Regulamin Systemu Informatycznego Jednostki Organizacyjnej Gminy Lublin

Pełny zakres dostępu do dokumentu – odczyt, modyfikacja:

1. Pełnomocnik ds. Systemu Zarządzania Bezpieczeństwem Informacji Urzędu Miasta Lublin,
2. Inspektor Ochrony Danych Urzędu Miasta Lublin,
3. Administrator Bezpieczeństwa Teleinformatycznego Urzędu Miasta Lublin,

Zakres dostępu do dokumentu – odczyt:

1. Administrator - Kierownik Jednostki Organizacyjnej Gminy Lublin,
2. Inspektor Ochrony Danych Jednostki Organizacyjnej Gminy Lublin,
3. Kierownictwo Jednostki Organizacyjnej Gminy Lublin,
4. Pracownicy Jednostki Organizacyjnej Gminy Lublin,
5. Administratorzy systemów informatycznych Urzędu Miasta Lublin
6. Administratorzy Systemów Informatycznych Jednostki Organizacyjnej Gminy Lublin,
7. Podmioty trzecie zarządzające systemem informatycznym Jednostki Organizacyjnej Gminy Lublin, upoważnione przez Kierownictwo tej Jednostki,

Spis treści:

1 Cel

Celem dokumentu w Jednostkach Organizacyjnych Gminy Lublin jest:

a. określenie minimalnych wymagań w zakresie bezpieczeństwa informacji dla Jednostek Organizacyjnych Gminy Lublin,

b. określenie minimalnych wymagań w zakresie zabezpieczeń systemów teleinformatycznych zgodnie z Regulaminem Organizacyjnym Urzędu Miasta Lublin oraz kompetencjami Biura Bezpieczeństwa Informacji i Wydziału Informatyki i Telekomunikacji Urzędu Miasta Lublin

2 Zakres

Niniejszy dokument stosuje się do systemów informatycznych używanych w Jednostce Organizacyjnej.

3 Terminologia

a. **ABT** – Administrator Bezpieczeństwa Systemów Informatycznych Urzędu Miasta Lublin,

b. **ADO/Administrator** – Kierownik Jednostki Organizacyjnej,

c. **ADO UML/Administrator UML**– Prezydent Miasta Lublin,

d. **ASI** – Administrator Systemu Informatycznego Jednostki Organizacyjnej Gminy Lublin (pracownik lub podmiot zewnętrzny),

e. **BBI UML** – Biuro Bezpieczeństwa Informacji Urzędu Miasta Lublin,

f. **CPD** – Centrum Przetwarzania Danych Urzędu Miasta Lublin,

g. **Dane osobowe** – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej. Dane osobowe dzieli się na dane zwykłe i dane wrażliwe.

   Jako przykład danych zwykłych można wskazać:

   - numery identyfikacyjne: imię, nazwisko, adres zamieszkania, PESEL, NIP, paszport, dowód osobisty,
   - cechy fizyczne: wygląd zewnętrzny, siatkówka oka, linie papilarne,
   - cechy fizjologiczne: grupa krwi,
   - cechy ekonomiczne: status majątkowy, lista zaległości finansowych.
   - środki komunikacji elektronicznej: numer telefonu, adres e-mai.

   Do danych wrażliwych zaliczają się dane dotyczące:

   - pochodzenie rasowe i etniczne,
   - przekonania religijne czy światopoglądowe,
   - przynależność do związków zawodowych czy partii,
   - poglądy polityczne,
   - stan zdrowia,
   - kod genetyczny,
   - dane biometryczne
   - dane o seksualności lub orientacji seksualnej,

- wyroków skazujących i naruszeń prawa.

h. **Dostępność danych** - rozumie się przez to właściwość zapewniającą, że dane są udostępniane dla upoważnionego podmiotu wtedy, gdy ich potrzebuje do przetwarzania,

i. **Integralność danych** – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,

j. **IOD** – Inspektor Ochrony Danych,

k. **IOD UML** – Inspektor Ochrony Danych Urzędu Miasta Lublin,

l. **Jednostka/Jednostka Organizacyjna** – Jednostka Organizacyjna Gminy Lublin,

m. **KJO** – Kierownik Jednostki Organizacyjnej Gminy Lublin,

n. **KK** – Komórka Jednostki odpowiedzialna za procesy kadrowe,

o. **KKO** – Kierownik Komórki Organizacyjna Jednostki, pion Jednostki,

p. **Kierownictwo Jednostki** – najwyższe kierownictwo Jednostki Organizacyjnej Gminy Lublin,

q. **Naruszenie bezpieczeństwa informacji** – wszelkie zdarzenia lub działania, w tym również niezamierzone, które mogą stanowić przyczynę utraty zasobów, zmian poufności, integralności, dostępności informacji lub niezawodności systemów, a także odstępstwa od obowiązujących procedur postępowania, nawet jeżeli n prowadzą do negatywnych skutków dla organizacji,

r. **Naruszenie ochrony danych osobowych** - naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych,

s. **Odbiorca danych** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem powszechnie obowiązującym, nie są jednak uznawane za odbiorców - przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania. Przy czym przez sformułowanie „ „strona trzecia" rozumie się osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, Administrator, podmiot przetwarzający czy osoby, które – z upoważnienia Administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe,

t. **Osoba upoważniona do przetwarzania danych osobowych** – osoba, która złożyła ADO oświadczenie o zachowaniu w tajemnicy przetwarzanych danych i stosowanych sposobach zabezpieczenia tych danyc posiadająca imienne upoważnienie wydane przez ADO, określające imię i nazwisko osoby upoważnionej, datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych oraz identyfikator, jeżeli dane są przetwarzane w systemie informatycznym,

u. **PML** – Prezydent Miasta Lublin,

v. **PSZBI** – Pełnomocnik ds. Systemu Zarządzania Bezpieczeństwem Informacji Urzędu Miasta Lublin – Sekretarz Miasta,

w. **UML** – Urząd Miasta Lublin,

x. **Podmiot przetwarzający** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora,

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

z. **Poufność danych** - rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom,

aa. **Regulamin/RSI** – Regulamin Systemu Informatycznego Jednostki Organizacyjne Gminy Lublin,

bb. **RBI** – Regulamin Bezpieczeństwa Informacji Jednostki Organizacyjne Gminy Lublin,

cc. **Rozliczalność danych** - rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,

dd. **RODO** – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych),

ee. **System CPD** – system informatyczny administrowany przez Wydział Informatyki i Telekomunikacji Urzędu Miasta Lublin,

ff. **System CPD Jednostki** – system informatyczny administrowany przez Jednostkę Organizacyjna i zlokalizowany w CPD,

gg. **System Jednostki** – system informatyczny administrowany przez Jednostkę Organizacyjną i zlokalizowany w niej lub na serwerach innych niż należące do Gminy Lublin (np. serwery rządowe, serwery w chmurze obliczeniowej, i itp.),

hh. **Systemy** – System CPD, System CPD Jednostki Organizacyjnej oraz System Jednostki Organizacyjnej,

ii. **Usuwanie danych** – trwałe zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,

jj. **Usługa CPD** – usługa informatyczna administrowana przez WI,

kk. **Usługa CPD Jednostki** – usługa informatyczna administrowana przez Jednostkę Organizacyjną i zlokalizowana w CPD,

ll. **Usługa Jednostki** – usługa informatyczna Jednostki Organizacyjnej administrowana przez Jednostkę i zlokalizowana w niej,

mm. **Ustawa** - ustawa z dnia .....o ochronie danych osobowych,

nn. **Uwierzytelnianie** – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu,

oo. **Użytkownik CPD** – osoba przetwarzająca dane w Systemie CPD lub Usłudze CPD, niezależnie od formy zatrudnienia lub formy prawnej wiążącej Jednostkę Organizacyjną z tą osobą, w szczególności mogą być to osoby zatrudnione na umowę o pracę, stażyści, praktykanci, osoby realizujące zadania na podstawie umowy cywilnoprawnej,

pp. **Użytkownik/Pracownik (w tym podmiotu trzeciego)** - osoba przetwarzająca dane w Systemie Jednostki oraz poza nim (np. dokumentacji w formie tradycyjnej), niezależnie od formy zatrudnienia w Jednostce lub formy prawnej wiążącej Jednostkę z tą osobą. W szczególności mogą być to osoby zatrudnione na umowę o pracę, stażyści, praktykanci, osoby realizujące zadania na podstawie podpisanej umowy cywilnoprawnej,

qq. **Zbiór danych** – to uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie,

rr. **Zgoda osoby, której dane dotyczą** – oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

4 Postanowienia ogólne

1. Regulamin Systemu Informatycznego dla Jednostki Organizacyjnej Gminy Lublin, zwany dalej Regulaminem lub RSI, określa zakres obowiązków i odpowiedzialności Jednostki Organizacyjnej w zakresie bezpieczeństwa informacji i ochrony danych osobowych. Regulamin obejmuje swoim zakresem wszystkich użytkowników.

