Załącznik nr 1 do Zarządzenia nr 134/2023
Wojewody Łódzkiego z 5 lipca 2023 r.

POLITYKA BEZPIECZEŃSTWA INFORMACJI
DLA ŁÓDZKIEGO URZĘDU WOJEWÓDZKIEGO W ŁODZI

ROZDZIAŁ I POSTANOWIENIA OGÓLNE

§ 1. 1. Celem Polityki Bezpieczeństwa Informacji jest zapewnienie ochrony informacji przetwarzanych przez Łódzki Urząd Wojewódzki w Łodzi przed: udostępnieniem osobom nieupoważnionym, wejściem w posiadanie przez osobę nieuprawnioną, wykorzystywaniem z naruszeniem przepisów oraz przed niekontrolowaną zmianą, uszkodzeniem lub zniszczeniem.

2. Polityka Bezpieczeństwa Informacji określa reguły dotyczące procedur zapewnienia bezpieczeństwa danych w postaci papierowej oraz w systemach informatycznych Łódzkiego Urzędu Wojewódzkiego w Łodzi.

3. Polityka Bezpieczeństwa Informacji obowiązuje wszystkich pracowników Łódzkiego Urzędu Wojewódzkiego w Łodzi, stażystów, praktykantów oraz dostawców usług, podmioty współpracujące na zasadzie umów, z Łódzkim Urzędem Wojewódzkim w Łodzi.

4. Ochrona danych jest realizowana poprzez: zabezpieczenia fizyczne, procedury organizacyjne, sprzęt i oprogramowanie systemowe, aplikacje oraz użytkowników.

5. Polityka Bezpieczeństwa Informacji nie obejmuje przetwarzania informacji niejawnych w rozumieniu ustawy z 5 sierpnia 2010 r. o ochronie informacji niejawnych (t.j. Dz.U. z 2023 r. poz. 756).

ROZDZIAŁ II PODSTAWOWE DEFINICJE

§ 2. Ilekroć w Polityce Bezpieczeństwa Informacji jest mowa o:

1) Kierowniku Jednostki Organizacyjnej (KJO) - rozumie się przez to Wojewodę Łódzkiego;
2) Administratorze Systemu Informatycznego (ASI) - rozumie się przez to osobę nadzorującą pracę systemów informatycznych;
3) CSIRT.GOV.PL - rozumie się przez to Rządowy Zespół Reagowania na Incydenty Komputerowe powołany do reakcji na zdarzenia naruszające bezpieczeństwo w sieci Internet, przy pomocy którego właściwy minister ds. informatyzacji zapewnia koordynację i spójność działań podejmowanych w celu zapewnienia bezpieczeństwa Cyberprzestrzeni Rzeczpospolitej Polskiej;
4) DKBW – rozumie się przez to Delegaturę Krajowego Biura Wyborczego w Łodzi
5) EZD - rozumie się przez to system Elektronicznego Zarządzania Dokumentacją służący do przetwarzania dokumentów w wersji elektronicznej w sposób zgodny z instrukcją kancelaryjną oraz Regulaminem organizacyjnym Łódzkiego Urzędu Wojewódzkiego w Łodzi;

