



DZIENNIK URZĘDOWY

MINISTRA ENERGII

Warszawa, dnia 8 października 2026 r.

Poz. 28



Signed by /
Podpisano przez:
Przemysław
Grzeziok
Date / Data: 2026-
10-08 21:58

ZARZĄDZENIE MINISTRA ENERGII¹⁾

z dnia 7 października 2026 r.

w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji Ministerstwa Energii

Na podstawie art. 34 ust. 1 ustawy z dnia 8 sierpnia 1996 r. o Radzie Ministrów (Dz. U. z 2025 r. poz. 780 oraz z 2026 r. poz. 160) zarządza się, co następuje:

§ 1. 1. W Ministerstwie Energii wprowadza się Politykę Bezpieczeństwa Informacji Ministerstwa Energii, zwaną dalej „PBI”, stanowiącą załącznik do zarządzenia.

2. PBI obowiązuje pracowników Ministerstwa Energii, zwanego dalej „Ministerstwem”, a także osoby i podmioty współpracujące z Ministerstwem – w zakresie wynikającym z zawartych umów, porozumień lub podpisanych oświadczeń.

§ 2. 1. Ustanawia się Pełnomocnika do spraw bezpieczeństwa informacji, zwanego dalej „Pełnomocnikiem”, oraz Zastępcę Pełnomocnika.

2. Pełnomocnika oraz Zastępcę Pełnomocnika powołuje i odwołuje Dyrektor Generalny Ministerstwa.

§ 3. 1. Nadzór nad wdrożeniem, utrzymaniem i doskonaleniem PBI sprawuje Dyrektor Generalny Ministerstwa.

2. Za operacyjne zarządzanie bezpieczeństwem informacji, w tym koordynację działań i monitorowanie ich zgodności z PBI, odpowiada Pełnomocnik.

3. Kierownicy komórek organizacyjnych Ministerstwa zapewniają stosowanie PBI w podległych im komórkach.

4. Incydenty bezpieczeństwa informacji zgłasza się na zasadach określonych w PBI.

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

Minister Energii: *Miłosz Motyka*

¹⁾ Minister Energii kieruje działami administracji rządowej – energia i gospodarka surowcami energetycznymi, na podstawie § 1 ust. 2 rozporządzenia Prezesa Rady Ministrów z dnia 25 lipca 2025 r. w sprawie szczegółowego zakresu działania Ministra Energii (Dz. U. poz. 1206).

Załącznik do zarządzenia Ministra Energii z dnia
7 października 2026 r. (Dz. Urz. Min. Ener. poz. 28)



**Ministerstwo
Energii**

POLITYKA BEZPIECZEŃSTWA INFORMACJI MINISTERSTWA ENERGII

§ 1. Cel i zakres Polityki

1. Celem Polityki Bezpieczeństwa Informacji Ministerstwa Energii, zwanej dalej „PBI”, jest zapewnienie poufności, integralności i dostępności informacji przetwarzanych w Ministerstwie Energii, zwanym dalej „Ministerstwem”.
2. PBI ma zastosowanie do wszystkich aktywów, informacji, systemów teleinformatycznych, lokalizacji, procesów, usług oraz osób związanych z przetwarzaniem informacji. PBI nie ma zastosowania do informacji niejawnych w rozumieniu ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2025 r. poz. 1209).
3. PBI określa zasady i sposób wdrażania zabezpieczeń fizycznych, technicznych i organizacyjnych, ograniczających zidentyfikowane zagrożenia bezpieczeństwa informacji.
4. Ministerstwo zapewnia zgodność działań w zakresie bezpieczeństwa informacji z przepisami prawa powszechnie obowiązującego oraz postanowieniami umownymi, mającymi zastosowanie do działalności Ministerstwa, w szczególności w zakresie bezpieczeństwa informacji, ochrony danych osobowych, cyberbezpieczeństwa oraz informatyzacji działalności podmiotów realizujących zadania publiczne.
5. Szczegółowe zasady funkcjonowania Systemu Zarządzania Bezpieczeństwem Informacji, zwanego dalej „SZBI”, opracowuje się i doskonali przez tworzenie polityk, procedur, instrukcji, metodyk, regulaminów oraz innych dokumentów, które uszczegóławiają zasady określone w PBI.
6. Dokumenty, o których mowa w ust. 5, są zgodne z zasadami zawartymi w niniejszym dokumencie.