2. **Przed** uzyskaniem dostępu do Usług i Systemów CPD oraz Usług i Systemów CPD, Jednostka Organizacyjna powinna spełniać wymagania niniejszego Regulaminu przed uzyskaniem dostępu do Usług i Systemów CPD oraz Usług i Systemów CPD. W szczególności wymagania należy spełnić w Systemie.

3. Przed rozpoczęciem przetwarzania informacji chronionych, w szczególności danych osobowych, których Administratorem jest Prezydent Miasta Lublin:

   a. Jednostka podpisuje umowę powierzenia przetwarzania danych osobowych lub porozumienie dotyczące współadministrowania danymi osobowym.

   b. Każdy użytkownik podpisuje oświadczenie na wzorze będącym załącznikiem nr 2 do Regulaminu Bezpieczeństwa Informacji.

4. Użytkownicy w Jednostce zobowiązani są do zapoznania z zasadami bezpieczeństwa informacji zawartymi w **Regulaminie Bezpieczeństwa Informacji Jednostki Organizacyjnej Gminy Lublin.**

5. W przypadku braku możliwości spełnienia przez Jednostkę minimalnych wymogów opisanych w RSI, KJO zobowiązany jest do poinformowania o tym fakcie BBI oraz WI wskazując w sposób precyzyjny zapisy, które nie mogą być realizowane wraz z uzasadnieniem.

5 Nadawanie, zmiana bądź odebranie uprawnień Użytkowników CPD do Systemów i Usług CPD administrowanych przez UML

1. Decyzję o dostępie Jednostki Organizacyjnej do Systemu podejmuje Dyrektor WI po spełnieniu przez Jednostkę Organizacyjną wymagań bezpieczeństwa informacji określonych w RSI.

2. Nadawanie, zmiana bądź odebranie uprawnień dla użytkownika do Systemu CPD odbywa się na podstawie wniosku KJO lub osoby przez niego upoważnionej, przesłanego do Urzędu Miasta Lublin wyłącznie za pośrednictwem platformy ePUAP ma skrytkę: /UMLublin/SkrytkaESP . Wniosek musi zostać podpisany elektronicznym podpisem z kwalifikowanym certyfikatem przez KJO lub osobę przez niego upoważnioną.

   Wzór wniosku stanowi Załącznik nr 1 do RSI.

3. Wniosek należy wypełnić w przypadku:

   a. pierwszego zgłoszenia do pracy w Systemie CPD,

   b. modyfikacji uprawnień,

   c. odebrania uprawnień,

   d. konieczności nadania/modyfikacji/odebrania uprawnień do Usługi CPD, aplikacji, zasobów sieciowych, poczty e-mail, innych zasobów Systemu CPD.

4. Nadanie/Zmiana/Odebranie uprawnień w systemach informatycznych dotyczy zmiany istniejących uprawnień Użytkownika CPD do:

   a. uprawnień do Usługi CPD, aplikacji, programu, zasobów sieciowych, usługi informatycznej,

   b. dostępu do danych w aplikacjach, których Administratorem jest inna Jednostka Organizacyjna,

   c. zmiany stanowiska, awansu, zmiany zakresu obowiązków związanych ze zmianą zakresu uprawnień w Systemie CPD,

   d. przejęcia obowiązków przez innego Użytkownika CPD na dowolny czas,

   e. przekazania zasobów od/do Użytkownika CPD zwolnionego lub przechodzącego na inne stanowisko,

f. przejęcia zasobów na czas dłuższej nieobecności Użytkownika CPD (urlop wypoczynkowy lub bezpłatny, zwolnienie lekarskie, inne) wg uznania Kierownika Jednostki Organizacyjnej.

5. W przypadku wątpliwości dotyczących zakresu uprawnień Użytkownika CPD należy skontaktować się z WI. Zakres upoważnienia i uprawnień Użytkownika CPD w Systemach CPD powinien być adekwatny do wykonywanych przez niego zadań. Za wskazanie właściwego zakresu upoważnienia i uprawnień odpowiada bezpośredni przełożony lub KJO.

6. Właściwy administrator systemu nadaje/modyfikuje/odbiera użytkownikowi uprawnienia zgodnie z zasadami nadawania/ modyfikacji/odbierania uprawnień przyjętymi w Urzędzie Miasta Lublin.

   a. podczas rejestracji Użytkownika CPD nadawany jest unikalny identyfikator użytkownika oraz ustawiane jest hasło tymczasowe niezbędne do logowania po raz pierwszy w Systemie CPD, hasło musi być zgodne z zasadami tworzenia haseł opisanymi w RSI Jednostki Organizacyjnej,

   b. upoważnionym do odbioru hasła jest wyłącznie użytkownik CPD,

   c. osoba upoważniona może odebrać nowe i zmienione hasła:

      - osobiście u właściwego administratora systemu po otrzymaniu zwrotnej informacji, że hasło jest gotowe do odbioru; hasło tymczasowe przekazywane jest w zamkniętej kopercie do rąk własnych osoby upoważnionej, za pokwitowaniem odbioru w Ewidencji Wydanych Haseł, po weryfikacji tożsamości osoby odbierającej poprzez wgląd do dowodu tożsamości,

      - podczas rozmowy telefonicznej z właściwym administratorem systemu – tylko pod warunkiem weryfikacji tożsamości rozmówcy na podstawie nr PESEL i zapytania o losowo wskazane 4 cyfry,

   e. o nadaniu/zmianie/odebraniu uprawnień Użytkownika CPD w odpowiednich Systemach CPD administrator systemu informuje drogą elektroniczną wnioskującego w Jednostce oraz ABT.

7. W przypadku wystąpienia okoliczności skutkujących koniecznością odebrania uprawnień do Systemu CPD/ Usług CPD (np. rozwiązanie umowy o pracę z pracę z użytkownikiem, zakończeniem stażu, umowy cywilno-prawnej, itp.) obowiązkiem KJO jest złożenie wniosku o nadanie/zmianę/odebranie uprawnień nie później niż 3 dni robocze przed datą zakończenia umowy o pracę/ stażu/umowy cywilno-prawnej do WI. Wniosek może również złożyć osoba upoważniona przez KJO.

8. Przed rozpoczęciem pracy w systemie Użytkownik CPD musi mieć podpisane Oświadczenie stanowiące Załącznik nr 2 do Regulaminu Bezpieczeństwa Informacji w Jednostce Organizacyjnej Gminy Lublin.

9. Dopuszcza się nadanie uprawnień osobom spoza Jednostki Organizacyjnej w szczególnie uzasadnionych przypadkach. Każdy taki przypadek KJO uzasadnia na Wniosku o Nadanie/Zmianę/Odebranie uprawnień.

10. W uzasadnionych przypadkach istnieje możliwość natychmiastowego odebrania uprawnień przez ABT lub na wniosek KJO skierowany do BBI oraz WI. Wniosek może być przekazany dowolną drogą komunikacji. Administrator Systemu CPD blokuje konto w systemie, a wnioskujący ma obowiązek wystawić w ciągu 7 dni wniosek o odebranie uprawnień wraz z uzasadnieniem. Formalnego odebrania uprawnień dla Użytkownika CPD dokonuje się w Systemie CPD po wpłynięciu wniosku o odebranie uprawnień.

11. W uzasadnionym przypadkach na wniosek KJO lub osoby przez niego upoważnionej, złożony w postaci wiadomości elektronicznej e-mail lub tradycyjnej formie pisemnej, istnieje możliwość zmiany hasła danego Użytkownika CPD do określonego Systemu CPD. Przekazanie hasła następuje zgodnie z niniejszą procedurą.