6) incydencie naruszenia danych - rozumie się przez to nieuprawniony dostęp do danych oraz nielegalne ujawnienie, pozyskanie, nieuprawnioną modyfikację lub zniszczenie;
7) incydencie komputerowym - rozumie się przez to niekorzystne zdarzenia w systemach teleinformatycznych lub zagrożenia wystąpienia takiego zdarzenia m.in. utratę poufności danych, zakłócenie danych lub integralności systemu, lub zakłócenie/odmowę dostępności, np. nieautoryzowane użycie konta innego użytkownika, nieautoryzowane użycie prawa dostępu oraz wprowadzanie złośliwych kodów, które niszczą informacje;
8) IZSI - rozumie się przez to Instrukcję Zarządzania Systemem Informatycznym dla Łódzkiego Urzędu Wojewódzkiego w Łodzi;
9) nośnikach danych - rozumie się przez to: dokumenty papierowe, nagrania głosu, obrazu lub innych sygnałów, wydruki, jednorazowe taśmy barwiące do maszyn/drukarek, taśmy magnetyczne, przenośne dyski, pendrive, dyskietki, nośniki optyczne, wydruki kodu programów, dane z testów, dokumentację (np. instrukcje i inne materiały drukowane), karty pamięci, mapy, itp.;
10) Pełnomocniku ds. Bezpieczeństwa Cyberprzestrzeni - rozumie się przez to osobę powołaną przez Wojewodę Łódzkiego, odpowiedzialną za realizację Polityki Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej dla Łódzkiego Urzędu Wojewódzkiego w Łodzi;
11) Pełnomocniku ds. Ochrony Informacji Niejawnych - rozumie się przez to osobę powołaną przez Wojewodę Łódzkiego, odpowiedzialną za realizację zadań z zakresu informacji niejawnych;
12) Polityce/ PBI - rozumie się przez to Politykę Bezpieczeństwa Informacji dla Łódzkiego Urzędu Wojewódzkiego w Łodzi;
13) poufności danych - rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;
14) systemie nadzoru telewizyjnego (CCTV) (tj. monitoringu) - rozumie się przez to instalację składającą się z sprzętowych i programowych elementów służącą do odbioru obrazu, jego rejestracji, odtwarzania lub przetwarzania w celu osiągnięcia określonej funkcjonalności;
15) systemie teleinformatycznym - rozumie się przez to należący do Łódzkiego Urzędu Wojewódzkiego w Łodzi zespół współpracujących ze sobą urządzeń informatycznych i oprogramowań zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnych urządzenia końcowego w rozumieniu przepisów ustawy - Prawo telekomunikacyjne;
16) Urzędzie/ŁUW - rozumie się przez to Łódzki Urząd Wojewódzki w Łodzi;

17) zarządzeniu - rozumie się przez to Zarządzenie Wojewody Łódzkiego w sprawie przyjęcia i wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji dla Łódzkiego Urzędu Wojewódzkiego w Łodzi.

ROZDZIAŁ III PODSTAWY PRAWNE

§ 3. Podstawy prawne oraz wytyczne i normy dotyczące bezpieczeństwa informacji:

1) ustawa z 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz.U. z 2023 r. poz. 57);
2) ustawa z 16 lipca 2004 r. - Prawo telekomunikacyjne (t.j. Dz.U. z 2022 r. poz. 1648);
3) rozporządzenie Rady Ministrów z 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2016 r. poz. 113 ze zm.);
4) wytyczne Agencji Bezpieczeństwa Wewnętrznego w zakresie zapewnienia bezpieczeństwa w systemach teleinformatycznych urzędów administracji publicznej;
5) Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej.

ROZDZIAŁ IV ORGANIZACJA BEZPIECZEŃSTWA INFORMACJI

§ 4. KJO realizując zadania z zakresu bezpieczeństwa informacji:

1) zapewnia środki techniczne i organizacyjne chroniące przetwarzanie danych oraz prowadzi dokumentację w tym zakresie;
2) może powołać ASI, jako odpowiedzialnego za ochronę systemu informatycznego (wg wzoru stanowiącego załącznik nr 1 do PBI) oraz określić zakres jego zadań;
3) powołuje:
   a) Pełnomocnika Wojewody ds. Bezpieczeństwa Cyberprzestrzeni, jako odpowiedzialnego za realizację Polityki Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej dla Łódzkiego Urzędu Wojewódzkiego w Łodzi oraz określa zakres jego zadań,
   b) Pełnomocnika Wojewody ds. Ochrony Informacji Niejawnych, jako odpowiedzialnego za realizację zadań z zakresu informacji niejawnych;
4) systematycznie unowocześnia stosowane na terenie Urzędu informatyczne, techniczne i organizacyjne środki bezpieczeństwa.