§ 2. Definicje

Na potrzeby PBI przyjmuje się następujące określenia:

- 1) **aktywo** – wszystko, co posiada wartość dla Ministerstwa, w szczególności informacje, systemy teleinformatyczne, infrastruktura, budynki stanowiące siedzibę Ministerstwa, struktura organizacyjna Ministerstwa, sprzęt, oprogramowanie, usługi oraz zasoby ludzkie;
- 2) **autentyczność** – właściwość zapewniająca, że pochodzenie informacji, jej źródło lub nadawca są takie, jak deklarowane, a informacja może być jednoznacznie powiązana z tym źródłem;
- 3) **bezpieczeństwo informacji** – zachowanie poufności, integralności i dostępności informacji zgodnie z zasadami określonymi w niniejszej PBI i politykach tematycznych;
- 4) **dostępność** – właściwość zapewniająca, że osoby upoważnione mają dostęp do informacji i związanych z nimi aktywów w przypadku, gdy jest to potrzebne;
- 5) **incydent bezpieczeństwa informacji** – zdarzenie lub seria zdarzeń związanych z bezpieczeństwem informacji, które powodują lub mogą powodować naruszenie poufności, integralności lub dostępności informacji;
- 6) **informacja** – dane posiadające znaczenie i wartość dla Ministerstwa, niezależnie od formy ich utrwalenia lub przekazu;
- 7) **integralność** – właściwość zapewniająca, że informacje nie zostały zmienione lub zniszczone w sposób nieuprawniony;
- 8) **kierownictwo Ministerstwa** – Minister Energii, sekretarz stanu, podsekretarz stanu, Dyrektor Generalny Ministerstwa oraz Szef Gabinetu Politycznego Ministra;
- 9) **nośnik informacji** – każdy fizyczny lub logiczny element, w tym plik, baza danych, urządzenie końcowe, na których informacje są zapisywane, przechowywane lub przetwarzane, niezależnie od formy, technologii i sposobu dostępu;
- 10) **opiekun aktywa** – osoba wspierająca właściciela aktywa w odniesieniu do jego utrzymania, konfiguracji lub nadzoru; opiekunem aktywa może być kierownik komórki organizacyjnej Ministerstwa, w której aktywo jest wykorzystywane, bądź wyznaczona przez niego osoba;
- 11) **osoba współpracująca** – osoba fizyczna niebędąca pracownikiem Ministerstwa, która na podstawie umowy cywilnoprawnej, porozumienia, delegowania, stażu, praktyk, wolontariatu lub innej formy współpracy, niezależnie od jej podstawy prawnej, wykonuje czynności na rzecz Ministerstwa oraz uzyskuje dostęp do informacji, systemów teleinformatycznych lub aktywów Ministerstwa;
- 12) **poufność** – właściwość zapewniająca, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom, procesom lub podmiotom;

- 13) **pracownik** – osoba zatrudniona w Ministerstwie w ramach stosunku pracy;
- 14) **rozliczalność** – właściwość zapewniająca, że działania dokonywane w związku z przetwarzaniem informacji są przypisane do konkretnej osoby, podmiotu lub procesu;
- 15) **ryzyko** – możliwość wystąpienia zagrożenia wykorzystującego podatność aktywa i powodującego negatywne skutki;
- 16) **system teleinformatyczny** – system teleinformatyczny w rozumieniu przepisów ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2026 r. poz. 20, 252, 815, 1003 i 1206);
- 17) **System Zarządzania Bezpieczeństwem Informacji (SZBI)** – zbiór zasad, procesów, ról i środków organizacyjnych oraz technicznych służących systematycznemu zarządzaniu ryzykiem bezpieczeństwa informacji i ochronie informacji w Ministerstwie;
- 18) **właściciel aktywa** – pracownik Ministerstwa bądź osoba współpracująca, odpowiedzialna za dane aktywo i poziom jego ochrony;
- 19) **zagrożenie** – potencjalna przyczyna niepożądanego incydentu, który może spowodować szkodę dla systemu, informacji lub instytucji;
- 20) **złośliwe oprogramowanie** – oprogramowanie lub kod, którego celem jest nieuprawnione działanie mogące naruszyć bezpieczeństwo informacji lub ciągłość działania organizacji.

§ 3. Oświadczenie kierownictwa Ministerstwa

1. Kierownictwo Ministerstwa deklaruje pełne zaangażowanie w zapewnienie bezpieczeństwa informacji oraz ciągłe doskonalenie SZBI. Kierownictwo Ministerstwa zobowiązuje się do zapewnienia zasobów niezbędnych do skutecznego funkcjonowania i rozwoju SZBI.
2. Bezpieczeństwo informacji stanowi integralny element realizacji zadań publicznych Ministerstwa oraz zapewnia zgodność z obowiązującymi przepisami prawa oraz, w zakresie przyjętym przez Ministerstwo, normami i standardami bezpieczeństwa, a także buduje świadomość i odpowiedzialność pracowników, a także współpracowników w zakresie bezpieczeństwa informacji.