6 Nadawanie, zmiana bądź odebranie uprawnień Użytkowników Jednostki do systemów CPD Jednostki oraz systemów Jednostki Organizacyjnej Gminy Lublin

W przypadku, gdy Jednostka Organizacyjnie samodzielnie zarządza uprawnieniami do systemu, ASI jest odpowiedzialny za utworzenie instrukcji nadawania/modyfikacji/odbierania uprawnień w systemie, za który odpowiada. Instrukcja musi zapewnić nadawanie adekwatnych uprawnień do wykonywanych obowiązków przez Użytkownika. Instrukcja musi zawierać w szczególności:

   a. sposób zarządzania uprawnieniami użytkowników, w tym nadawania i odbierania uprawnień,

b. sposób zarządzania kontami użytkowników, w tym zakładania i blokowania kont,

c. uwzględnienie nadania stosownego upoważnienia do przetwarzania danych osobowych zgodnie z Polityką Bezpieczeństwa Informacji Jednostki Organizacyjnej Gminy Lublin, profile uprawnień dla grup użytkowników, powiązanych z ich zakresem czynności,

d. sposób i częstość wykonywania przeglądów uprawnień użytkowników.

7 Sposób przepływu danych pomiędzy systemami

1. Opis sposobu przepływu danych wskazuje, które z systemów są połączone oraz w jakim zakresie. Opis ten może być przedstawiony w postaci graficznej, ukazującej istniejące powiązania pomiędzy obiektami, jak również w postaci opisu tekstowego. Tworząc sposób przepływu danych osobowych należy uwzględnić możliwość wystąpienia przepływów:

   a. automatycznych,

   b. półautomatycznych (np. import export plików przesyłanych za pomocą sieci),

   c. manualnych – przy wykorzystaniu zewnętrznych nośników danych (płyty CD, DVD, PenDrive itp.).

2. Przedstawiając przepływ danych, można posłużyć się schematami, które wskazują, z jakimi zbiorami danych system lub moduł systemu współpracuje, czy przepływ informacji pomiędzy systemami informatycznymi jest jednokierunkowy czy dwukierunkowy.

8 Metody i środki uwierzytelniania

Dostęp do poszczególnych części systemu informatycznego jest możliwy wyłącznie poprzez podanie prawidłowego identyfikatora i hasła przyznanych użytkownikowi podczas procesu nadawania uprawnień do Systemu Teleinformatycznego. Celem zapewnienia bezpieczeństwa zaleca się stosowanie usług uwierzytelniania, szyfrowania, integralności i niezaprzeczalności za pośrednictwem kryptografii klucza publicznego.

8.1 Hasła użytkowników

1. Hasła Użytkowników do systemów podlegają następującym zasadom:

   a. hasło składa się z minimum 8 znaków,

   b. hasło musi spełniać warunek złożoności polegający na występowaniu w nim: wielkiej i małej litery, oraz cyfry lub znaku specjalnego (np. !@#),

   c. hasło musi być zmieniane minimum co 30 dni,

   d. kolejne hasła muszą być różne,

   e. hasła należy przechowywać w sposób gwarantujący ich poufność.

2. Zabrania się udostępniania haseł innym osobom.

3. Zabrania się tworzenia haseł na podstawie:

   a. cech i numerów osobistych (np. dat urodzenia, imion itp.),

   b. sekwencji klawiszy klawiatury (np. qwerty, 12qwaszx),

   c. identyfikatora użytkownika.

4. Zabrania się tworzenia haseł łatwych do odgadnięcia.

5. Logowanie anonimowe do systemu informatycznego jest zabronione dla użytkowników.
6. Uwierzytelnienie następuje wyłącznie po podaniu zgodnego hasła i powiązanego z nim identyfikatora.
7. W przypadku logowania do systemu informatycznego odbywającego się po raz pierwszy, użytkownik ma obowiązek zmiany hasła tymczasowego na właściwe, na znane tylko użytkownikowi.
8. W przypadku systemów, które nie wymuszają automatycznie cyklicznej zmiany hasła oraz nie kontrolują jego znaków obowiązkiem Użytkownika jest samodzielna cykliczna zmiana hasła zgodnie z zasadami określonymi w ust. poprzednich.
9. Użytkownik ponosi pełną odpowiedzialność za utworzenie hasła i jego bezpieczne przechowywanie.
10. Hasła nie mogą być ujawniane w sposób celowy lub przypadkowy i powinny być znane wyłącznie użytkownikowi.
11. Hasła nie mogą być przechowywane w formie dostępnej dla osób nieupoważnionych:
    a. w plikach,
    b. na kartkach papieru w miejscach dostępnych dla osób trzecich,
    c. w skryptach,
    d. w innych zapisach elektronicznych i papierowych, które byłyby dostępne dla osób trzecich.
12. W przypadku podejrzenia ujawnienia haseł osobie nieupoważnionej, użytkownik niezwłocznie zmienia hasło lub zgłasza wniosek o zmianę hasła:
    a. do ABT w przypadku hasła do Systemów CPD,
    b. do ASI w przypadku Systemów Jednostki Organizacyjnej lub Systemów CPD Jednostki Organizacyjnej.
13. Użytkownik utrzymuje hasło w tajemnicy również po upływie jego ważności.
14. Zabrania się przekazywania hasła za pomocą telefonu, przesyłania z pomocą faksu i poczty e-mail w formie jawnej (niezaszyfrowanej).
15. Uwierzytelniające karty mikroprocesorowe pozwalające zidentyfikować użytkownika na podstawie indywidualnego kodu PIN muszą być przechowywane w sposób uniemożliwiający ich zniszczenie lub zagubienie, co najmniej w zamykanych na klucz szafkach.
16. Zabrania się udostępniania innym osobom indywidualnych identyfikatorów, w tym w szczególności nazwy użytkownika, tokenu, karty inteligentnej i innych danych umożliwiających uwierzytelnienie, w tym haseł, pinów, kodów itp.).

8.2 Hasła administracyjne

1. O ile jest to możliwe zaleca się wyłączanie bądź zmianę nazwy kont administracyjnych domyślnie wbudowanych w system. Uruchamianie usług bądź aplikacji w systemach należy wykonywać logując się na konto z uprawnieniami użytkownika, stosując do wykonania zadania narzędzia tymczasowo podnoszące poziom uprawnień.
2. Hasła administracyjne do Systemów CPD Jednostki Organizacyjnej oraz Systemów Jednostki Organizacyjnej podlegają następującym zasadom:
    a. hasło administracyjne składa się z minimum 10 znaków,
    b. hasło musi spełniać warunek złożoności polegający na występowaniu w nim: wielkiej i małej litery, dwóch cyfr oraz znaku specjalnego (np. !@#),
    c. hasło administracyjne do systemu musi być cyklicznie zmieniane minimum co 90 dni. Zasada jest stosowana do haseł przypisanych do identyfikatorów, które nie są wykorzystywane przez użytkowników do przetwarzania danych osobowych; w przeciwnym wypadku należy stosować zasadę zmiany hasła cyklicznie co 30 dni,

d. kolejne hasła muszą być różne.

3. Stosowanie jako haseł: imion osób, imion zwierząt, dat urodzin, nazw drużyn piłkarskich, nazw zespołów muzycznych, nazw marek samochodów, nazwy Jednostki Organizacyjnej, nazw miejscowości, nazwiska lub imienia użytkownika jest zabronione.

4. Stosowanie łatwych do odgadnięcia ciągów znaków w hasłach jest zabronione.

5. Utworzone hasło administracyjne wraz z powiązanym identyfikatorem w systemie (np. root, admin, administrator) musi zostać zapisane na kartce papieru, włożone do koperty, która następnie musi zostać zaklejona.

6. Koperta z hasłem musi zostać następnie zdeponowana w bezpiecznym miejscu niedostępnym dla osób nieupoważnionych w metalowej kasetce lub sejfie.

7. Zarejestrowane hasła administratora, oprócz treści hasła, winny posiadać adnotację o dacie ich wprowadzenia do systemu oraz być przechowywane z rotacją 1 wstecz.