§ 5. Do zadań ASI należy w szczególności:

1) prowadzenie działań w celu zapewnienia ciągłości działania systemów informatycznych i prawidłowego przepływu danych pomiędzy poszczególnymi systemami;
2) współpraca z Inspektorem Ochrony Danych w zakresie bezpieczeństwa informacji oraz usuwania skutków i wyjaśnianiu przyczyn jego naruszenia;
3) podejmowanie natychmiastowych działań zabezpieczających w przypadku otrzymania informacji o naruszeniu zabezpieczeń systemu informatycznego lub informacji o zmianach w sposobie pracy elementów systemu informatycznego, wskazujących na incydent komputerowy;
4) aktualizowanie PBI i IZSI;
5) nadzorowanie wykonywania napraw, konserwacji oraz likwidacji urządzeń komputerowych;
6) nadzorowanie wykonywania kopii zapasowych, ich przetwarzania oraz okresowego sprawdzania, pod kątem ich przydatności w przypadku awarii systemu informatycznego;
7) nadzorowanie wszelkich prac związanych z ingerencją podmiotów zewnętrznych w systemy;
8) prowadzenie wykazu systemów informatycznych używanych w Urzędzie (według wzoru stanowiącego załącznik nr 2 do PBI) oraz dokonywanie jego aktualizacji.

§ 6. Do zadań Pełnomocnika Wojewody ds. Bezpieczeństwa Cyberprzestrzeni należy w szczególności:

1) opracowywanie i wdrażanie procedur reagowania na incydenty komputerowe, które będą obowiązywały w Urzędzie;
2) identyfikacja i prowadzenie cyklicznych analiz ryzyka bezpieczeństwa teleinformatycznego oraz przygotowanie rocznego sprawozdania właściwemu ministrowi ds. informatyzacji;
3) przygotowanie planów awaryjnych oraz ich testowanie;
4) opracowywanie procedur zapewniających informowanie właściwych zespołów CSIRT.GOV.PL o wystąpieniu incydentów komputerowych, zmianie lokalizacji jednostki organizacyjnej, danych kontaktowych, itp.;
5) przestrzeganie zasad określonych w Polityce Ochrony Cyberprzestrzeni, opracowanej przez właściwego ministra ds. informatyzacji;
6) przeprowadzanie szkoleń dla pracowników Urzędu w zakresie bezpieczeństwa informatycznego;
7) realizacja obowiązków wynikających z przepisów aktów prawnych właściwych dla zapewnienia bezpieczeństwa cyberprzestrzeni.

§ 7. Do zadań Pełnomocnika Wojewody ds. Ochrony Informacji Niejawnych należy w szczególności:

1) nadzór nad ochroną informacji niejawnych;
2) nadzór nad danymi zawartymi w oświadczeniach o stanie majątkowym;
3) współpraca z KJO i ASI w zakresie ich działań, dotyczących realizacji PBI.

§ 8. Za poprawne funkcjonowanie wydziału/ równorzędnej komórki organizacyjnej odpowiada Dyrektor. Do jego zadań należy w szczególności:

1) zapoznanie podległych pracowników z PBI, IZSI Urzędu oraz dbałość o przestrzeganie zawartych w nich zasad;
2) zorganizowanie komputerowego stanowiska pracy, zapewnienie bezpieczeństwa danych wykorzystywanych na stanowisku pracy oraz prawidłowej eksploatacji sprzętu komputerowego;
3) zapewnienie prawidłowego wykonywania wszystkich procedur bezpieczeństwa obszaru, za który jest odpowiedzialny;
4) wnioskowanie o nadanie uprawnień do systemu teleinformatycznego dla nowoprzyjętych lub przeniesionych z innej komórki organizacyjnej pracowników;
5) informowanie pracowników o osobach nieuprawnionych, przebywających na terenie wydziału, w związku z realizacją usług na rzecz Urzędu.

§ 9. 1. Pracownicy Urzędu są zobowiązani do:

1) zapoznania się z PBI i IZSI w Urzędzie oraz ich stosowania;
2) stosowania procedur mających na celu zgodne z prawem, a zwłaszcza adekwatne do potrzeb Urzędu przetwarzanie danych;
3) stosowania się do poleceń i wytycznych ASI;
4) odpowiedniego zabezpieczenia danych przed udostępnieniem osobom nieupoważnionym, w tym:
   a) przechowywania dokumentów papierowych i innych nośników informacji w meblach biurowych zamykanych na klucz (zasada „czystego biurka”),
   b) nieprzetwarzania danych w celach prywatnych,
   c) niepozostawiania pomieszczeń lub kluczy do pomieszczeń bez nadzoru,
   d) chronienia wydruków papierowych,
   e) niszczenia nośników danych w odpowiednich niszczarkach,
   f) chronienia ekranów komputerowych (ustawienie ma uniemożliwić podgląd);
5) eksploatacji systemu informatycznego, służącego do realizacji zadań, zgodnie z uregulowaniami wewnętrznymi ŁUW;
6) wykonywania pracy wyłącznie na urządzeniach będących własnością Urzędu lub użyczonych Urzędowi na podstawie odrębnych umów;
7) zachowania w tajemnicy danych oraz sposobów ich zabezpieczenia, zarówno w czasie trwania stosunku prawnego (umowa, staż, praktyka itp.), jak i po jego ustaniu;
8) zgłaszania przełożonym przypadków związanych z naruszeniem bezpieczeństwa danych oraz niewłaściwego funkcjonowania systemu teleinformatycznego;
9) w zakresie obsługi systemu EZD:
   a) korzystania z dostępu do danych wyłącznie w zakresie niezbędnym do wykonywania czynności służbowych i zgodnie z przyznanymi uprawnieniami,
   b) powiadomienia przełożonego o każdym przypadku nieuprawnionego dostępu do dokumentów.

2. Nieuzasadnione próby przekraczania swoich uprawnień, będą traktowane jako naruszenie obowiązków pracowniczych i mogą stanowić podstawę do zastosowania odpowiednich sankcji dyscyplinarnych.

ROZDZIAŁ V ORGANIZACYJNE I TECHNICZNE ŚRODKI BEZPIECZEŃSTWA

§ 10. 1. Obszarem, na którym należy zapewnić bezpieczeństwo danych w Urzędzie są pomieszczenia budynków, którymi administruje lub korzysta na podstawie innych umów Urząd, mieszczące się przy: ul. Piotrkowskiej 103 i 104, Żeromskiego 87, Traugutta 25, Pienistej 71, Leczniczej 6 i Gdańskiej 73 w Łodzi, a także przy ul. Sienkiewicza 16a i Glinianej 11 w Piotrkowie Trybunalskim, Pl. Wojewódzkim 3 w Sieradzu, ul. Jagiellońskiej 29 w Skierniewicach.

2. Przebywanie osób nieuprawnionych w pomieszczeniach tego obszaru jest ograniczone i odbywać się może tylko w obecności osób upoważnionych lub po uzyskaniu odpowiedniej zgody KJO.

Ochrona fizyczna i system nadzoru telewizyjnego (CCTV)

§ 11. 1. W celu ochrony obszarów ŁUW w Łodzi, stosuje się fizyczne zabezpieczenie wejść. Dostęp do budynków Urzędu jest nadzorowany przez służbę ochrony bezpośrednio, a dla lokalizacji przy ul. Piotrkowskiej 103 i 104, Żeromskiego 87, Gdańskiej 73, Traugutta 25 również za pomocą systemu nadzoru telewizyjnego (CCTV).

2. W miejscach ciągłego kontaktu z klientami w tym m.in. punktach obsługi kancelaryjnej oraz sekretariatach, może być umieszczona instalacja antynapadowa, umożliwiająca wezwanie służby ochrony.

3. Posterunki ochrony przy wejściach od ulicy Piotrkowskiej 104, przy ul. Piotrkowskiej 103 i Żeromskiego 87 pełnią służbę całodobowo.

4. Drzwi wejściowe do budynków oraz pomieszczeń Urzędu, po godzinach pracy Urzędu są zamykane na klucz, a klucze deponowane w wyznaczonych posterunkach ochrony. Nie dotyczy to pomieszczeń, w których wdrożony został elektroniczny system kontroli dostępu.

5. Dodatkowo otoczenie budynków Urzędu przy ul. Piotrkowskiej 103 i 104, Gdańskiej 73 oraz Żeromskiego 87 objęte jest systemem nadzoru telewizyjnego (CCTV), który na bieżąco jest obserwowany przez służbę ochrony.

6. System nadzoru telewizyjnego (CCTV) stanowi wsparcie dla ochrony fizycznej. Administratorem systemu jest Wojewoda Łódzki.

7. Monitoringiem objęte są obszary ważne dla ochrony osób i mienia, takie jak: wejścia do budynków, klatki schodowe i korytarze, docelowe pomieszczenia lub sąsiadujące z nimi lokalizacje, w których umieszczono urządzenia, osprzęt lub inne istotne mienie niezbędne do niezakłóconego funkcjonowania Urzędu, a także przyległe parkingi oraz tereny wewnętrzne.

