności pracowników lub funkcjonariuszy za wystąpienie incydentu oraz sformułowanie wniosków wypływających z zaistniałej sytuacji, ze szczególnym uwzględnieniem propozycji zmian w unormowaniach obowiązujących w ePUAP. Jeśli przyczyną incydentu jest nieprzestrzeganie przez pracownika lub funkcjonariusza obowiązujących zasad, wobec takiego pracownika ABI kieruje wniosek do Dyrektora Generalnego Ministerstwa o wszczęcie postępowania dyscyplinarnego.
4. Jeśli przyczyna incydentu leży poza Ministerstwem, ABI podejmuje czynności, stosownie do zaistniałego incydentu. i zawiadamia o podejrzeniu popełnieniu przestępstwa zgodnie z obowiązującymi przepisami prawa.
5. W przypadkach szczególnie groźnych incydentów, godzących w kluczowe zasoby ePUAP, wnioski wynikające z postępowania wyjaśniającego muszą być przedstawiane na ZKBI.
6. Każdy pracownik ma prawo i obowiązek zgłaszania na drodze służbowej zauważonych podatności ePUAP na zagrożenia i na zjawiska powodujące jego nieprawidłowe funkcjonowanie oraz wniosków mających na celu podniesienie poziomu bezpieczeństwa systemu. Wnioski takie kierowane są do ServiceDesku.

5. ZABEZPIECZENIA FIZYCZNE I BEZPIECZEŃSTWO ŚRODOWISKA

Obszary bezpieczne

1. Ustala się podział obszarów wykorzystywanych przez ePUAP na strefy administracyjne i strefy bezpieczeństwa.
2. Na granicach strefy administracyjnej odbywa się kontrola ruchu osobowego i środków w postaci rzeczowej.
3. Strefa bezpieczeństwa, to obszar wydzielony „solidnymi konstrukcjami budowlanymi", posiadający wejście ze strefy administracyjnej. Za solidne konstrukcje budowlane uznaje się takie, których ściany zewnętrzne i stropy budynków, w których zlokalizowane są strefy bezpieczeństwa powinny mieć klasę odporności włamaniowej równoważnej murowi wykonanemu z „pełnej cegły" (25 cm).
4. Wszystkie osoby przebywające w strefie administracyjnej muszą posiadać identyfikatory. Pracownicy Ministerstwa posiadają identyfikatory zawierające: zdjęcie, imię i nazwisko, nazwę komórki organizacyjnej. Goście posiadają identyfikatory z napisem „Gość".
5. W przypadku, gdy wejście do strefy administracyjnej sterowane jest systemem kontroli dostępu, identyfikator powiązany jest z urządzeniem aktywującym przejście.
6. W przypadku stosowania systemu kontroli dostępu musi być to system z klasą dostępu B i klasą rozpoznania 2 na wejściu i na wyjściu.
7. Wszystkie drzwi z kontrolą dostępu muszą być zaopatrzone w urządzenia samozamykające.
8. Kontrolę ruchu osobowego i materiałowego na granicy strefy administracyjnej sprawuje dodatkowo pracownik ochrony, który wydaje identyfikatory gościom oraz jest zobowiązany do dopilnowania ich zwrotu.
9. Pomieszczenia biurowe w strefie administracyjnej, w których znajdują się terminale systemu teleinformatycznego powinny posiadać zamki klasy co najmniej A. Pomieszczenia w strefach bezpieczeństwa powinny posiadać zamki klasy C według Polskiej Normy PN-EN 12209.
10. Klucze od pomieszczeń przechowywane są u ochrony obiektu, z tym, że klucze do pomieszczeń w strefach bezpieczeństwa muszą być zdawane na przechowanie w zaplombowanych pojemnikach.
11. Klucze wydaje się na podstawie rejestru osób upoważnionych do pobierania kluczy, po sprawdzeniu tożsamości osoby pobierającej klucz. Fakt wydania kluczy i przyjęcia ich na przechowanie musi być odnotowany w książce wydawania kluczy.
12. Za przyznanie i odebranie prawa do pobierania kluczy do konkretnego pomieszczenia odpowiedzialny jest w dyrektor komórki organizacyjnej, któremu podlega dane pomieszczenie.
13. Za zamawianie kluczy odpowiada Biuro Administracyjno-Finansowe Ministerstwa, zwane dalej „BAF". Wydawaniem kluczy oraz prowadzeniem rejestru osób upoważnionych do wydania kluczy do pomieszczeń zawierających zasoby ePUAP zajmuje się Biuro Ochrony Informacji Niejawnych Ministerstwa, zwane dalej „BOiN" i odbywa się zgodnie z obowiązującą procedurą, która musi być uzgodniona z ABI oraz dyrektorami DSI i DEPiT w zakresie ich kompetencji.
14. Wstęp do strefy bezpieczeństwa jest ograniczony tylko do tych osób, które uzyskały stosowne uprawnienia nadane przez Dyrektora BOiN, w porozumieniu dyrektorami DSI i DEPIT w zakresie ich kompetencji, zgodnie z obowiązującą procedurą.
15. Wejście oraz wyjście ze stref bezpieczeństwa jest rejestrowane. Rejestruje się tożsamość osób oraz czas ich wejścia i wyjścia.
16. Wnoszenie do stref i wynoszenie ze stref bezpieczeństwa komputerowych nośników danych może mieć miejsce tylko w przypadkach wynikających z procedur eksploatacji zainstalowanego tam sprzętu teleinformatycznego i podlega rejestracji.
17. Zabrania się wnoszenia do stref bezpieczeństwa urządzeń elektronicznych i zewnętrznych nośników danych. W wyjątkowych przypadkach zezwala się na ich wnoszenie za indywidualną zgodą dyrektorów DSI i DEPiT w zakresie ich kompetencji, zgodnie z obowiązującą procedurą.
18. Zabrania się wnoszenia do stref bezpieczeństwa urządzeń służących rejestracji dźwięku i obrazu, w tym telefonów komórkowych.
19. Strefy bezpieczeństwa powinny być chronione systemem sygnalizacji włamania i napadu oraz wyposażane w urządzenia pozwalające na alarmowe powiadomienie obsługi/ochrony w wypadku zagrożenia zdrowia i życia osób w nich przebywających.
20. W uzasadnionych przypadkach, zarówno strefy administracyjne jak i strefy bezpieczeństwa, powinny być poddane monitoringowi wizyjnemu.
21. W strefach bezpieczeństwa dopuszcza się przebywanie osób bez uprawnień dostępu do tych stref tylko w wyjątkowych przypadkach, za zezwoleniem osoby sprawującej funkcję IBI w określonym celu i wyłącznie pod nadzorem osoby posiadającej uprawnienia dostępu do danej strefy.

22. Pobyt osoby, która nie posiada uprawnień do przebywania w strefie bezpieczeństwa musi zostać odnotowany w rejestrze pobytu. Rejestr zakładany jest przez IBI, a wpisy dokonywane są pod nadzorem osoby uprawnionej do przebywania w danej strefie.
23. Ochrona stref administracyjnych i stref bezpieczeństwa sprawowana jest na zasadach określonych w ustawie o ochronie osób i mienia oraz zgodnie z Planem Ochrony.
24. Za organizację ochrony fizycznej odpowiedzialne jest BOiN.