§ 4. Ogólne zasady bezpieczeństwa informacji

1. SZBI zapewnia w szczególności poufność, integralność i dostępność informacji.
2. Informacje są chronione adekwatnie do ich wartości, znaczenia i poziomu ryzyka.
3. Pracownicy, osoby współpracujące oraz podmioty zewnętrzne realizujące zadania na rzecz Ministerstwa ponoszą odpowiedzialność za bezpieczne przetwarzanie informacji.
4. Dostęp do informacji jest przyznawany w zakresie niezbędnym do realizacji powierzonych obowiązków, zgodnie z zasadą minimalnych uprawnień.
5. Minimalny wymagany poziom bezpieczeństwa informacji określają obowiązujące przepisy prawa.
6. Informacje, dokumenty oraz nośniki informacji nie są pozostawiane bez nadzoru w miejscach dostępnych dla osób nieupoważnionych. Stanowiska pracy zabezpiecza się każdorazowo w przypadku pozostawienia ich bez nadzoru przez osoby, o których mowa w ust. 3.
7. Bezpieczeństwo informacji uwzględnia się na etapie projektowania, wdrażania, realizacji oraz doskonalenia procesów, systemów, usług oraz rozwiązań organizacyjnych, z uwzględnieniem analizy ryzyka, klasyfikacji informacji oraz obowiązujących wymagań prawnych i regulacyjnych.
8. W szczególnie uzasadnionych przypadkach dopuszcza się odstępstwo od wybranych postanowień PBI, jeżeli odstępstwo to nie narusza przepisów powszechnie obowiązującego prawa oraz nie powoduje nieakceptowalnego poziomu ryzyka dla bezpieczeństwa informacji. Odstępstwo wymaga udokumentowania, przeprowadzenia analizy ryzyka oraz zatwierdzenia przez Ministra Energii, upoważnionego przez niego członka kierownictwa Ministerstwa albo Dyrektora Generalnego Ministerstwa, po uzyskaniu pisemnej opinii Pełnomocnika do spraw bezpieczeństwa informacji.
9. W procesach krytycznych oraz przy zarządzaniu systemami teleinformatycznymi stosuje się zasadę podziału obowiązków, tak aby ta sama osoba nie posiadała uprawnień umożliwiających jednocześnie wykonanie i zatwierdzenie operacji wrażliwej.

§ 5. Klasyfikacja informacji

1. W Ministerstwie stosuje się klasyfikację informacji określoną w niniejszej PBI z uwzględnieniem przepisów prawa powszechnie obowiązującego oraz wewnętrznych regulacji dotyczących ochrony informacji.
2. Informacje klasyfikuje się na następujące kategorie:
 - 1) publiczne;
 - 2) do użytku wewnętrznego;
 - 3) chronione na podstawie przepisów szczególnych.
3. Za dokonanie klasyfikacji informacji oraz jej aktualizację odpowiada właściciel aktywa.
4. W przypadku braku wyraźnego sklasyfikowania informacji, przyjmuje się, że stanowi ona informację „do użytku wewnętrznego”.

§ 6. Aktywa i inwentaryzacja

1. Wszystkie aktywa wykorzystywane w Ministerstwie podlegają identyfikacji, inwentaryzacji oraz ochronie w zakresie adekwatnym do ich znaczenia dla realizowanych zadań.
2. Każdemu aktywowi przypisuje się właściciela odpowiedzialnego za zapewnienie jego właściwej ochrony, w tym za określenie wymagań bezpieczeństwa oraz nadzór nad ich stosowaniem.
3. Aktywa stanowiące własność Ministerstwa lub wykorzystywane w jego imieniu podlegają ewidencji oraz są przypisane do osoby lub komórki organizacyjnej Ministerstwa odpowiedzialnej za ich użytkowanie.
4. Aktywa podlegają zwrotowi, dezaktywacji, bezpiecznemu usunięciu danych lub fizycznej utylizacji w przypadku zakończenia współpracy, zmiany zakresu obowiązków, poziomu uprawnień albo wycofania zasobu z eksploatacji.

§ 7. Kontrola dostępu

1. Dostęp fizyczny do obiektów i pomieszczeń, w których są przetwarzane informacje, jest ograniczony i kontrolowany.
2. Dostęp logiczny do systemów teleinformatycznych oraz do nośników informacji jest realizowany na podstawie indywidualnych uprawnień, które są niezwłocznie nadawane, modyfikowane i odbierane zgodnie z obowiązującymi procedurami, stosownie do zakresu obowiązków użytkownika oraz zasady minimalnych uprawnień.
3. Dostęp uprzywilejowany jest przyznawany wyłącznie w uzasadnionych przypadkach, w minimalnym niezbędnym zakresie i na określony czas, z zapewnieniem odpowiednich mechanizmów kontroli, monitorowania i rozliczalności.
4. Uprawnienia dostępu podlegają okresowym przeglądom realizowanym przez właścicieli aktywów, zgodnie z obowiązującymi procedurami, nie rzadziej niż raz w roku, w celu zweryfikowania ich aktualności i zasadności.

§ 8. Obsługa nośników informacji

1. Nośniki informacji podlegają ochronie przed nieuprawnionym dostępem, utratą i zniszczeniem, zgodnie z przeznaczeniem i kategorią informacji.
2. Korzystanie z nośników informacji odbywa się wyłącznie w celach służbowych oraz zgodnie z obowiązującymi procedurami.
3. Wnoszenie nośników informacji, w których są przetwarzane informacje, poza lokalizację Ministerstwa, w tym poza miejsca wykonywania pracy zdalnej, dopuszcza się wyłącznie w przypadkach uzasadnionych potrzebami służbowymi, pod warunkiem zastosowania adekwatnych zabezpieczeń technicznych, w szczególności szyfrowania całej zawartości nośnika lub poszczególnych zbiorów danych.
4. Usuwanie danych z nośników oraz niszczenie nośników odbywa się w sposób uniemożliwiający odtworzenie informacji.