8. Obszary objęte monitoringiem są oznakowane tabliczką zawierającą piktogram (rysunek kamery) oraz napis „obiekt monitorowany”.

9. Urząd stosuje środki techniczne i organizacyjne zapewniające ochronę odbieranego, rejestrowanego, odtwarzanego lub przetwarzanego obrazu, przed udostępnieniem osobom nieupoważnionym, zabraniem kopii zarejestrowanego obrazu przez osobę nieuprawnioną, zmianą, utratą lub zniszczeniem zarejestrowanego obrazu.

10. Szczegółowe zasady funkcjonowania systemu nadzoru telewizyjnego (CCTV) określa stosowne zarządzenie. Nadzór w tym zakresie sprawuje Dyrektor komórki organizacyjnej wskazanej w regulaminie organizacyjnym Urzędu.

11. Ochronę fizyczną Urzędu zapewnia specjalistyczna firma, na podstawie odrębnej umowy. Nadzór w tym zakresie sprawuje Dyrektor komórki organizacyjnej wskazanej w regulaminie organizacyjnym Urzędu.

Zasady organizacyjne zapewniające bezpieczeństwo

§ 12. 1. W celu zapewnienia zgodnego z przepisami bezpieczeństwa i uniknięcia błędów, mogących stanowić przyczynę naruszenia bezpieczeństwa informacji, stosuje się następujące zasady:

1) po zakończeniu pracy lub zmianie stanowiska, wszelkie nadane uprawnienia wygasają bądź zostają zaktualizowane;
2) ważność domenowych kont pracowników jest w sposób zautomatyzowany synchronizowana z terminami umów zapisanymi w systemie kadrowym. Po upływie terminu umowy o pracę danego pracownika jego konto domenowe jest wyłączane, a konto poczty elektronicznej jest usuwane. Konto EZD po zakończeniu umowy o pracę lub zmianie stanowiska pracy może zostać wyłączone albo pozostawione włączone z adnotacją NIEAKTYWNE do czasu zakończenia realizacji zadań przez zastępców mających dostęp do tego konta;
3) konta pracowników mogą zostać zablokowane przez oddział właściwy ds. informatyzacji, na podstawie informacji przekazanych przez kierowników komórek organizacyjnych Urzędu, którzy zobowiązani są do niezwłocznego powiadomienia oddziału właściwego ds. informatyzacji o powzięciu informacji o zamiarze bądź zakończeniu pracy przez pracownika.
4) do niszczenia zbędnych nośników stosuje się odpowiednie urządzenia w tym m.in. niszczarki dokumentów papierowych oraz nośników CD/DVD. Zniszczenie powinno być dokonane niezwłocznie po zaprzestaniu pracy w sposób uniemożliwiający ich odczytanie,

2. Stosowane środki techniczne zapewniające bezpieczeństwo danych przetwarzanych w systemie informatycznym są opisane w IZSI, stanowiącej załącznik nr 2 do zarządzenia.

Polityka kluczy

§ 13. 1. Klucze do pomieszczeń Urzędu mogą pobierać z depozytów znajdujących się w wyznaczonych posterunkach ochrony, tylko i wyłącznie pracownicy wyznaczeni przez Dyrektora wydziału/ równorzędnej komórki organizacyjnej. Listy tych osób są przekazywane Dyrektorowi komórki organizacyjnej wskazanej w regulaminie organizacyjnym Urzędu, jako właściwej w zakresie bezpieczeństwa fizycznego, który następnie przekazuje je do posterunków. Dla Centrum Powiadamiania Ratunkowego oraz jednostek zamiejscowych Dyrektor właściwego wydziału ustanawia „Politykę kluczy".

2. Klucze do pomieszczeń Wydziału Bezpieczeństwa i Zarządzania Kryzysowego deponowane są w depozytorze kluczy, mieszczącym się w Wydziale.

3. Podczas nieobecności pracowników w pomieszczeniach w czasie godzin pracy, drzwi są zamknięte na klucz.

4. Codziennie po zakończeniu pracy okna są zamykane, wyłącza się urządzenia elektryczne i komputery, aktywuje urządzenia alarmowe, jeżeli znajdują się w pomieszczeniu i zamyka drzwi na klucz.