Zabezpieczenie sprzętu

1. Serwery, aktywne i pasywne urządzenia sieci teleinformatycznej, urządzenia zapewniające zasilanie bezprzerwowe oraz rozdzielnie energetyczne zasilające uprzednio wymieniony sprzęt, magazyny kopii zapasowych, archiwa, zbiory danych osobowych oraz zbiory innych informacji wrażliwych, muszą być umieszczone w strefach bezpieczeństwa.
2. Stopień ochrony zasobów wymienionych w ust. 1, wyrażający się użytymi do tego celu środkami, zależny jest od analizy ryzyka oraz od obowiązujących w tym zakresie przepisów prawa.
3. Zasoby, którym nadano status zasobu kluczowego podlegają szczególnej ochronie i są dodatkowo zabezpieczane.
4. Zabronione jest spożywanie posiłków oraz napojów w pomieszczeniach, w których rozmieszczono sprzęt wymieniony w ust. 1.
5. Warunki środowiska, w którym pracuje sprzęt teleinformatyczny zaliczany do zasobów kluczowych muszą być monitorowane i raportowane. Raportowanie odbywa się na zasadach określonych w szczegółowych procedurach uwzględniających warunki konkretnej lokalizacji.
6. Urządzenia infrastruktury zapewniające warunki środowiska muszą być przeglądane i konserwowane zgodnie z instrukcjami i wymaganiami ich producentów.
7. Komputery przenośne podlegają szczególnej ochronie zgodnie z obowiązującą procedurą. Ich używanie poza siedzibą Ministerstwa musi mieć uzasadnienie w realizowanych przez ich użytkownika zadaniach.
8. Na użytkowniku komputera przenośnego spoczywa obowiązek jego ochrony. W szczególności zabrania się pozostawiania bez opieki tego typu komputerów w samochodach, przedziałach kolejowych oraz innych miejscach gdzie użytkownik nie ma możliwości sprawowania nad nimi skutecznego nadzoru.
9. Informacja wrażliwa, przechowywana na komputerze przenośnym jest szyfrowana.
10. W przypadku utraty komputera przenośnego, zawierającego dane związane z systemem ePUAP, użytkownik niezwłocznie powiadamia o tym fakcie swojego bezpośredniego przełożonego oraz ServiceDesk, a w przypadku kradzieży dokonuje również niezwłocznego zgłoszenia popełnienia. W powiadomieniu tym podane musi być imię i nazwisko użytkownika, nazwa jednostki lub komórki organizacyjnej, stanowisko oraz nazwa konta. W zawiadomieniu do bezpośredniego przełożonego użytkownik podaje okoliczności utraty komputera oraz opis charakteru utraconych danych wraz z podaniem ich znaczenia dla ePUAP. W szczególności w zawiadomieniu należy określić, czy utracone dane miały charakter danych osobowych. Przełożony danej osoby przekazuje informację o zdarzeniu do ServiceDesk.

Zasilanie

1. Wszystkie urządzenia sieci teleinformatycznej muszą być zasilane napięciem o parametrach zgodnych z wymaganiami producenta.
2. Urządzenia od ciągłości pracy których zależne jest realizowanie podstawowych zadań ePUAP, muszą być zasilane z gwarantowanych źródeł.
3. Gwarantowane zasilanie uzyskiwane jest przez zastosowanie dywersyfikacji zewnętrznych źródeł energii elektrycznej z samoczynnym załączaniem rezerwy (SZR), zastosowanie zasilaczy bezprzerwowych (UPS), zastosowanie awaryjnych agregatów prądotwórczych. Konfiguracja zasilania gwarantowanego musi wynikać z Planu Zapewnienia Ciągłości Działania.
4. Każde urządzenie, o którym jest mowa w ust. 2, musi być opatrzone tabliczką, z której wynika skąd dane urządzenie jest zasilane, zawierającą nazwę rozdzielnicy lub tablicy zabezpieczeń oraz nazwę pola w rozdzielnicy lub bezpiecznika na tablicy zabezpieczeń.
5. Stan zasilania zasobów, którym nadano status zasobu kluczowego, musi być na bieżąco monitorowany i raportowany dyżurnym administratorom. Jakość zasilania pozostałych zasobów musi być okresowo sprawdzana.
6. Zasilacze bezprzerwowe, zasilające kluczowe zasoby, muszą raportować stan swojej pracy (zasilanie z sieci, zasilanie z baterii) oraz parametry baterii (jej stopień naładowania i przewidziany czas pracy z baterii przy danym obciążeniu) systemom operacyjnym serwerów. W przypadku, gdy stopień naładowania baterii osiągnie w czasie pracy z baterii poziom, którego przekroczenie nie gwarantuje podtrzymania ciągłości pracy, system operacyjny musi wymuszać automatyczne zamknięcie aplikacji i baz danych oraz kontrolowane wyłączenie serwera.

7. Elementy systemu zasilania gwarantowanego muszą podlegać okresowym przeglądom i konserwacjom. Szczególną uwagę należy zwrócić na konserwacje akumulatorów i bezwzględne przestrzeganie ich wymiany po okresach eksploatacji przewidzianych w instrukcjach użytkowania. Agregaty prądotwórcze muszą być okresowo uruchamiane w okresach przewidzianych przez ich producentów i pracować przez czas i w warunkach przez tych producentów ustalonych. Wyniki przeglądów i czynności konserwacyjnych muszą być dokumentowane i przedstawiane w formie raportów Dyrektorowi DEPiT do wiadomości Dyrektora DSI.
8. Agregaty prądotwórcze, o ile są stosowane, muszą posiadać niezbędny zapas paliwa oraz muszą być opracowane procedury uzupełniania paliwa pozwalające na zasilanie z wykorzystaniem tych agregatów do momentu przywrócenia zasilania zewnętrznego.
9. Przeciwpożarowe wyłączniki zasilania muszą być umieszczone w miejscach uzgodnionych ze Strażą Pożarną, przy jednoczesnym ich zabezpieczeniu przed użyciem przypadkowym bądź wykorzystaniem do celów sabotażowych.
10. W miarę potrzeb budynki powinny być wyposażone w instalację odgromową, a linie energetyczne i telekomunikacyjne (wykorzystujące technologie z użyciem kabli przewodzących) powinny być zaopatrzone w zabezpieczenia przepięciowe.