5. Utrata, kradzież lub nieuprawnione użycie nośnika informacji podlega niezwłocznemu zgłoszeniu, zgodnie z procedurą obsługi i zgłaszania incydentów bezpieczeństwa informacji.
6. Zabrania się podłączania do systemów teleinformatycznych Ministerstwa prywatnych nośników informacji oraz wykorzystywania nośników służbowych do celów prywatnych, chyba że procedury szczegółowe stanowią inaczej.

§ 9. Bezpieczeństwo fizyczne i środowiskowe

1. Dostęp do obiektów, budynków i pomieszczeń Ministerstwa jest ograniczony i kontrolowany w sposób zapewniający ochronę informacji oraz zasobów teleinformatycznych przed dostępem osób nieuprawnionych.
2. Obszary o istotnym znaczeniu dla bezpieczeństwa informacji lub podwyższonym poziomie ryzyka są objęte kontrolą dostępu oraz monitoringiem w uzasadnionym zakresie, adekwatnym do celu ochrony.
3. Środki kontroli dostępu oraz monitoringu są stosowane z poszanowaniem obowiązujących przepisów prawa, w szczególności w zakresie ochrony danych osobowych i prywatności.
4. Zapisy z systemów monitoringu są chronione przed nieuprawnionym dostępem, modyfikacją i usunięciem oraz przechowywane zgodnie z przepisami prawa.
5. Ministerstwo zapewnia stosowanie odpowiednich zabezpieczeń fizycznych i środowiskowych, w tym w zakresie ochrony przeciwpożarowej oraz zasilania awaryjnego w odniesieniu do infrastruktury przetwarzania informacji.
6. Szczegółowe zasady kontroli dostępu, monitoringu, ochrony fizycznej oraz zabezpieczeń środowiskowych określają odrębne procedury i regulaminy obowiązujące w poszczególnych lokalizacjach Ministerstwa.
7. Osoby postronne, w tym goście, serwisanci, kurierzy, mogą przebywać w strefach ograniczonego dostępu wyłącznie pod nadzorem upoważnionego pracownika Ministerstwa lub po spełnieniu wymogów określonych w instrukcjach ochrony obiektów.
8. Miejsca dostaw, załadunku oraz inne punkty, przez które osoby nieuprawnione mogą uzyskać dostęp do obiektu, są odizolowane od pomieszczeń przetwarzania informacji i podlegają szczególnej kontroli.

§ 10. Zarządzanie ryzykiem bezpieczeństwa informacji

1. Ministerstwo stosuje podejście oparte na ryzyku.
2. Ryzyko bezpieczeństwa informacji jest identyfikowane, analizowane i oceniane zgodnie z Procedurą zarządzania ryzykiem w bezpieczeństwie informacji Ministerstwa.
3. Ocena ryzyka jest prowadzona cyklicznie, nierzadziej niż raz w roku lub doraźnie w przypadku wprowadzenia istotnych zmian organizacyjnych lub technologicznych w Ministerstwie, a także w przypadku zaobserwowania zagrożenia dla Ministerstwa, którego wystąpienie jest przewidywane w krótkim czasie lub którego skutki mogą mieć istotne znaczenie dla bezpieczeństwa informacji.
4. Na podstawie przeprowadzanej oceny ryzyka jest sporządzany plan postępowania z ryzykiem.
5. Ocena ryzyka stanowi podstawę podejmowania wszelkich działań w zakresie utrzymania i doskonalenia SZBI.
6. Poziom ryzyka pozostający po wdrożeniu planu postępowania z ryzykiem (ryzyko szczątkowe) podlega formalnej akceptacji przez Ministra Energii lub wyznaczonego przez niego członka kierownictwa Ministerstwa.

§ 11. Role i odpowiedzialności

W skład struktury organizacyjnej bezpieczeństwa informacji w Ministerstwie wchodzi w szczególności:

- 1) **Dyrektor Generalny Ministerstwa** – zapewnia funkcjonowanie SZBI, zasoby niezbędne do jego funkcjonowania, przeprowadzenie przeglądów SZBI oraz egzekwowanie odpowiedzialności za naruszenia bezpieczeństwa informacji; Dyrektor Generalny Ministerstwa powołuje Pełnomocnika do spraw bezpieczeństwa informacji i jego zastępcę;
- 2) **Pełnomocnik do spraw bezpieczeństwa informacji oraz jego zastępca** – nadzorują realizację PBI, koordynują i nadzorują prowadzenie rejestru aktywów informacyjnych Ministerstwa, rejestru ryzyk bezpieczeństwa informacji, rejestru incydentów bezpieczeństwa informacji, a także koordynują proces zarządzania ryzykiem w skali Ministerstwa oraz przeglądy zarządzania SZBI, wykonując zadania w zakresie oceny funkcjonowania SZBI w sposób zapewniający niezależność i obiektywizm;