5. Pomieszczenia i klucze do nich pozostają pod stałym nadzorem pracowników Urzędu lub pracowników ochrony.

Infrastruktura energetyczna, teleinformatyczna i telekomunikacyjna

§ 14. 1. Okablowania zasilające, teleinformatyczne i telekomunikacyjne służące do przesyłania danych lub wspomagające usługi informacyjne, są chronione przed przejęciem lub uszkodzeniem za pomocą odpowiednich zabezpieczeń, zgodnych z wymaganymi normami w tym zakresie.

2. Węzły informatyczne i energetyczne oraz centrala telefoniczna, umieszczone są w pomieszczeniach zabezpieczonych przed włamaniem drzwiami z zamkami bądź kodami. Poza tymi pomieszczeniami instalacje powinny być umieszczone w odpowiednio zabezpieczonych i oznaczonych skrzynkach i szafach rozdzielczych.

3. W przypadku konieczności umieszczenia kabli lub innych urządzeń do transmisji danych, muszą być zastosowane odpowiednie środki techniczne (m.in. osłony umieszczone na odpowiedniej wysokości lub w instalacjach podziemnych, uniemożliwiające bezpośredni dostęp lub przypadkowe uszkodzenia).

4. Nadzór nad zabezpieczeniem i eksploatacją w powyższym zakresie sprawuje Dyrektor komórki organizacyjnej wskazanej w regulaminie organizacyjnym Urzędu.

Kategorie informacji

§ 15. PBI obejmuje następujące kategorie informacji:

1) informację publiczną;
2) dane osobowe;
3) inne prawnie chronione informacje (w tym informacje niejawne i informacje stanowiące tajemnicę skarbową), które są uregulowane w stosownych zarządzeniach wewnętrznych.

§ 16. 1. Informacja publiczna jest udostępniana na podstawie ustawy z 6 września 2001 r. o dostępie do informacji publicznej (t.j. Dz.U. z 2023 r. poz. 190) oraz wewnętrznych uregulowań w sprawie trybu udostępniania informacji publicznej obowiązujących w Łódzkim Urzędzie Wojewódzkim w Łodzi.

2. Informacja publiczna umieszczona na stronie internetowej oraz stronie BIP Urzędu podlega niżej wymienionym środkom ochrony:

1) bieżącej kontroli dostępu do narzędzi administracyjnych strony www, umożliwiających wprowadzanie, usuwanie oraz modyfikację informacji osobom upoważnionym. Kontrolę dostępu realizuje operator strony internetowej w uzgodnieniu z koordynatorem ds. BIP. Kontrola odbywa się przy użyciu indywidualnego identyfikatora oraz hasła;
2) wprowadzaniu informacji na stronę www za pośrednictwem koordynatora ds. BIP lub w uzasadnionych przypadkach przez uprawnionych pracowników, wyznaczonych przez Dyrektora wydziału/ równorzędnej komórki organizacyjnej w uzgodnieniu koordynatorem ds. BIP. Wykaz ww. pracowników przekazywany jest do Pełnomocnika ds. Bezpieczeństwa Cyberprzestrzeni;
3) stosowaniu przez operatora strony internetowej Urzędu oraz BIP, odpowiednich zabezpieczeń technicznych i systemowych, uniemożliwiających nieautoryzowany dostęp do narzędzi administracyjnych strony;
4) określeniu i zapisaniu w umowach, odpowiedniego zakresu zabezpieczeń i uprawnień operatora strony internetowej Urzędu i BIP, w uzgodnieniu z Pełnomocnikiem ds. Bezpieczeństwa Cyberprzestrzeni.

Bezpieczeństwo w umowach ze stroną trzecią

§ 17. 1. ASI prowadzi rejestr podmiotów zewnętrznych posiadających przyznany dostęp do systemów informatycznych ŁUW, według wzoru stanowiącego załącznik nr 3 do PBI.