Bezpieczeństwo okablowania

1. Za bezpieczeństwo okablowania energetycznego i telekomunikacyjnego odpowiada Dyrektor DEPiT.
2. Okablowanie energetyczne i telekomunikacyjne musi być między sobą oddalone na odległość gwarantującą brak wzajemnego oddziaływania linii.
3. Okablowanie musi być wykonane w taki sposób, aby ograniczyć możliwość dostępu do niego osób nieuprawnionych. Wymóg ten musi być uwzględniany przy projektowaniu sieci energetycznej i teleinformatycznej.
4. Kable i skrzynki kablowe muszą posiadać oznaczenia techniczne zgodne z dokumentacją. Oznaczenie takie nie może zawierać informacji pozwalającej osobie postronnej na identyfikację przeznaczenia danego okablowania lub skrzynki kablowej.
5. Przy projektowaniu przebiegu linii sieci teleinformatycznej poza strefami administracyjnymi należy w maksymalnym stopniu stosować rozwiązania wykorzystujące technologie światłowodowe.
6. Aktualnie niewykorzystywane segmenty sieci strukturalnej w zakresie ePUAP winny być niezwłocznie odłączone od sieci teleinformatycznej. Ich dołączenie do sieci odbywa się na wniosek kierownika wewnętrznej komórki organizacyjnej albo jednostki podległej lub nadzorowanej przez Ministra, zatwierdzony przez dyrektora danej jednostki lub komórki organizacyjnej. Podłączenia dokonuje administrator sieci. Kierownik wewnętrznej komórki organizacyjnej ma obowiązek powiadomić ServiceDesk o zaprzestaniu wykorzystywania danego segmentu sieci strukturalnej, a ten z kolei ma obowiązek zawiadomić administratora sieci, który dokonuje odłączenia takiego segmentu od sieci teleinformatycznej.

Konserwacja i naprawy sprzętu

1. Sprzęt, stanowiący zasób teleinformatyczny, podlega konserwacji według ustalonego planu, wynikającego z zaleceń jego producenta.
2. Konserwacja i naprawy mogą być prowadzone jedynie przez uprawniony personel Ministerstwa lub podmiot zewnętrzny świadczący tego rodzaju usługi na podstawie umowy lub w ramach gwarancji.
3. W przypadku, gdy na nośnikach informacji, stanowiących integralną część sprzętu przekazywanego do naprawy, znajduje się informacja chroniona prawnie, sprzęt taki naprawiany jest pod nadzorem uprawnionego pracownika Ministerstwa. Jeżeli zaś taki nadzór nie jest możliwy, informacja nadzorowana musi zostać skutecznie usunięta. O ile zachodzi taka możliwość, usuwana informacja powinna być uprzednio zarchiwizowana.
4. Jeżeli podmiot zewnętrzny, w ramach naprawy gwarancyjnej, żąda zwrotu urządzenia służącego do przechowywania informacji, informacja wrażliwa znajdująca się w takim urządzeniu musi zostać z niego trwale usunięta.
5. Umowy zawierające gwarancję dostawcy lub producenta muszą zawierać sformułowania umożliwiające usunięcie trwałe informacji z urządzenia o którym mowa w ust. 4 bez utraty gwarancji.
6. W przypadku zaprzestania użytkowania sprzętu w ramach ePUAP należy skutecznie usunąć z niego informacje.

Zabezpieczenia ogólne

1. W ePUAP wprowadza się „politykę czystego biurka i ekranu” obejmującą następujące zasady:
   1) dokumenty papierowe i nośniki komputerowe, kiedy nie są używane, przechowuje się w odpowiednich, zamykanych szafach lub innego rodzaju zabezpieczonych meblach, szczególnie poza godzinami pracy;
   2) nośniki informacji wrażliwej, jeśli nie są aktualnie wykorzystywane, zamykane są w meblach biurowych, szafkach metalowych lub sejfach, w zależności od ich ważności;
   3) komputery osobiste i stacje robocze nie mogą być pozostawiane bez nadzoru w stanie zarejestrowania do sieci.

2. Wydruki zawierające informacje wrażliwe muszą być niezwłocznie zabierane z drukarki sieciowej.
3. Fotokopiarki powinny uniemożliwiać nieautoryzowane wykonywanie kopii.
4. Wynoszenie mienia ePUAP poza pomieszczenia serwerowni może się odbywać jedynie na podstawie odpowiednich dokumentów. Nie dotyczy to komputerów przenośnych i telefonów komórkowych. Za ich bezpieczeństwo odpowiedzialne są osoby, którym te urządzenia przydzielono.

VI. ZARZĄDZANIE SYSTEMAMI I SIECIAMI

Procedury eksploatacyjne oraz zakresy odpowiedzialności

1. W celu zapewnienia prawidłowej i bezpiecznej eksploatacji systemów teleinformatycznych wprowadza się, realizuje i dokumentuje procedury związane z cyklem życia tychże systemów. W przypadku nowych systemów procedury obejmują prace projektowe, testowanie, obsługę i ich rozwój.
2. Dokumentacja wprowadzanych do eksploatacji systemów musi zawierać instrukcje i procedury ich bezpiecznej eksploatacji oraz dokładny opis zastosowanych w ich konstrukcji mechanizmów zabezpieczających, zarządzanych i nadzorowanych przez wyznaczoną grupę użytkowników.
3. Opracowane procedury eksploatacyjne są zatwierdzane przez Dyrektora DEPiT w uzgodnieniu z ABI.
4. Za zorganizowanie pracy, zapewnienie bezpieczeństwa oraz prawidłową eksploatację systemu i sprzętu komputerowego, przydzielonego do odpowiedzialnych za ePUAP poszczególnych komórek i jednostek organizacyjnych nadzorowanych przez Ministra, odpowiedzialni są ich kierownicy.
5. Za bezpieczeństwo i dostęp do terminala lub komputera oraz za jego prawidłową eksploatację odpowiedzialny jest użytkownik danego terminala lub komputera.
6. W przypadku korzystania z komputera przez kilku użytkowników, kierownik komórki organizacyjnej, bądź jednostki wyznacza osobę odpowiedzialną za sprzęt. Określa on uprawnienia i obowiązki wszystkich współużytkowników tego sprzętu.
7. Przy realizacji szczególnie odpowiedzialnych zadań wymagany jest podział uprawnień tak, aby wykonanie zadania wymagało ścisłej współpracy co najmniej dwóch osób (autoryzacja co najmniej dwóch osób).
8. Obowiązki użytkowników systemu teleinformatycznego określa w zakresie swoich kompetencji kierownik komórki organizacyjnej Ministerstwa w porozumieniu z ABI.
9. Uprawnienia użytkowników sprawujących funkcje administracyjne w ePUAP określa kierownik wewnętrznej komórki bądź jednostki organizacyjnej za zgodą Dyrektora DSI. Podlegają one wpisowi do zakresu czynności pracownika i są potwierdzane jego podpisem.
10. Pracownicy mogą zgłaszać drogą służbową postulaty dotyczące:
    1) funkcjonowania systemu teleinformatycznego — do ServiceDesk,
    2) bezpieczeństwa systemu teleinformatycznego — do ABI, IBI oraz bezpośredniego przełożonego.
11. Prace rozwojowe nie mogą być prowadzone w środowisku produkcyjnym lub testowym. Środowisko rozwojowe, w którym dokonywane są zmiany musi być fizycznie i logicznie odseparowane od środowiska produkcyjnego i testowego. Środowisko to musi być oddzielone od danych rzeczywistych, przetwarzanych w środowisku produkcyjnym.