- 3) **Inspektor Ochrony Danych** – monitoruje przestrzeganie przepisów oraz wewnętrznych regulacji w zakresie ochrony danych osobowych, zgodnie z Polityką Ochrony Danych Osobowych, a także uczestniczy w procesie oceny ryzyka w tym obszarze, w szczególności przez udzielanie zaleceń i monitorowanie prawidłowości jej przeprowadzania;
- 4) **Administrator bezpieczeństwa teleinformatycznego i jego zastępca** – odpowiadają za koordynację zadań w zakresie zarządzania bezpieczeństwem systemów teleinformatycznych, w tym ocenę ryzyka teleinformatycznego zgodnie z Polityką Bezpieczeństwa Teleinformatycznego, zwaną dalej „PBT”;
- 5) **administratorzy bezpieczeństwa fizycznego** – odpowiadają za koordynację zadań w zakresie bezpieczeństwa fizycznego, w tym ochronę obiektów i poszczególnych pomieszczeń, a także ocenę ryzyka w tym obszarze;
- 6) **dyrektorzy komórek organizacyjnych Ministerstwa** – odpowiadają za bezpieczeństwo informacji w podległych obszarach przez identyfikację aktywów oraz wdrożenie i przestrzeganie PBI w kierowanych przez siebie komórkach organizacyjnych Ministerstwa; dyrektor komórki organizacyjnej Ministerstwa może wyznaczyć koordynatora bezpieczeństwa informacji w tej komórce;
- 7) **właściciele aktywów** – odpowiadają za ochronę powierzonych informacji i przypisanych aktywów.

§ 12. Zgłaszanie incydentów

1. Każda osoba posiadająca dostęp do informacji lub systemów wykorzystywanych w Ministerstwie jest obowiązana do niezwłocznego zgłaszania incydentów bezpieczeństwa informacji oraz zdarzeń mogących mieć wpływ na ich bezpieczeństwo.
2. Incydenty bezpieczeństwa informacji są rejestrowane, analizowane oraz obsługiwane w sposób zapewniający możliwość oceny ich skutków oraz zapobiegania ich ponownemu wystąpieniu.
3. Na podstawie analizy incydentów są podejmowane działania korygujące lub zapobiegawcze, adekwatne do charakteru i skali incydentu.
4. Ministerstwo zapewnia realizację obowiązków sprawozdawczych wobec właściwych organów nadzorczych oraz zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) w terminach i na zasadach określonych w przepisach prawa.
5. Osoba zgłaszająca incydent jest obowiązana, w miarę swoich możliwości, do podjęcia działań mających na celu zachowanie informacji związanych z jego wystąpieniem, w szczególności przez niezwłoczne zgłoszenie incydentu, nieusuwanie danych oraz powstrzymanie się od samodzielnych prób jego usunięcia, które mogłyby utrudnić analizę przyczyn zdarzenia.

§ 13. Złośliwe oprogramowanie

1. Ministerstwo identyfikuje złośliwe oprogramowanie jako zagrożenie dla bezpieczeństwa informacji.
2. Ministerstwo stosuje odpowiednie środki w celu zapobiegania, wykrywania oraz reagowania na zagrożenia związane ze złośliwym oprogramowaniem, w tym techniczne i organizacyjne środki ochrony poczty elektronicznej, obejmujące w szczególności mechanizmy filtracji, oceny reputacji nadawców, wykrywania phishingu oraz ochrony integralności wiadomości.
3. Wszystkie systemy operacyjne oraz oprogramowanie wykorzystywane w Ministerstwie podlegają regularnym aktualizacjom bezpieczeństwa w celu eliminacji podatności wykorzystywanych przez złośliwe oprogramowanie.
4. Zabrania się instalowania i używania nieautoryzowanego oprogramowania oraz otwierania plików lub załączników pochodzących z nieznanych lub niezweryfikowanych źródeł.
5. Podejrzenia lub incydenty związane ze złośliwym oprogramowaniem podlegają zgłaszaniu i obsłudze zgodnie z procedurą zgłaszania i obsługi incydentów bezpieczeństwa informacji.

§ 14. Bezpieczeństwo zasobów ludzkich

1. W Ministerstwie, w zakresie dopuszczalnym przepisami prawa, przeprowadza się weryfikację kandydatów do pracy w zakresie dostosowanym do charakteru stanowiska oraz zakresu dostępu do informacji, zgodnie z obowiązującymi przepisami prawa oraz wewnętrznymi procedurami Ministerstwa.
2. Przed dopuszczeniem do informacji pracownicy oraz inne osoby uzyskujące dostęp do informacji Ministerstwa składają oświadczenia o zapoznaniu się z PBI oraz politykami tematycznymi i zobowiązują się do ich przestrzegania.

3. Dostęp, szkolenia stanowiskowe i przypisanie aktywów realizuje się na podstawie zgłoszeń uprawnień i rejestru aktywów, zgodnie z zasadą minimalnych uprawnień.
4. W przypadku zakończenia współpracy lub zmiany roli niezwłocznie odbiera się uprawnienia oraz rozlicza i przyjmuje zwrot aktywów.
5. Obowiązek zachowania poufności informacji chronionych obowiązuje również po ustaniu stosunku pracy lub zakończeniu współpracy, zgodnie z odrębnymi przepisami i podpisanymi zobowiązaniami.
6. Naruszenie zasad określonych w PBI może stanowić podstawę do pociągnięcia do odpowiedzialności dyscyplinarnej lub porządkowej, zgodnie z Kodeksem pracy lub właściwymi przepisami regulującymi odpowiedzialność dyscyplinarną osób zatrudnionych w administracji publicznej.