8. W przypadku ujawnienia hasła lub podejrzenia naruszenia bezpieczeństwa systemu, należy niezwłocznie zmienić hasła administracyjne.

9. Hasła administracyjne do systemu mogą być znane wyłącznie administratorom odpowiedzialnym za dany system.

9 Dostęp zdalny do Systemu CPD Jednostki Organizacyjnej

1. Dostęp zdalny do systemów CPD Jednostki Organizacyjnej możliwy jest jedynie za pomocą technologii VPN administrowanej przez WI.

2. Jednostka Organizacyjna prowadzi wykaz osób posiadających dostęp zdalny do zasobów Centrum Przetwarzania Danych Urzędu Miasta Lublin.

3. KJO składa wniosek do WI o nadanie / modyfikację/odebranie uprawnień (na wzorze określonym w Załączniku nr 1 do RSI)

4. Dostęp zdalny jest nadawany przez WI po pozytywnym wyniku przeprowadzonej przez WI analizy zagrożeń bezpieczeństwa teleinformatycznego. O nadaniu dostępu informowane jest BBI.

10 Dostęp zdalny do Systemu Jednostki Organizacyjnej

1. Zasady dotyczą wyłącznie systemów administrowanych lokalnie przez Jednostki Organizacyjne i posiadających zdalny dostęp z sieci Internet.

2. Dostęp zdalny do zasobów Jednostki Organizacyjnej, możliwy jest tylko po spełnieniu warunków wymienionych w niniejszym Regulaminie.

3. Dostępu do systemu udziela ASI na podstawie pisemnej decyzji KJO, który informuje WI o udzielonym dostępie.

4. Do dostępu zdalnego należy wykorzystywać poniższy standard bezpieczeństwa:

   a. Virtual Private Network,

   b. kanał SSL lub IPSec,

   c. algorytm szyfrujący AES z długością klucza min. 128 bit,

   d. długość klucza wstępnego: min. 20 znaków,

   e. hasła użytkownika muszą spełniać wymagania niniejszego Regulaminu.

5. ASI prowadzi pisemny wykaz osób posiadających dostęp zdalny do zasobów Jednostki Organizacyjnej (wraz z danymi historycznymi).

6. Zabrania się podejmowania czynności zmierzających do penetrowania zasobów sieci.

7. Zabrania się wykorzystywania dostępu zdalnego:
   a. z komputerów innych niż służbowe, należące do Jednostki Organizacyjnej,
   b. z sieci publicznie dostępnych np. kafejki internetowe, dworce PKP, restauracje, bezprzewodowe sieci otwarte (hotspoty).

11 Korzystanie z poczty elektronicznej

1. Jednostki Organizacyjne Gminy Lublin mogą korzystać wyłącznie z poczty hostowanej przez Urząd Miasta Lublin.
2. Zasady korzystania z poczty elektronicznej opisane zostały w Regulaminie Bezpieczeństwa Informacji Jednostki Organizacyjnej Gminy Lublin.

12 Wymagania zabezpieczeń dla stacji roboczych

1. Za spełnienie wymagań zabezpieczeń dla stacji roboczych odpowiedzialny jest ASI.
2. Do Systemów mogą być podłączane wyłącznie komputery i urządzenia zgodne z minimalnymi wymaganiami bezpieczeństwa, które są opracowywane przez BBI i udostępniane Jednostce. W przypadku braku takiego standardu, stosuje się minimalne wymagania bezpieczeństwa podane w punktach 13.1, 13.2 oraz 13.3.

12.1 Zabezpieczenia dostępu fizycznego

Należy stosować poniższe zasady bezpieczeństwa:

a. zabezpieczyć dostęp do BIOSu hasłem; hasło musi spełniać wymagania zawarte w RSI,
b. jako urządzenie boot'ujące ustawić wyłącznie dysk twardy,
c. ustawić stację roboczą w miejscu, w którym sprzęt nie będzie narażony na uszkodzenia fizyczne np. potrącenie, zalanie, przegrzanie,
d. zabezpieczyć kable i utworzyć zwarte wiązki,
e. w sytuacji, gdy jest to możliwe, zamknąć obudowę stacji roboczej na klucz,
f. w strefach dostępu osób nieupoważnionych np. Biuro Obsługi Klienta, należy zabezpieczyć stację roboczą przed dostępem tych osób,
g. w miejscach szczególnie zagrożonych kradzieżą należy stosować linki zabezpieczające sprzęt,
h. monitory stacji roboczych należy ustawić w sposób uniemożliwiający osobom trzecim zapoznanie się z informacjami wyświetlanymi na monitorach,
i. w miejscach dostępnych publicznie, gdy nie ma możliwości ustawienia monitora zgodnie z zasadami powyżej, należy stosować filtry prywatyzujące na monitory,
j. należy zapewnić ciągłość działania kluczowych stacji roboczych poprzez zapewnienie nieprzerwanego zasilania,
k. zaleca posiadanie zapasowej stacji roboczej w celu szybkiej wymiany na stanowisku pracy.

12.2 Konfiguracja systemu operacyjnego

Należy stosować zasady:

a. ustawić hasło konta administratora lokalnego, które musi spełniać wymagania zawarte w RSI,
b. użytkownicy posiadają konta z ograniczeniami uniemożliwiającymi ingerencję w system operacyjny oraz samodzielną instalację oprogramowania,

c. użytkownicy muszą mieć zablokowaną funkcję udostępniania zasobów sieciowych na własnych komputerach innym użytkownikom (samodzielne udostępnianie folderów w sieci przez użytkownika),

d. należy używać systemu plików NTFS,

e. ustawienia muszą wymuszać automatyczne blokowanie stacji roboczej po upływie 5 minut nieaktywności użytkownika,

f. należy wyłączyć lub odinstalować wszystkie nieużywane usługi oraz aplikacje,

g. dostęp zdalny do stacji roboczych musi wykorzystywać zaszyfrowane i uwierzytelniane połączenie,

h. konfiguracja dostępu zdalnego do stacji roboczej muszą pozwalać na każdorazową akceptację dostępu przez użytkownika stacji roboczej,

i. każda stacja robocza musi mieć zaktualizowany system operacyjny,

j. każda stacja robocza musi mieć zaktualizowany program antywirusowy,

k. każda stacja robocza musi mieć włączoną zaporę ogniową (Firewall),

l. na komputerach przenośnych należy stosować szyfrowanie dysków twardych,

m. oprogramowanie jest zainstalowane zgodnie z postanowieniami licencji producenta oprogramowania,

n. oprogramowanie jest stosowane zgodnie z ustawą Prawo autorskie i prawach pokrewnych.

o. użytkownik może otrzymać uprawnienia lokalnego administratora w systemie operacyjnym swojego komputera wyłącznie na podstawie decyzji KJO. Wówczas odpowiedzialność za aplikacje, zagrożenia i stan zabezpieczeń komputera odpowiada Użytkownik od momentu przekazaniu dostępu przez ASI.

12.3 Stosowanie zabezpieczeń kryptograficznych

W celu ochrony poufności i integralności przesyłanych oraz przechowywanych danych stosuje się zabezpieczenia kryptograficzne. Miejsca stosowania kryptografii musi być zgodne z wymaganiami przepisów prawa oraz regulacjami wewnętrznymi, w szczególności należy stosować zabezpieczenia kryptograficzne:

1. na dyskach twardych komputerów przenośnych zawierających dane podlegające ochronie,
2. na pendrive'ach zawierających dane podlegające ochronie,
3. systemach zdalnego dostępu,
4. w załącznikach do wiadomości poczty elektronicznej, w których przesyłane są dane objęte ochroi w szczególności dane osobowe,

rozwiązania kryptograficzne musi wykorzystywać algorytm AES o długości klucza min. 128 bit.