§ 18. 1. Na podstawie umowy użyczenia nr 40/2010 z 16 września 2010 r. w urzędzie działa Delegatura Krajowego Biura Wyborczego w Łodzi (DKBW). W sytuacji konieczności pracy poza godzinami funkcjonowania Urzędu Dyrektor DKBW zawiadamia o tym fakcie Dyrektora Generalnego Urzędu. Na taką okoliczność zostają wydzielone strefy, poprzez zamknięcie drzwi między korytarzami, w których mogą poruszać się pracownicy DKBW oraz osoby z zewnątrz, przynoszące dokumenty.

2. Wyznaczeni pracownicy DKBW posiadają przepustki umożliwiające przebywanie na terenie Urzędu poza godzinami jego funkcjonowania.

Zarządzanie ciągłością działania Urzędu

§ 19. Zarządzanie ciągłością działania Urzędu odnosi się do czynności wykonywanych codziennie, mających na celu zapobieganie (ograniczanie ryzyka) wystąpieniu sytuacji awaryjnej oraz utrzymywania gotowości, do natychmiastowej reakcji w przypadku zaistnienia sytuacji, zagrażających funkcjonowaniu Urzędu.

§ 20. Proces zarządzania ciągłością działania Urzędu, regulują odpowiednie procedury opracowane przez właściwe komórki organizacyjne Urzędu.

Zarządzanie ryzykiem

§ 22. 1. Analizę ryzyka bezpieczeństwa informacji, przeprowadza się w celu zapewnienia ochrony informacji przetwarzanych w Urzędzie, poprzez szacowanie zagrożeń oraz określenie sposobu postępowania w przypadku ich wystąpienia.

2. Analizę ryzyka bezpieczeństwa informacji należy przeprowadzać zgodnie z Zarządzeniem Wojewody Łódzkiego w sprawie zarządzania ryzykiem w Łódzkim Urzędzie Wojewódzkim w Łodzi.

3. Ryzyko bezpieczeństwa informacji z wyłączeniem ryzyka bezpieczeństwa systemów teleinformatycznych, wprowadza się do wydziałowych rejestrów ryzyk.

4. Analizę ryzyka w zakresie bezpieczeństwa systemów teleinformatycznych, przeprowadza Pełnomocnik Wojewody ds. Bezpieczeństwa Cyberprzestrzeni.

5. Metodykę analizy i oceny ryzyka bezpieczeństwa systemów teleinformatycznych określają wytyczne do Polityki Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej.

ROZDZIAŁ VI INNE SYSTEMY UŻYWANE W ŁUW W ŁODZI

§ 23. 1. W Urzędzie użytkuje się systemy informatyczne, dostarczone bądź udostępnione przez ministerstwa lub inne organy centralne, które określają zasady i zakres przetwarzania danych przez Wojewodę.

2. W przypadku użytkowania systemów informatycznych innych administratorów, należy stosować PBI oraz odpowiednio polityki bezpieczeństwa przekazane przez ich administratorów.

3. ASI raz do roku aktualizuje wykaz systemów informatycznych użytkowanych w Urzędzie, dla których administratorem danych jest inny organ niż Wojewoda Łódzki. Powyższe czynności powinny być dokumentowane w formie wykazu.

4. Wykaz systemów powinien zawierać: nazwę systemu, nazwę administratora danych, lokalizację (wydział/oddział).

5. Dla systemu EZD, oprócz niniejszej PBI stosuje się również Politykę Bezpieczeństwa EZD, opracowaną i przekazaną wraz z systemem przez Podlaski Urząd Wojewódzki w Białymstoku stanowiącą załącznik nr 4 do PBI.

§ 24. Przy Wojewodzie Łódzkim działa Wojewódzki Zespół ds. Orzekania o Niepełnosprawności. Zgodnie z art. 6d ust. 2 ustawy z 27 sierpnia 1997 r. o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych (t.j. Dz.U. z 2023 r. poz. 100.) wojewódzkie zespoły oraz Pełnomocnik są administratorami danych w prowadzonych przez siebie bazach danych systemu.