§ 15. Podnoszenie świadomości

1. Pracownicy Ministerstwa podlegają cyklicznym szkoleniom z zakresu bezpieczeństwa informacji.
2. Pełnomocnik do spraw bezpieczeństwa informacji zapewnia pracownikom Ministerstwa cykliczne szkolenia wewnętrzne w zakresie bezpieczeństwa informacji, we współpracy z komórką właściwą do spraw kadr i szkoleń.
3. Pracownicy Ministerstwa oraz osoby współpracujące, przed dopuszczeniem do informacji lub systemów teleinformatycznych, są szkoleni z zakresu bezpieczeństwa informacji w ramach szkoleń adaptacyjnych przez Pełnomocnika do spraw bezpieczeństwa informacji, jego zastępcę lub inną wyznaczoną przez niego osobę, we współpracy z komórką właściwą do spraw kadr i szkoleń.
4. Inne osoby przed dopuszczeniem do informacji lub systemów teleinformatycznych są szkolone z zakresu bezpieczeństwa informacji przez Pełnomocnika do spraw bezpieczeństwa informacji, jego zastępcę lub inną wyznaczoną przez niego osobę we współpracy z komórką właściwą do spraw kadr i szkoleń.

§ 16. Polityka Cyberhigieny

Wszyscy użytkownicy systemów teleinformatycznych Ministerstwa są obowiązani do stosowania zasad cyberhigieny, obejmujących co najmniej:

- 1) stosowanie aktualnych wersji oprogramowania oraz umożliwianie niezwłocznej instalacji poprawek bezpieczeństwa oraz stosowanie się do komunikatów systemowych dotyczących aktualizacji oprogramowania;
- 2) stosowanie unikalnych, silnych haseł oraz, w przypadkach wymaganych, uwierzytelniania wieloskładnikowego;
- 3) korzystanie wyłącznie z oprogramowania pozyskanego z autoryzowanych źródeł;
- 4) blokowanie stanowiska pracy podczas każdej nieobecności;
- 5) zachowanie ostrożności przy otwieraniu wiadomości e-mail, załączników i odnośników, szczególnie tych pochodzących od nieznanego nadawcy;
- 6) stosowanie zasad czystego biurka i czystego ekranu;
- 7) szyfrowanie nośników i urządzeń mobilnych, w szczególności przy ich wynoszeniu poza teren Ministerstwa;
- 8) korzystanie wyłącznie z zaufanych połączeń sieciowych oraz obowiązkowe stosowanie kanału VPN przy dostępie zdalnym do zasobów Ministerstwa.

§ 17. Zarządzanie błędami ludzkimi

1. Ministerstwo wdraża środki techniczne i organizacyjne minimalizujące ryzyko błędów ludzkich, w szczególności:
 - 1) systemy podpowiedzi i walidacji danych;
 - 2) dwuosobową kontrolę (zasadę „czterech oczu”) w procesach o podwyższonym ryzyku;
 - 3) ograniczenie uprawnień użytkowników do niezbędnego minimum;
 - 4) cykliczne szkolenia, o których mowa w § 15, oraz testy wiedzy.
2. Błędy ludzkie istotne pod kątem bezpieczeństwa informacji podlegają rejestrowaniu i analizie, zgodnie z § 12.
3. Środki minimalizujące błędy ludzkie są uwzględniane przy projektowaniu i modyfikacji procesów oraz systemów teleinformatycznych.

4. Analiza błędów ludzkich koncentruje się na identyfikacji ich przyczyn systemowych i organizacyjnych. W Ministerstwie jest promowana kultura otwartości i stabilności, co oznacza, że eliminowanie błędów ludzkich opiera się na analizie incydentów oraz wyciąganiu wniosków służących doskonaleniu procesów. Jeżeli stwierdzono, że incydent został spowodowany rażącym niedbalstwem lub działaniem umyślnym, mogą zostać zastosowane środki przewidziane przepisami prawa.