13 Wymagania dla aplikacji WWW uruchamianych w Centrum Przetwarzania Danych

13.1 Wymagania budowy aplikacji

Wszelkie aplikacje hostowane u dostawców zewnętrznych muszą zostać przeniesione do CPD UML celem minimalizacji kosztów oraz ujednolicenia standardów świadczonych usług przez Jednostki Organizacyjne Gminy Lublin. Aplikacja oparta o przeglądarkę internetową musi być zbudowana zgodnie z niżej wymienionymi zaleceniami:

1. w przypadku, gdy aplikacja ma współpracować z już istniejącymi aplikacjami, technologia może być taka sama lub kompatybilna w zakresie współpracy z aplikacjami i bazami danych istniejącymi już w środowisku produkcyjnym,
2. przed rozpoczęciem procesu zakupowego technologia (np. opisana w dokumentacji), z której korzysta aplikacja powinna zostać zatwierdzona przez WI,
3. bezpieczeństwo aplikacji należy zapewnić wdrażając możliwie dużo zabezpieczeń zgodnych z prawem (np. CAPTCHA, klawiatura ekranowa do wprowadzania hasła, klucze generujące hasło użytkownikom, hasła

maskowane itp.), zaleca się uwzględnienie innych okoliczności towarzyszących budowie aplikacji (np. niepełnosprawności użytkowników min. na poziomie WCAG 2.0),

4. KJO odpowiada za wykorzystanie aplikacji zgodnie z jej przeznaczeniem i z zaakceptowanymi przez WI parametrami technicznymi,

5. w przypadku, gdy działanie aplikacji prowadzi do naruszenia zasad bezpieczeństwa teleinformatycznego powiadamiany jest KJO, BBI UML oraz WI, w przypadku, gdy działania Jednostki Organizacyjnej w zakresie przywrócenia akceptowalnego poziomu bezpieczeństwa będą nieskuteczne lub będą prowadzić do destabilizacji innych systemów WI ma prawo zablokować pracę aplikacji lub wyłączyć serwer,

6. Szczegółowe zasady dostępu oraz korzystania z systemu hostingowego UML opisane zostały w Załączniku nr 4 – Regulamin korzystania z systemu hostingowego.

14 Zakupy sprzętu komputerowego, wyposażenia, oprogramowania i aplikacji

1. W celu zagwarantowania standardów zakupywanego sprzętu oraz oprogramowania komputerowego Jednostka Organizacyjna musi korzystać ze standardów sprzętu obowiązujących w UML.

2. Nowe stacje robocze, na których przetwarzane będą dane podlegające ochronie muszą być wyposażone w system operacyjny Windows w wersji profesjonalnej (nie home, nie domowej, nie starter).

15 Zasady korzystania z dostępu do sieci teleinformatycznej UML

Zgodnie z Zarządzeniem Nr 918/2011 Prezydenta Miasta Lublin z dnia 05 września 2011 r. w sprawie zasad korzystania z Miejskiej Sieci Teleinformatycznej przez Jednostki Organizacyjne Gminy Lublin, należy stosować poniższe zasady:

1. dostęp do Internetu realizowany jest wyłącznie z wykorzystaniem metod i łączy autoryzowanych przez Wydział Informatyki i Telekomunikacji,

2. zabrania się przeglądania stron Internetowych zawierających materiały godzące w dobre obyczaje lub niezgodne z prawem,

3. zabrania się wykonywania czynności mogących wpłynąć niekorzystnie na działanie Sieci Miejskiej, a w szczególności urządzeń dostępowych innych użytkowników, w szczególności zabronione jest:

   a. powodowanie zjawiska przeciążenia sieci i usług,

   b. przekazywanie danych zawierających złośliwy kod,

   c. przekazywanie pakietów IP z fałszywym adresem nadawcy,

   d. podejmowanie prób nieautoryzowanego wejścia do zasobów informatycznych innych użytkowników sieci Internet.

4. w przypadku stwierdzenia naruszenia powyższych zasad przez użytkownika sieci w jednostce, administrator sieci powiadamia kierownika jednostki, w której doszło do nadużycia,

5. jeżeli nadużycie powoduje przerwy lub niestabilną pracę sieci, administrator sieci może zablokować dostęp do Sieci Miejskiej,

6. Administrator sieci prowadzi stały monitoring postępu jednostek do Internetu i Intranetu w zakresie obejmującym w szczególności:

   a. transmisję danych,

   b. przestrzeganie zasad określonych w pkt. 16 ppkt. 1- pkt. 16 ppkt. 4.

7. Na żądanie Kierownika Jednostki administrator sieci udostępni szczegółowe informacje (logi) dotyczące stwierdzonych naruszeń lub nadużyć w czasie do 30 dni wstecz od dnia otrzymania zapytania.

16 Ewidencja zasobów teleinformatycznych

Każdy element systemu (np. sprzęt teleinformatyczny/oprogramowanie) musi być ewidencjonowany. Zakres informacji musi określać co najmniej:

a. unikalny identyfikator sprzętu (np. numer inwentarzowy),

b. opis elementu (np. komputer stacjonarny, drukarka),

c. lokalizacja elementu,

d. użytkownik,

e. zainstalowane aplikacje wymagające licencji wraz z określeniem czasu jej trwania,

f. wersja elementu (np. wersja systemu operacyjnego w przypadku komputerów, oprogramowania).

Ewidencja sprzętu i oprogramowania stanowi inwentaryzację sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację w rozumieniu rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.

17 Zarządzanie aktualizacjami systemów

Aktualizacje w systemach zgodnie z niniejszym Regulaminem są wprowadzane w szczególności:

1) w sytuacji pojawienia się poprawek dotyczących np. zabezpieczeń dostarczonych przez producenta,

2) w sytuacji wykrycia incydentu naruszenia bezpieczeństwa,

3) konieczności dopasowania funkcjonalności do nowych wymagań przetwarzania danych Jednostce,

4) konieczności instalacji poprawki lub aktualizacji oprogramowania,

5) instalacji nowych urządzeń lub oprogramowania.

17.1 Czynności przed wprowadzaniem aktualizacji

Przed wprowadzeniem aktualizacji oprogramowania na serwerach i usługach sieciowych należy:

1) w miarę możliwości oszacować potencjalny wpływu aktualizacji na bezpieczeństwo systemu i wprowadzeni adekwatnych zabezpieczeń,

2) wykonać kopię zapasową danych systemu objętego zmianami,

3) wykonać kopię zapasową systemu operacyjnego wraz z plikami aplikacji lub w systemach administrowanych lokalnie ustanowić punkt przywracania systemu,

4) w uzasadnionych przypadkach wykonać testy w wydzielonym (odseparowanym od produkcyjnego) środowisku testowym,

5) przed wprowadzeniem aktualizacji oprogramowania na komputerach użytkowników należy:

   a. wykonać kopię zapasową systemu operacyjnego wraz z plikami aplikacji lub w systemach administrowanych lokalnie ustanowić punkt przywracania systemu,

   b. wykonać kopię zapasową danych systemu objętego zmianami, jeżeli aktualizacja jest związana z ryzykiem utraty poufności, integralności lub dostępności danych systemu.

17.2 Proces wprowadzania aktualizacji

Przebieg procesu:

1) Wprowadzenie aktualizacji do systemu.

2) Przetestowanie poprawności po wprowadzeniu aktualizacji:

   a. sprawdzenie przez ASI działania usług sieciowych i aplikacji,

   b. sprawdzenie przez użytkowników poprawności funkcjonalności usług sieciowych i aplikacji oraz poprawności danych,

   c. w przypadku wykrycia poważnych błędów poinformowanie KJO i podjęcie decyzji dalszym sposobie postepowania, w tym przywróceniu stanu systemu z kopii zapasowej.

3) Przekazanie informacji użytkownikom o możliwości rozpoczęcia pracy w systemie.

18 Zarządzanie podatnościami

18.1 Informacje o podatnościach

Źródłem informacji o podatnościach mogą być w szczególności:

1) wiadomości od producentów sprzętu i oprogramowania,

2) bazy wiedzy w Internecie np. CVEDETAILS.COM,

3) wyniki testów podatności,

4) raporty z incydentów naruszenia bezpieczeństwa.

18.2 Reagowanie na podatności

1) Po pozyskaniu informacji o podatności, należy wprowadzić poprawki do konfiguracji i oprogramowania w celu minimalizacji ryzyka wykorzystania podatności lub poinformować WI o podatności.

2) W sytuacji, gdy usunięcie wymaga instalacji aktualizacji oprogramowania, należy posługiwać się procedurą zawartą w pkt 18 Regulaminu.