ROZDZIAŁ VII PRZEWOŻENIE DOKUMENTÓW PASZPORTOWYCH I KART POBYTU DLA CUDZOZIEMCÓW

§ 25. 1. W wyznaczone dni tygodnia pracownik Wydziału Spraw Obywatelskich i Cudzoziemców posiadający stosowne upoważnienie, samochodem służbowym wraz z kierowcą, odbiera dokumenty paszportowe i karty pobytowe dla cudzoziemców z Placówki Poczty Specjalnej Komendy Policji w Łodzi. Po pokwitowaniu przywozi je do siedziby Wydziału Spraw Obywatelskich i Cudzoziemców przy ul. Piotrkowskiej 103.

2. Dla Oddziału paszportowego mieszczącego się w Piotrkowie Trybunalskim, Sieradzu, Skierniewicach pracownik Wydziału Spraw Obywatelskich i Cudzoziemców posiadający stosowne upoważnienie odbiera dokumenty paszportowe z komend miejskich lub powiatowych znajdujących

się w powyższych miejscowościach. Transport w Piotrkowie Trybunalskim zapewnia Urząd, natomiast pozostałe lokalizacje są obsługiwane na podstawie stosownych umów:

1) w Sieradzu - umowa z Państwową Strażą Rybacką w Łodzi z siedzibą w Sieradzu;
2) w Skierniewicach - porozumienie z Wojewódzkim Inspektoratem Farmaceutycznym w Łodzi.

ROZDZIAŁ VIII POSTĘPOWANIE W PRZYPADKU NARUSZENIA BEZPIECZEŃSTWA SYSTEMÓW TELEINFORMATYCZNYCH

§ 26. 1. Każdy pracownik Urzędu, który posiada informację o naruszeniu bezpieczeństwa informacji, bądź posiada informację mogącą mieć wpływ na bezpieczeństwo danych lub systemów teleinformatycznych, co do zasady zobowiązany jest fakt ten zgłosić przełożonemu oraz ASI.

2. Do czasu przybycia na miejsce incydentu ASI i/lub przełożeni o których mowa w ust. 1, powinni uniemożliwić kontynuację pracy na danym stanowisku, zabezpieczyć komputer i inne dowody.

3. W ww. sytuacji ASI podejmuje następujące działania:

1) zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania, mając na uwadze ewentualne zagrożenia dla prawidłowości pracy;
2) może żądać określonej informacji od pracownika Urzędu w celu rozpoznania zakresu naruszenia;
3) powiadamia o zaistniałym naruszeniu Dyrektora Generalnego Urzędu i KJO;
4) ASI uzupełnia kartę zgłoszenia naruszenia bezpieczeństwa informacji, według wzoru stanowiącego załącznik nr 5 do PBI, przeprowadzają postępowanie wyjaśniające i określają kierunki dalszych działań naprawczych. Swoje wnioski przedstawia Dyrektorowi Generalnemu Urzędu i/lub KJO.

4. W przypadku włamania lub podejrzenia włamania do systemu teleinformatycznego, ASI lub z jego upoważnienia kierownik właściwego oddziału ds. informatyzacji, podejmuje niezbędne działania np.: czasowo wyłącza komunikację między elementami systemu, zmienia hasła administracyjne i/lub użytkowników, przekazuje informacje o incydencie Dyrektorowi Generalnemu Urzędu lub KJO, podejmuje decyzję o przywróceniu systemu do pracy.

5. W przypadku uszkodzenia danych ASI podejmuje działania w celu odtworzenia danych z kopii zapasowej zawierającej poprawne dane.

§ 27. 1. W szczególnych przypadkach KJO może powołać Zespół, którego zadaniem będzie wszechstronna ocena zaistniałego naruszenia oraz opracowanie wniosków dotyczących

ewentualnych przedsięwzięć proceduralnych, organizacyjnych i technicznych, które powinny zapobiec podobnym naruszeniom w przyszłości.

2. W skład Zespołu powinni wchodzić ASI, Pełnomocnik Wojewody ds. Bezpieczeństwa Cyberprzestrzeni, jako członkowie stali oraz merytoryczni pracownicy wydziału, w których naruszenie nastąpiło.

ROZDZIAŁ IX POSTANOWIENIA KOŃCOWE

§ 28. Świadome bądź przypadkowe naruszenie PBI może skutkować odpowiedzialnością dyscyplinarną lub karną, jeżeli przepisy prawa tak stanowią.

§ 29 Za aktualizację i nadzór nad realizacją postanowień PBI odpowiada Administrator Systemu Informatycznego.