Rozwój i utrzymanie systemu

1. Dyrektor DEPiT, w porozumieniu z Dyrektorem DSI, przynajmniej raz do roku ustala zalecenia konfiguracji sprzętu, które obowiązują w Ministerstwie. Zamówienia w zakresie wykraczające poza te zalecenia zatwierdzane będą przez Dyrektora DEPiT, przy akceptacji Dyrektora DSI.
2. Wybór dostawcy regulowany jest odrębnymi przepisami.
3. W przypadku zakupów sprzętu komputerowego i oprogramowania dotyczących przetwarzania informacji wrażliwych zgodę na zakup wyraża Dyrektor DEPIT w porozumieniu z Dyrektorem DSI.
4. Specyfikacja dotycząca wymogów bezpieczeństwa powinna być integralną częścią umowy.
5. Decyzję o przeniesieniu oprogramowania ze środowiska rozwojowego do środowiska produkcyjnego podejmuje Dyrektor DEPiT w porozumieniu z Dyrektorem DSI.
6. System teleinformatyczny musi umożliwiać szczegółowe monitorowanie wprowadzanych zmian.
7. Przed oddaniem oprogramowania do użytkowania należy usunąć zeń wszystkie „tylne furtki" i uprawnienia systemowe stworzone w procesie tworzenia i testowania oprogramowania.
8. W trakcie projektowania, tworzenia i testowania oprogramowania stosuje się jednolitą konwencję nazewnictwa plików, bibliotek oraz transakcji, która obejmuje również zasady nazewnictwa w środowisku produkcyjnym tak, aby nie występowały konflikty nazw pomiędzy środowiskami.
9. Dostęp do narzędzi i oprogramowania służących do testowania danego systemu teleinformatycznego posiadają jedynie osoby w zakresie posiadanego posiadanego upoważnienia.

10. Do celów testowych nie wolno wykorzystywać danych rzeczywistych. W wypadku uzasadnionej konieczności przeprowadzania testów opartych na danych rzeczywistych, należy korzystać z odrębnej instancji (kopii) danych, poddanej anonimizacji.
11. Uprawnienia osób korzystających ze środowisk rozwojowych i produkcyjnych określa zakres ich obowiązków.
12. Testy nowych lub zmodyfikowanych aplikacji nie mogą być przeprowadzane przez osoby związane z projektowaniem lub tworzeniem tych aplikacji.

Ochrona przed szkodliwym oprogramowaniem

1. Koniecznym jest stosowanie mechanizmów zabezpieczających dane, w tym bazy danych, które nie dopuszczają do zainfekowania szkodliwym oprogramowaniem, równocześnie posiadając możliwość wykrywania programów destrukcyjnych już zagnieżdżonych w systemie, usuwających je i zabezpieczających przed wystąpieniem następnych.
2. Na stacjach roboczych i serwerach instalowane jest oprogramowanie chroniące przed kodem złośliwym, aktualizowane zgodnie z zaleceniami producenta pod względem wykrywania nowopowstających programów destrukcyjnych.
3. Działania w zakresie standardów ochrony antywirusowej organizuje i koordynuje Dyrektor DEPiT.
4. Zmniejszenie ryzyka zarażenia wirusem komputerowym lub innym złośliwym kodem systemu teleinformatycznego, lub jego części, wymaga przestrzegania następujących zasad:
   1) w każdej jednostce organizacyjnej korzystającej z ePUAP elektroniczne nośniki informacji muszą być sprawdzone przez aktualne oprogramowanie antywirusowe,
   2) po każdej naprawie i konserwacji komputera należy stosować oprogramowanie antywirusowe zawierające najnowsze bazy antywirusowe,
   3) wszystkie komputery podłączone do sieci lokalnej, jak i rozległej, muszą być skonfigurowane tak, aby zapewnić ochronę danych przez centralne oprogramowanie antywirusowe,
   4) wszystkie zaobserwowane przez użytkowników systemu sytuacje, świadczące o nieprawidłowym jego działaniu, muszą być natychmiast zgłaszane do ServiceDesku.

Procedury wewnętrzne

1. Instrukcje użytkowania systemu teleinformatycznego eksploatowanego w ePUAP, muszą zawierać zasady tworzenia kopii bezpieczeństwa i odzyskiwania z nich danych.
2. Za tworzenie kopii bezpieczeństwa w systemie teleinformatycznym odpowiedzialny jest administrator systemu. Zobowiązany jest on do tworzenia kopii bezpieczeństwa programów i zbiorów na nośnikach informacji (backup) zgodnie z procedurą wykonywania kopii zapasowych.
3. Instrukcje o których mowa w pkt 1 oraz procedury, o których mowa w pkt 2, muszą zawierać postanowienia dotyczące:
   1) ilości egzemplarzy tworzonych kopii,
   2) zarządzania nośnikami informacji (ewidencjonowanie, magazynowanie, czas przechowywania, zasady niszczenia i wymiany),
   3) kopiowania programów po dokonaniu każdej zmiany,
   4) wymiany kopii programów co trzy miesiące w przypadku nie dokonywania zmian,
   5) strategii tworzenia kopii uwzględniającej okresy tworzenia kopii, rodzaje składowania w poszczególnych okresach, sposobu weryfikacji poprawności wykonanej kopii, miejsca i sposobu przechowywania,
   6) kopiowania w cyklu dziennym zbiorów danych użytkowych, a zbiorów kończących okresy przetwarzania po zakończeniu danego okresu przetwarzania (w szczególności zbiory kończące rok — w cyklu rocznym),
   7) kopiowania w cyklu rocznym innych zbiorów, chyba że odrębne przepisy przewidują inne terminy,
   8) procesu składowania danych, określającego urządzenia, sposób wykonywania kopii (przyrostowa, pełna, różnicowa) oraz częstotliwość ich wykonywania,
   9) procesu odtwarzania danych ePUAP,
   10) sposobu okresowej weryfikacji nośników pod względem ich przydatności do ewentualnego odtworzenia zachowanych danych.
4. Okresowo, co najmniej raz na rok, należy przeprowadzić pełną procedurę odtworzenia i uruchomienia systemu z kopii bezpieczeństwa.
5. Co najmniej jedną kopię przechowywać należy w sejfach na nośniki magnetyczne, charakteryzujących się odpowiednią klasą odporności na temperaturę, tzn. klasą odporności S120 DIS, czyli odpornością ogniową na oddziaływanie temperatury 1090° C przez czas 2 godzin. Temperatura wewnątrz nie może przekraczać 50° C, a wilgotność 85%.