3) W sytuacji pozyskania informacji o nieujawnionych podatnościach oprogramowania, należy podjąć niezwłoczne działania w celu minimalizacji ryzyka wykorzystania podatności:

   a. zgłoszenie podatności do producenta,

   b. wyłączenie części systemu objętej podatnością o wysokim ryzyku,

   c. kontrolowanie podatności za pomocą dodatkowych zabezpieczeń wykrywających i blokujących próby wykorzystania tej podatności.

19 Zasady monitorowania, przeglądu i konserwacji systemu informatycznego

19.1 Przeglądy i konserwacje

1. W sytuacji, kiedy konieczne jest dokonanie czynności konserwacyjnych i przeglądów elementów systemu, należy je wykonywać w sposób nie wpływający na ciągłość działania systemu i bezpieczeństwo danych.

2. W przypadku, kiedy zachowanie ciągłości działania systemu informatycznego nie jest możliwe, przedmiotowe czynności musi zostać przeprowadzone po godzinach pracy obowiązujących w Jednostce Organizacyjnej.

3. Czynności związane z przeglądem i konserwacją systemu muszą być prowadzone w sposób profesjonalny, nie stanowiący zagrożenia dla danych przetwarzanych w systemie oraz dla nośników informacji.

4. Osoby dokonujące czynności opisanych w niniejszym Regulaminie związanych z konserwacją i przeglądem systemu informatycznego oraz nośników danych, zobowiązane są przygotować protokół zawierający datę, rodzaj czynności, zużyte i wykorzystane do ich wykonania materiały i urządzenia, wynik oraz informacje o wszystkich zaobserwowanych w czasie prac nieprawidłowościach w działaniu i konfiguracji systemu oraz stanie nośników informacji. Wzór protokołu z przeglądu lub konserwacji systemu informatycznego jest Załącznikiem nr 2 do Regulaminu.

5. Za regularne przeglądy i konserwacje systemu informatycznego oraz nośników informacji odpowiada ASI, a wyniki przeglądu przekazuje do KJO w postaci protokołu z przeglądu.
6. Przeglądy oraz konserwacje należy przeprowadzać minimum raz w roku.
7. Przegląd zakresów uprawnień użytkowników w Systemie Jednostki i Systemach CPD Jednostki należy wykonywać minimum raz w roku.
8. Przeglądy oraz konserwacje systemu informatycznego służącego do przetwarzania danych osobowych musi być przeprowadzane w regularnych odstępach czasu.

19.2 Monitorowanie

1. Monitorowaniu podlegają wszystkie transmisje sieciowe do i z systemu informatycznego.
2. Zakres monitorowania ustala KJO w porozumieniu z ASI, który jest odpowiedzialny za odpowiednią konfigurację urządzeń i oprogramowania monitorującego.
3. System informatyczny podlega monitorowaniu w zakresie ochrony i bezpieczeństwa danych.
4. Monitorowanie Użytkownika jest prowadzone w zakresie:
   a. rejestrowania odwiedzanych stron internetowych,
   b. nadzoru nad efektywnością pracy w aplikacjach zainstalowanych na stanowisku komputerowym,
   c. automatycznej ochrony antywirusowej poczty służbowej oraz systemu operacyjnego komputera Użytkownika,
   d. automatycznej kontroli dostępu do zasobów informacyjnych sieci wewnętrznej.
5. Monitorowanie w Jednostce Organizacyjnej jest prowadzone w zakresie nie naruszającym prawa do prywatności zatrudnionych pracowników.

20 Ciągłość działania

1. Zarządzanie ciągłością działania jest kluczowym elementem dla działania organizacji. Wdraża się wszystkie możliwe i uzasadnione do zastosowania środki zapewniające dostępność Systemu Jednostki.
2. Stosuje się w szczególności zasady:
   a. konfiguracja zasobów wymagających wysokiej dostępności uwzględnia redundancję elementów, w tym dyski twarde macierzy serwerowych, karty sieciowe serwerów, hypervisory służące do wirtualizacji zasobów,
   b. w celu zachowania ciągłości działania podczas awarii zasilania, serwery powinny być podłączone do systemu zasilaczy awaryjnych UPS, system podtrzymania zasilania musi utrzymywać konieczne napięcie do czasu bezpiecznego wyłączenia urządzeń i systemów operacyjnych.
   b. W miarę możliwości kadrowych w celu zachowania ciągłość obsługi systemów stosuje się zastępstwa (np. przez drugiego ASI lub jego zastępcę).

20.2 Wykonywanie kopii zapasowych

1. ASI jest odpowiedzialny za zapewnienie sprawnego funkcjonowania procedur tworzenia, przechowywania i niszczenia kopii zapasowych danych Systemu Jednostki.
2. Kopie zapasowe danych są wykonywane według następującego harmonogramu:
   a. codziennie – kopie różnicowe lub przyrostowe baz danych oraz innych istotnych danych znajdujących się na serwerach, niezbędnych do sprawnego funkcjonowania Jednostki, po zakończeniu godzin pracy.
   b. przed każdym serwisem baz danych lub aktualizacją oprogramowania obsługujących bazy danych i systemów operacyjnych na serwerach,

c. w cyklu miesięcznym – kopia całościowa systemów operacyjnych na serwerach oraz baz danych aplikacji.

3. Szczegółowy harmonogram wykonywania kopii zapasowych jest utrzymywany przez ASI zgodnie ze wzorem z zawartym w załączniku nr 3 do Regulaminu. Wykonywane kopie zbiorów danych są przechowywane w wyznaczonych, zamkniętych i zabezpieczonych pomieszczeniach.

4. Kopie zapasowe przechowywane są w odpowiednio zabezpieczonych szafach, w odrębnych pomieszczeniach bezpiecznie oddalonych od serwera lub urządzenia, z którego kopia danych została wykonana, w szczególności podczas wyboru miejsca przechowywania kopii zapasowych należy uwzględnić wyniki analizy ryzyka.

5. Kopie zapasowe przechowywane poza budynkami i pomieszczeniami Jednostki Organizacyjnej muszą być zabezpieczone kryptograficznie algorytmem AES o długości klucza min. 128 bit lub algorytmem o podobnej skuteczności.

6. Hasło do klucza, o którym mowa powyżej, musi posiadać długość min. 16 znaków i być utworzone zgodnie z zasadami tworzenia haseł opisanymi Regulaminie.

7. Nadzór nad wykonywaniem kopii danych, ich rejestracją oraz dostępem do danych prowadzi ASI.

8. Zniszczenie nośnika kopii zapasowej musi być ewidencjonowane przez ASI z uwzględnieniem daty i opisu sposobu zniszczenia.

9. Kopie zapasowe muszą być testowane minimum raz na 6 miesięcy. Test musi pozwalać na potwierdzenie kompletności i poprawności przechowywanych danych na nośniku kopii zapasowej.

10. ASI ewidencjonuje każdorazowo przeprowadzenie testu kopii zapasowej uwzględniając następujące informacje:

    a. nazwa: [bazy danych lub danych lub systemu lub aplikacji],

    b. rodzaj nośnika kopii: taśma, dysk, udział sieciowy,

    c. rodzaj testu: pełny test lub częściowy [podanie zakresu danych],

    d. wynik testu: poprawny/niepoprawny [podanie szczegółów błędu i sposobu usunięcia błędu],

    e. imię i nazwisko osoby odpowiedzialnej za wykonanie testu kopii.

21 Reagowanie na incydenty

21.1 Terminologia

1. **Naruszenie (incydent) bezpieczeństwa informacji** – to pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań Jednostki lub Urzędu Miasta Lublin, a także zagrażają bezpieczeństwu informacji.

2. **Incydent informatyczny** – każde nieautoryzowane lub niezaakceptowane działanie powodujące straty w aktywach informacyjnych Jednostki lub Urzędu Miasta Lublin, które zostało dokonane przy użyciu urządzenia sieciowego i/lub sieci komputerowej.

3. Przykładowe naruszenia bezpieczeństwa (incydenty) wskazane są w Załączniku nr 1 do Regulaminu Bezpieczeństwa Informacji.

21.2 Reagowanie na incydenty

1. Wszystkie zaistniałe incydenty oraz problemy z zakresu bezpieczeństwa informacji należy bezzwłocznie zgłaszać do KJO oraz ASI i IOD. Zasady postępowania z incydentami związanymi z danymi osobowymi zostały określone w Polityce Bezpieczeństwa Informacji.