§ 18. Nadzór nad dokumentacją i brakowanie

1. Ministerstwo opracowuje, stosuje, aktualizuje oraz utrzymuje dokumentację dotyczącą bezpieczeństwa informacji, zgodnie z przepisami prawa oraz wymaganiami określonymi w dokumentacji SZBI.
2. Ministerstwo ustanawia nadzór nad dokumentacją, obejmujący co najmniej:
 - 1) zapewnienie dostępu do dokumentów wyłącznie osobom upoważnionym;
 - 2) ochronę dokumentacji przed uszkodzeniem, utratą, nieuprawnionym dostępem, modyfikacją lub niewłaściwym użyciem;
 - 3) oznaczanie wersji dokumentów oraz prowadzenie rejestru zmian;
 - 4) przechowywanie dokumentacji w sposób zapewniający jej integralność i dostępność.
3. Dokumentacja dotycząca bezpieczeństwa systemu teleinformatycznego jest przechowywana przez okres co najmniej 2 lat od dnia jej wycofania z użytkowania lub od dnia zakończenia świadczenia usługi, której dotyczy, chyba że przepisy odrębne, w tym przepisy archiwalne i Jednolity Rzeczowy Wykaz Akt, przewidują dłuższy okres przechowywania.
4. Zniszczenie wycofanej dokumentacji dotyczącej bezpieczeństwa informacji następuje zgodnie z obowiązującymi w Ministerstwie przepisami kancelaryjno-archiwalnymi na podstawie protokołu brakowania, który zawiera co najmniej:
 - 1) datę sporządzenia protokołu;
 - 2) wykaz dokumentacji przeznaczonej do zniszczenia;
 - 3) opis sposobu zniszczenia;
 - 4) dane osoby zatwierdzającej protokół.
5. Protokoły brakowania są przechowywane w sposób trwały i stanowią element dokumentacji operacyjnej SZBI.
6. Pełnomocnik do spraw bezpieczeństwa informacji nadzoruje realizację obowiązków, o których mowa w niniejszym paragrafie.

§ 19. Monitoring i audyty wewnętrzne

1. Skuteczność wdrożonych zasad zapewniających bezpieczeństwo informacji jest kluczowym elementem Systemu Zarządzania Bezpieczeństwem Informacji.
2. Co najmniej raz na 12 miesięcy przeprowadza się przegląd funkcjonowania SZBI, w ramach którego są analizowane wyniki audytów SZBI, skuteczność zastosowanych zabezpieczeń, wyniki ocen ryzyka i status planów postępowania z ryzykiem, zarządzanie incydentami bezpieczeństwa informacji, rekomendacje Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa, stan realizacji działań poaudytowych z poprzednich okresów oraz zmiany prawne, a także inne zdarzenia mające wpływ na bezpieczeństwo informacji.
3. Wyniki przeglądu są dokumentowane w raporcie przekazywanym Dyrektorowi Generalnemu Ministerstwa.
4. Audyt wewnętrzny bezpieczeństwa informacji służy potwierdzeniu zgodności SZBI Ministerstwa z wymaganiami prawnymi dotyczącymi bezpieczeństwa informacji. Jest mechanizmem niezależnej oceny, a także weryfikacji poziomu świadomości i kompetencji pracowników.
5. Audyt bezpieczeństwa informacji jest procesem systematycznym, cyklicznie realizowanym, który jest przeprowadzany nierzadziej niż raz w roku przez komórkę właściwą do spraw audytu wewnętrznego lub komórkę właściwą do spraw kontroli, we współpracy z komórką właściwą do spraw informatyki lub przez podmiot zewnętrzny, z zapewnieniem obiektywizmu i bezstronności procesu audytu.

6. Na podstawie wyników audytów oraz przeglądu zarządzania, Dyrektor Generalny Ministerstwa wyznacza właściwe komórki organizacyjne Ministerstwa do wdrożenia działań korygujących, które są realizowane w terminach uzgodnionych z Pełnomocnikiem do spraw bezpieczeństwa informacji.

§ 20. Wskaźniki

1. Ministerstwo monitoruje i mierzy skuteczność SZBI za pomocą wskaźników.
2. Pełnomocnik do spraw bezpieczeństwa informacji w porozumieniu z dyrektorami właściwych komórek organizacyjnych Ministerstwa określa, co, w jaki sposób i w jakich odstępach czasu podlega monitorowaniu i mierzeniu.
3. Wyniki monitorowania wskaźników stanowią podstawę do doskonalenia SZBI oraz są wykorzystywane w procesie przeglądu funkcjonowania SZBI, o którym mowa w § 19.
4. Wyniki monitorowania wskaźników są raportowane Dyrektorowi Generalnemu Ministerstwa przez Pełnomocnika do spraw bezpieczeństwa informacji lub jego zastępcę.
5. Wskaźniki obejmują w szczególności ocenę skuteczności wdrożonych zabezpieczeń, poziom świadomości użytkowników oraz terminowość obsługi incydentów i podatności.

§ 21. Zasady udostępniania informacji

Informacje zawarte w dokumentacji SZBI, jeżeli stanowią informację publiczną, udostępnia się na zasadach i w trybie określonych w przepisach o dostępie do informacji publicznej, z uwzględnieniem ograniczeń wynikających z przepisów prawa.