6. Kopie bezpieczeństwa przechowywane są poza pomieszczeniami, w których zostały utworzone, w pomieszczeniach na tyle oddalonych, aby lokalny pożar czy zalanie wodą nie zniszczył jednocześnie nośników w obu pomieszczeniach. Pomieszczenia te powinny zabezpieczać przed zniszczeniem w skutek pożaru, zalania, bądź oddziaływania silnego pola elektromagnetyczne, jak również przed kradzieżą i nieuprawnionym dostępem.
7. Miejsce przechowywania kopii wskazuje Dyrektor DEPiT, w porozumieniu z Dyrektorem DSI. O miejscu przechowywania kopii informowane są osoby odpowiedzialne za bezpieczeństwo systemu w zakresie s kompetencji.
8. W przypadku przesyłania danych w celu składowania poprzez sieć na inny serwer, przesyłane dane są szyfrowane.
9. Tworzenie i odzyskiwanie (robocze oraz testowe) kopii bezpieczeństwa jest ewidencjonowane w rejestrze kopii bezpieczeństwa prowadzonym przez administratora systemu zgodnie z procedurą wykonywania kopii zapasowych.
10. Odzyskiwanie danych z kopii bezpieczeństwa wykonuje administrator systemu, na polecenie Dyrektora DEPiT, lub osoby przez niego upoważnionej,
11. Nośnik do sporządzania kopii bezpieczeństwa nie może być użyty więcej razy niż wskazuje producent, ani też używany przez czas dłuższy, niż określony przez producenta okres gwarantujący poprawność jego użytkowania. Rozpoczęcie użytkowania danego nośnika kopii jest ewidencjonowane w rejestrze kopii bezpieczeństwa.
12. Ośrodek podstawowy oraz zapasowy ePUAP posiada dziennik systemowy, prowadzony przez administratora.
13. Dzienniki systemowe prowadzone są w formie papierowej oraz, w przypadkach określonych przez Dyrektora DEPiT dodatkowo w formie elektronicznej.
14. Formę papierową dziennika systemowego przechowuje właściwy do zadań administrator systemu, w bezpiecznym miejscu wskazanym przez Dyrektora DEPiT.
15. Wszystkie zmiany w dziennikach powinny być poprawiane w taki sposób aby możliwe było odczytanie poprzedniej treści wpisu wraz z podpisem osoby, która takiej zmiany dokonała.
16. W dzienniku systemowym muszą znajdować się innymi szczególności adnotacje dotyczące:
    1) wykonywanych operacji w systemie teleinformatycznym (zmiany konfiguracyjne systemu, wersja oprogramowania, działania serwisowe),
    2) wystąpienia jakichkolwiek awarii oraz zastosowanych rozwiązań (z wyszczególnieniem osób dokonujących interwencji, czasu interwencji oraz stanu po interwencji).
17. Przed dokonaniem zmian w ePUAP należy sporządzić harmonogram planowanych zmian oraz kopię zapasową. Fakt realizacji poszczególnych zmian należy umieścić w dzienniku systemowym.
18. Wszystkie zmiany muszą być autoryzowane przez osoby odpowiedzialne za bezpieczeństwo systemu w zakresie swoich kompetencji.
19. Zmiany przeprowadzane są w sposób bezpieczny to jest umożliwiający prawidłowe działanie ePUAP oraz powrót do wersji sprzed dokonania zmiany.
20. Szczegółowy opis czynności wykonywanych w ePUAP oraz zapewnienie jego bezpieczeństwa określają odrębne procedury. Procedury te dotyczą wprowadzania istotnych zmian w odniesieniu do sprzętu, łączy komunikacyjnych, procedur i danych.
21. Awaryjne zmiany do oprogramowania mogą mieć miejsce jedynie w przypadkach określonych przez Dyrektora DEPiT w porozumieniu z Dyrektorem DSI i są przeprowadzane pod szczególnym nadzorem.
22. Wnioski o dokonanie zmiany są rejestrowane, analizowane pod kątem zasadności, ryzyka, wykonalności, kosztu, zysku z przeprowadzenia danej zmiany, wpływu na pozostałe części systemu teleinformatycznego, a także pod kątem możliwości późniejszej weryfikacji tej zmiany.
23. Zmianę ePUAP w zakresie materialnym oraz jej techniczną i użytkową dokumentację przyjmuje Dyrektor Generalny Ministerstwa.
24. Przed wprowadzeniem zmiany do środowiska produkcyjnego przeprowadzane są następujące testy: bezpieczeństwa, obciążeniowe, równoległe, objętościowe, integracyjne, funkcjonalne, akceptacyjne użytkowników oraz regresyjne wykonywane w środowisku testowym.
25. Po wprowadzeniu kluczowej zmiany każdorazowo przeprowadzana jest ponownie analiza ryzyka systemu, uwzględniająca zmiany i jest przekazywana do akceptacji Dyrektorowi DSI. Po jej zaakceptowaniu jest przekazywana Dyrektorowi DEPiT w celu jej wykorzystania.
26. Na podstawie zaakceptowanej analizy ryzyka ePUAP wykonywana jest aktualizacja dokumentacji bezpieczeństwa systemu oraz wprowadzane są ewentualne czynności zaradcze w celu minimalizacji wykrytego ryzyka.
27. Szczegółowy raport z przebiegu testów oraz ich wyniki przekazywane są Dyrektorowi Generalnemu i Dyrektorowi DSI oraz Dyrektorowi DEPiT, którzy zatwierdzają wdrożenie zmiany. Jeśli jednak zmiana nie spełnia wymagań, zmiana kierowana jest do poprawki.

28. Wszystkie instrukcje użytkowania i materiały dla użytkowników zatwierdzane są przez WZ.
29. Jeśli zmiana ma charakter nagły, jej dokumentacja może być dostarczona Dyrektorowi DSI i DEPiT najpóźniej w przeciągu 7 dni od dokonania zmiany.
30. Pracownicy korzystający z danej aplikacji są szkoleni w związku z jej zmianami.
31. ePUAP jest poddawany okresowym kontrolom przez IBI, nie rzadziej niż raz na 6 miesięcy, w celu stwierdzenia, czy nie miały miejsca jakiekolwiek nieautoryzowane zmiany.
32. AS dokonuje regularnych przeglądów ePUAP pod kątem konieczności instalacji poprawek i aktualizacji. Poprawki i aktualizacje bezpieczeństwa należy instalować niezwłocznie i zgodnie z procedurą zarządzania zmianą.
33. Wszystkie uaktualnienia instalowane są za zgodą Dyrektora DEPiT.
34. W sytuacji, gdy niezbędne jest potwierdzenie wykonania prac w ePUAP, należy na kopii papierowej dziennika umieścić stosowny wpis, zawierający opis zdarzenia, datę i podpis osoby wykonującej prace.
35. Działania serwisowe w ePUAP w szczególności: modyfikacja konfiguracji, czynności serwisowe, muszą być dokonywane pod nadzorem AS i zostać przez niego zatwierdzone oraz muszą być odnotowane w dzienniku systemowym. W przypadku działań, które dotyczą elementów przetwarzania informacji wrażliwej oraz mającej wpływ na bezpieczeństwo systemu, wymagany jest również nadzór IBI.
36. Wszelkie zmiany przejęcia obowiązków AS są odnotowywane w dzienniku systemowym. O powyższej zmianie informowany jest IBI oraz ABI.
37. AS, na polecenie Dyrektora DEPiT lub Dyrektora DSI, na podstawie dzienników systemowych przygotowuje raporty dotyczące funkcjonowania systemu.
38. Dzienniki systemowe przeglądane są regularnie przez IBI.
39. Minimum raz w roku IBI sporządza raport z przeglądów dzienników systemowych i przedkłada do wiadomości Dyrektorowi DSI oraz Dyrektorowi DEPiT.