2. Prowadzony jest rejestr incydentów bezpieczeństwa w każdej Jednostce Organizacyjnej. Za prowadzenie rejestru odpowiada Inspektor Ochrony Danych.

3. Reakcja na incydent zależy od jego powagi, mierzonej skutkami i poziomem oddziaływania na Jednostkę Organizacyjną lub Gminę Lublin lub osoby, których dane osobowe były objęte incydentem.

4. KJO we współpracy z ASI oraz IOD podejmuje decyzję o tym, czy incydent będzie zgłoszony do BBI UML.

5. Do BBI należy zgłaszać incydenty dotyczące w szczególności:

   a. utraty ciągłości działania przez Jednostkę Organizacyjną (np. awarii serwerów lub co najmniej 3 stacji roboczych jednocześnie, atak typu ransomware, Dos, DDos, sniffing i inne),

   b. kradzież/ zagubienie dokumentów lub nośników z danymi podlegającymi ochronie,

   c. wyciek informacji chronionych,

   d. nieuprawniony przekaz danych,

   e. ujawnienie haseł lub kodów PIN,

   f. wyłudzanie, kradzież i fałszowanie haseł dostępu,

   g. przełamanie zabezpieczeń lub ich obejście,

   h. nieuprawniony dostęp do systemu od strony sieci publicznej lub bezprzewodowej,

   i. nieuprawniony dostęp do systemu od strony sieci wewnętrznej.

6. Określone w pkt 5 naruszenia bezpieczeństwa informacji należy zgłaszać do BBI drogą elektroniczną na adres incydenty.bezpieczenstwa@lublin.eu lub w formie pisemnej.

7. Osobą odpowiedzialną za zgłoszenie incydentu jest KJO.

8. Jeśli zdarzenie jest ewidentnym naruszeniem bezpieczeństwa, KJO we współpracy z IOD oraz ASI może zdecydować o natychmiastowym odebraniu upoważnień i uprawnień w systemach użytkownikowi.

9. IOD oraz ASI w porozumieniu z KJO zabezpieczają ślady (np. logi systemowe) naruszenia bezpieczeństwa. W szczególnych przypadkach KJO w we współpracy z UML informuje organy ścigania o zaistniałej sytuacji. Ostatnim etapem zamykania naruszenia bezpieczeństwa jest usunięcie skutków naruszenia bezpieczeństwa oraz wprowadzenie dodatkowych zabezpieczeń (np. zmieniając konfigurację) w porozumieniu z ASI.

10. Każdy incydent związany z naruszeniem bezpieczeństwa informacji musi być zarejestrowany w rejestrze incydentów prowadzonym w Jednostce Organizacyjnej przez IOD.

22 Domyślna ochrona i ochrona w fazie projektowania

1. Podczas tworzenia produktów, usług i aplikacji, które opierają się na przetwarzaniu danych osobowych albo przetwarzają dane osobowe w celu realizacji swojego zadania, Administrator oraz podmioty przetwarzające podczas opracowywania i projektowania biorą pod uwagę prawo do ochrony danych osobowych.

2. Wytwórcy produktów, usług i aplikacji z uwzględnieniem stanu wiedzy technicznej zapewniają Administratorowi i podmiotom przetwarzającym możliwość wywiązania się obowiązków ochrony danych osobowych.

3. Stosowanie zasad domyślnej ochrony oraz ochrony w fazie projektowania sprowadza się do stosowania zabezpieczeń organizacyjnych i technicznych adekwatnych do oszacowanego ryzyka dla projektowanych lub planowanych operacji przetwarzania, a w szczególności do stosowania:

   a. pseudonimizacji,

   b. szyfrowania,

   c. minimalizacji danych,

   d. ograniczenia do niezbędnej ilości zbieranych danych osobowych,

   e. ograniczenia do niezbędnego zakresu przetwarzania danych,

f. ograniczenia do niezbędnego okresu przechowywania danych,

g. technik zapewniających odpowiedni poziom dostępności,

h. zasady nie udostępniania danych osobowych bez interwencji danej osoby nieokreślonej liczbie osób fizycznych.

4. Zasadę uwzględniania ochrony danych w fazie projektowania i zasadę domyślnej ochrony danych należy też brać pod uwagę w zamówieniach publicznych na produkty, usługi i aplikacje, które służą do przetwarzania danych osobowych.

22.1 Zapewnianie praw osób w systemach służących do przetwarzania danych osobowych

1. Systemy informatyczne, które służą lub mają służyć do przetwarzania danych osobowych, powinny zapewnić minimalne wymagania funkcjonalne wynikające z RODO.

2. W trakcie eksploatacji systemów oraz w fazie ich projektowania lub zamawiania należy zapewnić poniższe funkcje:

a. Możliwość eksportu danych do pliku w formacie nadającym się do odczytu maszynowego w przypadku wniosku o przeniesienie danych pomiędzy administratorami danych.

b. Funkcja wygenerowania w postaci raportu, który powinien zawierać kopie danych osobowych dot. podmiotu danych.

c. Możliwość oznaczenia przechowywanych danych osobowych w celu ograniczenia przetwarzania.

d. Odnotowanie informacji i jej zakresu o udostępnieniu danych podmiotu odbiorcom.

e. Rozwiązanie techniczne lub organizacyjne pozwalające wyrażenie, odnotowanie i cofniecie zgody na przetwarzanie danych.

f. Mechanizm retencji danych.

g. Granularne usuwanie danych osobowych pojedynczych podmiotów danych z systemu.

h. Szyfrowanie lub pseudonimizacja danych.

i. Odnotowywanie anomalii w zachowaniu użytkowników w celu zbierania i raportowania o zdarzeń mogących świadczyć o próbie naruszenia lub faktycznym naruszeniu bezpieczeństwa danych osobowych.

j. Rejestrowanie czynności przetwarzania użytkowników w logach w zakresie adekwatnym do ryzyka oszacowanego dla danych osobowych w systemie.

22.2 Ocena skutków

W przypadku, gdy planowane jest wdrożenie systemu służącego do przetwarzania danych osobowych, lub w sytuacji, gdy planowane jest wprowadzenie istotnej zmiany w eksploatowanym systemie, ASI w porozumieniu z KJO określa, czy niezbędne jest dokonanie oceny skutków dla ochrony danych osobowych przetwarzanych w systemie.

2. Dokonanie oceny skutków jest realizowane zgodnie z art. 35 RODO oraz Polityką Bezpieczeństwa Informacji Jednostki Organizacyjnej Gminy Lublin.

23 Bezpieczeństwo fizyczne i środowiskowe Systemu Jednostki Organizacyjnej

1. Przetwarzanie danych w Systemie Jednostki Organizacyjnej może być prowadzone wyłącznie w pomieszczeniach odpowiednio zabezpieczonych przed nieuprawnionym dostępem, uszkodzeniem bądź zniszczeniem sprzętu i danych Systemu Jednostki Organizacyjnej.

2. Zabezpieczenia w pomieszczeniach pracowniczych musi spełniać minimalne wymagania wymienione poniżej:

b. Drzwi do pomieszczenia zwykłe – nie przeciwpożarowe, nie antywłamaniowe.

c. Zamki w drzwiach do pomieszczenia zwykłe – nie antywłamaniowy.

d. Pomieszczenia zabezpieczone są przed skutkami pożaru za pomocą wolnostojącej gaśnicy zgodnie z obowiązującymi przepisami PPOŻ.

e. Szafki przeznaczone na nośniki z danymi niemetalowe, zamykane na zamki zwykłe.