§ 22. Postanowienia końcowe

1. Pracownicy są obowiązani do zapoznania się z treścią PBI w terminie miesiąca od dnia jej wejścia w życie albo od dnia rozpoczęcia pracy w Ministerstwie.
2. Z treścią poszczególnych polityk tematycznych są obowiązani zapoznać się pracownicy, których zakres obowiązków, posiadane uprawnienia lub wykonywane zadania są objęte zakresem stosowania danego dokumentu. Zapoznanie się z tymi dokumentami następuje w terminie miesiąca od dnia ich wejścia w życie albo od dnia objęcia pracownika zakresem stosowania danej polityki.
3. Zapoznanie się z dokumentami, o których mowa w ust. 1 i 2, potwierdza się w EZD przez złożenie oświadczenia.
4. Osoby współpracujące zapoznają się z PBI przed rozpoczęciem współpracy oraz zobowiązują się do przestrzegania PBI w formie pisemnego oświadczenia lub stosownych postanowień w umowie lub porozumieniu.
5. W przypadku gdy udostępnienie dokumentów, o których mowa w ust. 1 i 2, lub potwierdzenie zapoznania się z nimi za pośrednictwem EZD jest niemożliwe albo istotnie utrudnione z przyczyn technicznych lub organizacyjnych, w szczególności z powodu niedostępności systemu, braku dostępu pracownika do EZD albo nieutworzenia konta użytkownika, Pełnomocnik do spraw bezpieczeństwa informacji może określić alternatywny sposób udostępnienia dokumentów i potwierdzenia zapoznania się z ich treścią.
6. Alternatywny sposób potwierdzenia zapoznania się z dokumentami, o których mowa w ust. 1 i 2, może w szczególności polegać na złożeniu oświadczenia w postaci papierowej lub elektronicznej albo podpisaniu listy potwierdzającej zapoznanie się z dokumentami w ramach szkolenia lub instruktażu.
7. W przypadku istotnej zmiany PBI, PBT lub polityki tematycznej akt zmieniający dany dokument określa obowiązek ponownego zapoznania się z jego treścią.
8. Wzór oświadczenia o zapoznaniu się z PBI i politykami tematycznymi stanowi załącznik do PBI.

Załącznik do Polityki Bezpieczeństwa
Informacji Ministerstwa Energii

WZÓR OŚWIADCZENIA O ZAPOZNANIU SIĘ Z POLITYKĄ BEZPIECZEŃSTWA INFORMACJI I POLITYKAMI TEMATYCZNYMI

1. Część A – Klauzula dla pracowników / współpracowników

Ja, niżej podpisany/a, oświadczam, że:

1. Zapoznałem/am się z Polityką Bezpieczeństwa Informacji obowiązującą w Ministerstwie Energii oraz z zasadami bezpieczeństwa teleinformatycznego i ochrony informacji w niej określonymi.
2. Zapoznałem/am się z politykami tematycznymi, procedurami i innymi dokumentami z zakresu bezpieczeństwa informacji, które mają zastosowanie do wykonywanych przeze mnie obowiązków, posiadanych uprawnień oraz zakresu dostępu do informacji i systemów teleinformatycznych Ministerstwa Energii.
3. Zapoznałem/am się z postanowieniami Polityki Bezpieczeństwa Teleinformatycznego, mającymi zastosowanie do wykonywanych przeze mnie obowiązków, oraz zobowiązuję się do ich przestrzegania.
4. Zobowiązuję się stosować zasady i wymagania określone w dokumentach wskazanych powyżej oraz niezwłocznie zgłaszać wszelkie incydenty, naruszenia lub podejrzenia naruszeń bezpieczeństwa informacji.
5. Przyjmuję do wiadomości, że naruszenie obowiązujących zasad może skutkować odpowiedzialnością przewidzianą przez przepisy prawa.

Imię i nazwisko: _____

Stanowisko / rola: _____

Data: _____

Podpis: _____

2. Część B – Klauzula dla wykonawców / przedstawicieli firm zewnętrznych

Ja, niżej podpisany/a, działając w imieniu własnym lub reprezentując firmę zewnętrzną wykonującą usługi na rzecz Ministerstwa Energii, oświadczam, że:

1. Zapoznałem/am się z Polityką Bezpieczeństwa Informacji, politykami tematycznymi oraz zasadami bezpieczeństwa teleinformatycznego obowiązującymi w Ministerstwie Energii w zakresie mającym zastosowanie do wykonywanych przeze mnie czynności i przyznanych mi uprawnień.
2. Zapoznałem/am się z Polityką Bezpieczeństwa Teleinformatycznego w zakresie mającym zastosowanie do wykonywanych przeze mnie czynności na rzecz Ministerstwa Energii oraz zobowiązuję się do jej przestrzegania i stosowania odpowiednich procedur podczas realizacji usług, prac serwisowych, zadań wdrożeniowych lub innych czynności wykonywanych na rzecz Ministerstwa.
3. Zobowiązuję się do zachowania poufności wszystkich informacji uzyskanych w trakcie realizacji prac oraz wykorzystywania ich wyłącznie w celu wykonania umowy.
4. Zobowiązuję się stosować wszystkie środki bezpieczeństwa wymagane przez Ministerstwo Energii, w tym procedury dostępu do systemów, pomieszczeń technicznych oraz danych.
5. Zobowiązuję się niezwłocznie zgłaszać wszelkie incydenty lub podejrzenia naruszeń bezpieczeństwa, zgodnie z obowiązującymi procedurami.
6. Przyjmuję do wiadomości, że naruszenie zasad bezpieczeństwa może skutkować konsekwencjami wynikającymi z umowy, w tym karami umownymi, zakończeniem współpracy lub odpowiedzialnością przewidzianą przepisami prawa.

Imię i nazwisko: _____

Nazwa firmy: _____

Zakres wykonywanych prac/usług: _____

Data: _____

Podpis: _____