Zarządzanie sieciami i kontrola dostępu do sieci

1. System teleinformatyczny ePUAP, w tym sieci lokalne komórek organizacyjnych Ministerstwa, może być podłączona do sieci ogólnodostępnych szczególnie sieć publiczna Internet tylko na poziomie WAN'u i jedynie przy użyciu specjalnych systemów zabezpieczających (aplikacje i urządzenia typu firewall, systemy IDS/IPS, VPN).
2. Reguły filtrowania zapór sieciowych ustalane są przez Dyrektora DEPiT, po uzgodnieniu z Dyrektorem DSI.
3. Zdalne zarządzanie urządzeniami sieciowymi możliwe jest wyłącznie z odseparowanej fizycznie, od reszty środowiska, sieci zarządzania lub przez konsole podłączone bezpośrednio do urządzeń.
4. W ramach sieci zarządzania powinien zostać logicznie rozdzielony dostęp do urządzeń środowiska testowego oraz produkcyjnego umożliwiający indywidualną rozliczalność dostępu.
5. Dostęp do sieci zarządzania z zewnątrz odbywa się przez VPN.
6. Dostęp do sieci zarządzania posiada jedynie uprawniony personel posiadający imiennie nadany dostęp. Nie dozwolone jest używanie tego samego identyfikatora użytkownika przez więcej niż jedną osobę.
7. Za kwestie rozliczalności dostępu do zasobów sieci zarządzania ePUAP odpowiada podmiot posiadający do niego dostęp, który jest zobowiązany przedstawiać Dyrektorowi DEPiT lub upoważnionemu przez niego pracownikowi cykliczne raporty.
8. Ruch w sieci zarządzania jest monitorowany.
9. Hasła w urządzeniach powinny być okresowo zmieniane zgodnie z odpowiednią procedurą.
10. Wszystkie punkty zdalnego dostępu do sieci ePUAP muszą być zweryfikowane i zatwierdzone przez DSI w porozumieniu z DEPiT. Wykorzystywanie przez użytkowników nieautoryzowanych rozwiązań stanowi pogwałcenie Polityki Bezpieczeństwa i będzie skutkowało zablokowaniem dostępu.
11. Kontroli podlega każdy ruch docierający do systemu ePUAP z innych systemów oraz ruch związany z komunikacją podsystemów ePUAP z innymi systemami. Ponadto kontrolowany jest ruch wewnętrzny systemu ePUAP, w zakresie jaki jest wymagany do ochrony poszczególnych podsystemów systemów wewnętrznych szczególnie podsystemu usług bezpieczeństwa związanych z autoryzacją i obsługą podpisu cyfrowego w rozumieniu ustawy o podpisie elektronicznym.
12. Testy agresywne ePUAP możliwe są jedynie na podstawie scenariusza zatwierdzonego przez Dyrektora DEPiT w porozumieniu z Dyrektorem DSI, ABI oraz IBI.
13. Zabrania się testowania zabezpieczeń w środowisku produkcyjnym oraz wykonywania prób przełamywania tych zabezpieczeń bez scenariusza zatwierdzonego przez Dyrektora DEPiT w porozumieniu z Dyrektorem DSI, ABI oraz IBI.
14. Serwery zewnętrznych usług sieciowych są zlokalizowane w wydzielonych sekcjach (DMZ).
15. Sekcje DMZ są sekcjami o zwiększonym ryzyku ataku, wobec czego nie mogą znajdować się w niej urządzenia przetwarzające informacje wrażliwe.
16. Wszelkie usługi sieciowe udostępniane w sieci publicznej muszą zostać zaakceptowane przez ZKBI.

17. Za zgodą ZKBI ePUAP może zostać połączona z innymi sieciami zewnętrznymi w sposób nie powodujący obniżenia poziomu bezpieczeństwa systemu. Każdorazowo projekt podłączenia musi być poprzedzony analizą ryzyka nowego rozwiązania.
18. Hasła dostępu do kluczowych zasobów systemu można przesyłać za pośrednictwem sieci publicznych jedynie przy wykorzystaniu silnych mechanizmów kryptograficznych.
19. W miarę możliwości pracownicy poszczególnych jednostek organizacyjnych Ministerstwa oraz jednostek organizacyjnych podległych Ministrowi lub przez niego nadzorowanych powinni być grupowani w VLAN'y.

Postępowanie z nośnikami i ich bezpieczeństwo

1. Nośniki informacji zawierające dane wrażliwe, w tym wydruki, przechowuje się w miejscach uniemożliwiających dostęp do nich osobom nieuprawnionym.
2. Magnetyczne nośniki informacji zawierające kopie bezpieczeństwa oraz informacje archiwalne należy przechowywać w specjalnych, atestowanych, ogniotrwałych szafach do przechowywania magnetycznych nośników informacji. Pozostałe nośniki przechowuje i zabezpiecza się zgodnie z wymaganiami obowiązującymi dla informacji na nich zapisanych.
3. Ogranicza się do niezbędnego minimum ilość wytwarzanych kopii i wydruków. Między innymi należy zastępować wydruki kopiami na innych nośnikach, jeżeli jest to uzasadnione ekonomicznie.
4. W szczególności zbędne wydruki, notatki, kopie dokumentów, muszą być bezwzględnie niszczone zgodnie z obowiązującymi procedurami i w sposób uniemożliwiający odtworzenie ich treści.
5. Wszystkie nośniki informacji w szczególności dyskietki, taśmy magnetyczne, płyty CD, wymienne dyski twarde oraz wydruki komputerowe, wytworzone w ePUAP i zawierające informacje wrażliwe, są ewidencjonowane i odpowiednio oznakowane.
6. Przemieszczanie elektronicznych nośników danych w szczególności komputerów przenośnych zawierających informacje chronione poza pomieszczenia, w których są one przetwarzane, wymaga stosowania środków ochrony gwarantujących ich zabezpieczenie przed nieuprawnionym dostępem i ujawnieniem informacji.
7. Wycofane nośniki informacji, które były wykorzystywane do przetwarzania informacji chronionych, nie mogą być wynoszone poza teren komórki bądź jednostki organizacyjnej, w której były użytkowane, bez wcześniejszego skutecznego usunięcia danych.
8. Pomieszczenia, w których znajdują się szafy do przechowywania informacji wrażliwych, powinny posiadać system sygnalizacji pożaru oraz system sygnalizacji włamania.
9. Szafy do przechowywania danych wrażliwych powinny zapewniać ochronę przed:
   1) pożarem i eksplozją;
   2) działaniem gazów powstałych podczas pożaru;
   3) zalaniem i wodą występującą podczas gaszenia pożaru;
   4) działaniem silnych pól elektromagnetycznych (dotyczy nośników).
10. Uszkodzone dyski twarde, dyskietki i taśmy magnetyczne, płyty CD i inne komputerowe nośniki danych, zawierające dane wrażliwe, należy komisyjnie niszczyć w sposób uniemożliwiający odczytanie zapisanych na nich informacji w szczególności poprzez zgniatanie, łamanie, działanie silnym polem magnetycznym. W skład komisji wchodzą upoważnieni pracownicy przez Dyrektora DEPiT oraz upoważnieni pracownicy przez Dyrektora DSI.

VII. KONTROLA LOGICZNA DOSTĘPU DO SYSTEMU

Dostęp do systemu

1. Kontrola dostępu do zasobów ePUAP jest realizowana z wykorzystaniem odpowiednich mechanizmów autentykacji użytkowników zapewniających wymagany dla systemu poziom bezpieczeństwa.

Zarządzanie dostępem użytkowników

1. Użytkownik ePUAP jest jednoznacznie rozpoznawany poprzez indywidualny identyfikator (login) użytkownika systemu. Niedopuszczalne jest korzystanie z tego samego identyfikatora przez więcej niż jednego użytkownika. Raz użyty identyfikator nie może być przydzielony innemu użytkownikowi.
2. Uprawnienia dostępu do ePUAP przydzielane są zgodnie z obowiązującymi procedurami. Prawa dostępu do zasobów kluczowych, podsystemu bezpieczeństwa, kont operatorskich oraz kont o podwyższonych uprawnieniach przydzielane są wyłącznie na pisemny wniosek zweryfikowany przez ABI, IBI oraz AS skierowany do Dyrektora DSI i zatwierdzony. Każdorazowy fakt zmiany uprawnień w systemie teleinformatycznym ePUAP musi być odnotowany w odpowiednim dzienniku systemowym.
3. Przyznane użytkownikowi uprawnienia dostępu zgodnie z wnioskiem odpowiadają zajmowanemu stanowisku i wykonywanym zadaniom służbowym oraz są zgodne z polityką bezpieczeństwa ePUAP.
4. AS prowadzi rejestr użytkowników dopuszczonych do zasobów ePUAP. AS po każdej zmianie przekazuje zaktualizowany rejestr IBI oraz na żądanie Dyrektorowi DSI.

5. W razie zmiany zakresu obowiązków pracownika, zmiany stosunku pracy, lub innej umotywowanej przyczyny AS zgodnie z procedurą niezwłocznie dokonuje zmiany uprawnień dostępu do zasobów wymienionych w ust. 2 ePUAP.
6. Obowiązek poinformowania administratora o zmianie związanej z zakresem uprawnień do zasobów systemu spoczywa na osobie wnioskującej o nadanie uprawnień lub bezpośrednim przełożonym takiej osoby.
7. AS ePUAP sprawdza i usuwa zbędne identyfikatory użytkowników oraz kont i nie wykorzystuje ich w celu wydania innym użytkownikom.
8. Prawa dostępu są przydzielane poszczególnym użytkownikom zgodnie z zasadą uprawnień minimalnych oraz wiedzy koniecznej.
9. Hasła do kont dostępu są przekazywane w sposób bezpieczny, jest zaimplementowany automatyczny mechanizm wymuszeniem ich zmiany przy pierwszym logowaniu.
10. Odzyskiwanie utraconego hasła do kont w systemie jest możliwe jedynie zgodnie z odpowiednią procedurą.
11. Zabronione jest przekazywanie haseł przez osoby trzecie lub za pośrednictwem otwartych wiadomości poczty elektronicznej.
12. Przy logowaniu się użytkownika do systemu stosuje się zasady:
    1) użytkownik musi podać swój identyfikator oraz hasło,
    2) w polu logowania nie jest prezentowana ostatnio użyta nazwa użytkownika,
    3) wpisywane hasło nie pojawia się w postaci jawnej na ekranie logowania (nie wyświetlają się znaki wpisywanego hasła).
13. Tworzenie i zarządzanie hasłami uwzględnia zasady:
    1) dotyczące minimalnej długości,
    2) dotyczące minimalnej złożoności,
    3) dotyczące zasad podziału sekretu,
    4) dotyczące maksymalnego okresu ważności,
    5) dotyczące zasad bezpiecznego składowania,
    6) możliwości ponownego wykorzystania.
14. Hasła nie spełniające wymogów bezpieczeństwa są automatycznie odrzucane.
15. Hasła administracyjne w systemie ePUAP muszą być składowane w bezpiecznej postaci i zgodnie z odpowiednimi procedurami składowania. Do przechowywania haseł zapisanych na papierze stosuje się wyłącznie bezpieczne koperty uniemożliwiające na nie zauważalny i nie autoryzowany dostęp do składowanych w nich treści. Koperty z hasłami dodatkowo są składowane w sejfie, w miejscu zapewniającym dostęp tylko osobom upoważnionym.
16. Koperty z hasłami podlegają ścisłej ewidencji. Za przechowywanie oraz ewidencję haseł odpowiadają, w zależności od zasobu Dyrektor DSI lub Dyrektor DEPiT lub osoba pisemnie upoważniona przez jednego z wyżej wymienionych.
17. Ewidencja haseł „bezpiecznych" prowadzona jest w książce ewidencji haseł, która zawiera:
    1) numer ewidencyjny;
    2) oznaczenie przynależności hasła zawartego w kopercie w szczególności: nazwa systemu, zasobu, komputera, elementu aktywnego;
    3) imię i nazwisko, pełnioną funkcję oraz podpis osoby składającej kopertę (właściciela hasła);
    4) datę złożenia koperty;
    5) podpis osoby przyjmującej kopertę na przechowanie;
    6) datę wygaśnięcia ważności hasła zawartego w kopercie;
    7) adnotację o wydaniu koperty z hasłem (użyciu awaryjnym).
18. Przechowywaniu w postaci bezpiecznej podlegają w szczególności hasła dostępu do:
    1) elementów aktywnych sieci teleinformatycznej;
    2) główne hasła administracyjne systemów, aplikacji i baz danych;
    3) konsol serwisowych oraz konfiguracji urządzeń w szczególności: hasła do BIOS, EFI, SC, HMS;
    4) kart kryptograficznych.
19. Dane umieszczone na bezpiecznej kopercie muszą zawierać:
    1) numer koperty adekwatny do numeru ewidencyjnego podanego w książce ewidencji haseł;
    2) datę jej złożenia;
    3) podpis osoby składającej kopertę;
    4) skróconą nazwę przynależności hasła.

20. W sytuacjach szczególnych takich jak: nieobecność właściciela hasła w sytuacjach awaryjnych, zapomniane hasło, gdy konieczny jest dostęp do chronionego hasłem zasobu, Dyrektor DSI, Dyrektor DEPiT lub osoba przez niego upoważniona zezwala pisemnie na wydanie koperty z hasłami wyznaczonej osobie. Przed użyciem hasła w postaci bezpiecznej administrator obowiązany jest skutecznie powiadomić o uzyskanej zgodzie IBI oraz przesłać do DSI raport z użycia hasła w postaci bezpiecznej niezwłocznie po zakończeniu operacji.
21. Uprawnienia użytkowników są przeglądane w regularnych odstępach czasu, nie rzadziej niż co 6 miesięcy oraz każdorazowo po wprowadzeniu zmian w tych prawach.
22. Uprawnienia AS są przeglądane co trzy miesiące przez IBI.

Zakres odpowiedzialności użytkowników i hasła dostępu

1. Użytkownik zobowiązany jest do zachowania haseł w poufności.
2. Użytkownikowi nie wolno udostępniać haseł innym użytkownikom.
3. Hasło nie może być zapisywane na papierze, za wyjątkiem sytuacji opisanej w § 21 ust. 15.
4. W przypadku podejrzenia, iż hasło zostało skompromitowane, użytkownik bezzwłocznie je zmienia i zgłasza ten fakt do ServiceDesk, który bezzwłocznie powiadamia o tym fakcie IBI.
5. Użytkownik wybiera hasło spełniające założone dla systemu warunki złożoności hasła.
6. Hasło tymczasowe, nadawane w momencie utworzenia konta, zmieniane jest podczas pierwszego logowania się użytkownika w ePUAP.
7. Hasło do kont administracyjnych i związanych z dostępem do danych osobowych zmieniane jest co miesiąc i może się powtórzyć dopiero po 5 zmianie.
8. Użytkownicy będący administratorami lub mający dostęp do danych osobowych zobowiązani są zamykać aktywne sesje po zakończeniu pracy, chyba że są one zabezpieczone przez odpowiedni mechanizm blokujący w szczególności wygaszacz ekranu chroniony hasłem.

Kontrola dostępu do systemów operacyjnych

1. Identyfikacja użytkownika odbywa się na podstawie identyfikatora skojarzonego z hasłem. Z identyfikatorem związane są również uprawnienia użytkownika.
2. Blokowany jest dostęp do systemu dla użytkownika, który trzykrotnie pod rząd podał błędne hasło. Odblokowania dokonuje administrator systemu, który nie może w tym celu tworzyć automatów (skryptów) programowych odblokowujących dostęp np. po określonym czasie.
3. System operacyjny po ustalonym okresie bezczynności użytkownika, jednak nie dłużej niż 10 minut, przechodzi w stan, w którym blokowany jest dostęp do konsoli. Powrót do stanu aktywności użytkownika wymaga podania hasła.
4. Stosowane są konta indywidualne, zapewniające zachowanie rozliczalności.
5. Użytkownik sam ustala hasło, którym się posługuje. W przypadku pierwszego logowania hasło generuje ePUAP.
6. System wymusza wybór hasła odpowiedniej jakości.
7. Użytkownik nie może samodzielnie instalować oprogramowania na komputerze służbowym.
8. Usuwane jest z ePUAP zbędne oprogramowanie narzędziowe i systemowe oraz wyłączane są nie używane funkcje oraz usługi systemowe.
9. Systemy operacyjne na których znajdują się kluczowe usługi ePUAP poddawane są obowiązkowo utwardzaniu w celu zwiększenia poziomu bezpieczeństwa. Na serwerach stosowane są rozwiązania zwiększające bezpieczeństwo oparte na RBAC, MAC. Na serwerach pracujących pod kontrolą systemu GNU/Linux wdrożone są i uruchomione rozwiązania takie jak SELinux lub równoważne. Na serwerach pracujących pod kontrolą systemu MS Windows wdrożona jest dodatkowa kontrola na poziomie GPO/GPP.

Kontrola dostępu do aplikacji

1. Aplikacje użytkowe, eksploatowane w ePUAP, posiadają:
   1) mechanizmy autoryzacji i sprawdzania wprowadzanych danych pod względem ich kompletności (dane są oceniane w trakcie procesu ich wprowadzania),
   2) procedury postępowania umożliwiające terminową i sumienną korektę danych,
   3) mechanizmy kontroli przetwarzanych danych, zapobiegających nieautoryzowanemu usunięciu lub modyfikacji danych.
2. Dostęp do danych chronionych w ePUAP jest rejestrowany. Kontrolę dostępu do tych danych w zakresie swoich kompetencji prowadzi Dyrektor DSI wraz z Dyrektorem DEPiT. O każdorazowej zmianie w rejestrze informowany bez zbędnej zwłoki jest ABI.
3. Wszystkie raporty generowane przez system są rejestrowane, z uwzględnieniem identyfikatora użytkownika zlecającego dany raport, oraz oznaczone datą i godziną jego wygenerowania.
4. Zasoby wrażliwe są izolowane ze środowiska, w którym funkcjonują zasoby niewrażliwe.

Monitorowanie dostępu do ePUAP

1. ePUAP jest monitorowany w celu wykrywania w nim nieuprawnionych działań.
2. Zapisywane i archiwizowane są logi zdarzeń. Zapisy te zawierają w szczególności:
   1) identyfikatory użytkowników,
   2) daty i czasy zarejestrowania i wyrejestrowania w systemie,
   3) identyfikator stacji roboczej lub terminala (nazwę komputera w systemie),
   4) zapisy udanych i nieudanych prób dostępu do ePUAP.
3. Monitorowane są fakty użycia urządzeń przetwarzania informacji, zapewniając weryfikację i rozliczalność użytkowników wykonujących procesy, do których zostali uprawnieni.
4. Rejestr zdarzeń jest zabezpieczony przed manipulacją i nieuprawnionymi zmianami.
5. Rejestry zdarzeń są systematycznie przeglądane przez IBI.

Korzystanie z oprogramowania, umożliwiającego zdalny dostęp do systemu teleinformatycznego ePUAP, jest możliwe jedynie za zgodą Dyrektora DSI w porozumieniu z Dyrektorem DEPiT.

Załącznik

OŚWIADCZENIE

Ja niżej podpisany(a)

..... oświadczam, że:

1. Zostałem(am) zapoznany(a) z Polityką Bezpieczeństwa obowiązującą w ePUAP oraz wyciągiem z Zasad Zarządzania Bezpieczeństwem Informacyjnym, dotyczącym mojego stanowiska służbowego i realizowanego zakresu obowiązków.
2. Zobowiązuję się przestrzegać reguł i postanowień tej polityki oraz poznanych zasad w zakresie zapewnienia bezpieczeństwa informacyjnego.
3. Zobowiązuję się do zachowania w tajemnicy wszelkich informacji, do których uzyskam dostęp.
4. Jestem świadomy(a), iż wszystkie moje działania, jako użytkownika zasobów ePUAP, w szczególności dotyczące zasobów wrażliwych, mogą być monitorowane na zasadach określonych przez Ministra Spraw Wewnętrznych i Administracji oraz Dyrektora Generalnego Ministerstwa i wyrażam na to zgodę.
5. Zostałem zapoznany(a) z konsekwencjami służbowymi za nieprzestrzeganie Polityki Bezpieczeństwa ePUAP oraz zasad, reguł i postanowień z niej wynikających.

....., dnia .....
/Data i miejsce złożenia oświadczenia/

.....
/Nr PESEL/

.....
/Podpis osoby składającej oświadczenie/