4. Szafki przeznaczone na nośniki z danymi osobowymi o solidnej konstrukcji zamykane na klucz lub szafy metalowe bądź w sejfy, w przypadku, gdy wskazuje na to wynik szacowania ryzyka.
5. Zabezpieczenia w pomieszczeniu serwerowni muszą spełniać minimalne wymagania wymienione poniżej.
   a. drzwi antywłamaniowe i przeciwpożarowe, jeżeli wyniki szacowania ryzyka wskazują na takie zabezpieczenie,
   b. system alarmowy przeciwwłamaniowy,
   c. prowadzona jest ewidencja wejść i wyjść osób nie będących Informatykami,
   d. czujnik temperatury z możliwością automatycznego zapisywania mierzonych wartości i alarmowania,
   e. zalecana redundantna klimatyzacja dedykowana do pracy ciągłej w pomieszczeniach technicznych,
   f. klimatyzacja o mocy dopasowanej do ilości energii cieplnej wypromieniowywanej przez urządzenia znajdujące się w pomieszczeniu,
   g. czujnik dymu wraz z możliwością alarmowania,
   h. czujnik wilgoci wraz z możliwością alarmowania,
   i. gaśnica w pomieszczeniu spełniająca wymagania gaszenia urządzeń elektrycznych,
   j. ograniczenie dostępu do pomieszczenia tylko dla upoważnionych przez KJO pracowników,
   k. żaluzje/rolety przeciwsłoneczne w oknach,
   l. zamykane na klucz metalowe szafy teleinformatyczne przeznaczone dla urządzeń pracujących w serwerowni,
   m. jeżeli pomieszczenie jest zlokalizowane na parterze zaleca się umieszczenie krat/rolet antywłamaniowych w oknach.
   n. zabezpieczenia w punkcie dystrybucyjnym powinny spełniać minimalne wymagania wymienione poniżej,
   o. zamykane na klucz szafki lub szafy teleinformatyczne przeznaczone dla urządzeń pracujących w pomieszczeniu.
6. Osoby postronne przebywające w pomieszczeniach ze sprzętem lub nośnikami danych i wykonujące prace z urządzeniami Systemu Teleinformatycznego powinny znajdować się pod nadzorem osób upoważnionych do dostępu do tych urządzeń.

24 Postanowienia końcowe

Za nadzór nad przestrzeganiem postanowień Regulaminu odpowiada:

a. ze strony Jednostki Organizacyjnej Gminy Lublin uprawniony przedstawiciel Jednostki Organizacyjnej,

b. ze strony Urzędu Miasta Lublin BBI UML oraz WI.

25 Dokumenty związane

1. Polityka Bezpieczeństwa Informacji Jednostki Organizacyjnej Gminy Lublin
2. Regulamin Bezpieczeństwa Informacji Jednostki Organizacyjnej Gminy Lublin

26 Załączniki

Załącznik nr 1 – Wzór wniosku o nadanie/modyfikację/uprawnień w systemach CPD UML

Załącznik nr 2 – Wzór protokołu z przeglądu/konserwacji systemu informatycznego służącego do przetwarzania danych.

Załącznik nr 3 – Wzór harmonogramu kopii zapasowych.

Załącznik nr 4 – Regulamin korzystania z systemu hostingowego

Załącznik nr 1 - Wzór wniosku o nadanie/modyfikację/uprawnień do systemów CPD UML

Wnioskujący: (określenie Jednostki oraz osoby wnioskującej).....

Adres e-mail oraz tel. Kontaktowy Wnioskującego:.....

System (aplikacja), w której dane będą przetwarzane:

.....

Typ zgłoszenia (należy zaznaczyć):

- ☐ Nadanie uprawnień
- ☐ Modyfikacja uprawnień
- ☐ Odebranie uprawnień

Informacje o użytkowniku:

Imię: .....

Nazwisko: .....

PESEL:.....

Rodzaj użytkownika (należy zaznaczyć):

- ☐ Pracownik (nazwa stanowiska np. księgowa, kadrowa, intendent, sekretarka .....)
- ☐ Stażysta
- ☐ Wolontariusz
- ☐ Praktykant
- ☐ Osoba, z którą zawarto umowę cywilnoprawną
- ☐ Pracownik podmiotu zewnętrznego
- ☐ Inne .....

Uzasadnienie (w przypadku wnioskowania o nadanie uprawnień dla podmiotu zewnętrznego lub innego):

.....
.....
.....
.....
.....

Zakres uprawnień do systemów (określenie np. modułu w systemie, czy ma być to przeglądanie danych czy modyfikacja danych)

.....
.....
.....
.....

Uwagi:

.....
.....
.....
.....

Podpis wnioskującego:

Załącznik nr 2 - Wzór protokołu z przeglądu/ konserwacji systemu informatycznego służącego do przetwarzania danych osobowych

Protokół z przeglądu/konserwacji* systemu informatycznego służącego do przetwarzania danych osobowych

W dniu ..... przeprowadzone zostały następujące prace z zakresu przeglądu/konserwacji systemu informatycznego

.....

.....

.....

.....

.....

.....

.....

Wykaz materiałów i urządzeń

.....

.....

.....

.....

.....

.....

Wykaz nieprawidłowości w działaniu systemu i stanie nośników informacji

.....

.....

.....

.....

.....

.....

.....

.....

.....

Osoba odbierająca prace

Wykonawca

Serwer/Usługa	Rodzaj	Typ kopii	Wyzwalacz	Nazwa skryptu/profilu	Zakres kopii	Źródło kopii	Nośnik docelowy kopii	Nazwa docelowa archiwum/pliku kopii	Czas przechowywania	Czas rozpoczęcia	Miejsce przechowywania nośnika kopii	Przewidywany rozmiar	Uwagi
1	2	3	4	5	6	7	8	9	10	11	12	13	14

Załącznik nr 4 - Regulamin korzystania z systemu hostingowego

Postanowienia ogólne

1. System hostingowy Urzędu Miasta Lublin jest systemem przeznaczonym do obsługi stron internetowych, kont pocztowych oraz domen.
2. Administratorem systemu hostingowego jest Wydział Informatyki i Telekomunikacji.
3. Administratorami poszczególnych kont hostingowych są właściwe jednostki organizacyjne.

Uzyskanie dostępu do systemu hostingowego

1. Użytkownik uzyskuje dostęp do systemu na podstawie pisemnego wniosku zweryfikowanego i zaakceptowanego przez Dyrektora Wydziału Informatyki i Telekomunikacji.
2. O dostęp do systemu dla użytkownika wnioskuje kierownik komórki lub jednostki organizacyjnej.
3. Wniosek musi zawierać:
4. imię i nazwisko użytkownika uzyskującego dostęp;
5. komórkę organizacyjną użytkownika;
6. uzasadnienie celowości dostępu do systemu przez użytkownika;
7. wskazanie charakteru i szacowanej ilości danych;
8. wnioskowaną domene w lublin.eu
9. Wniosek może zostać przesłany za pośrednictwem systemu obiegu spraw i dokumentów Mdok lub system ePUAP.
10. Po nadaniu uprawnień przez Wydział Informatyki i Telekomunikacji, użytkownik uzyskuje dostęp do systemu za pomocą indywidualnej nazwy użytkownika i hasła.

Treści i strony internetowe

1. System służy wyłącznie do celów bezpośrednio związanych z celami i zadaniami jednostki, mogą w nim być przechowywane i udostępniane wyłącznie materiały związane z funkcjonowaniem ww. jednostki organizacyjnej.
2. Zabrania się umieszczania w systemie treści mogących w jakikolwiek sposób naruszyć dobra osobiste osób trzecich, w szczególności treści obraźliwych oraz innych naruszających dobre obyczaje.
3. Materiały zamieszczane przez użytkownika w systemie muszą być zgodne z prawem, w szczególności nie mogą naruszać ustawy o prawie autorskim i prawach pokrewnych.
4. Za legalność umieszczanych treści odpowiada osoba zamieszczająca.

5. Administrator systemu zastrzega sobie prawo do natychmiastowego zablokowania konta użytkownika, strony użytkownika lub poszczególnych kont email, w przypadku złamania zasad wynikających z niniejszego Regulaminu lub w przypadku wykrycia innych naruszeń w szczególności zagrażających bezpieczeństwu systemu.

6. W przypadku wykrycia ataku skutkującego przełamaniem zabezpieczeń, w szczególności:

   a) podmiana strony internetowej, treści strony,
   b) zamieszczenie strony lub innych treści phishingowych,
   c) rozsyłanie spamu, masowego mailingu,
   d) stwierdzeniu udostępnienia konta osobom nieupoważnionym,

   administrator blokuje działanie strony, konta/kont pocztowych wykorzystywanych do ww. działań, oraz informuje o ww. fakcie osobę wskazaną do kontaktu we właściwej jednostce organizacyjnej.

7. W przypadku stwierdzenia występowania luk bezpieczeństwa w oprogramowaniu mogącym spowodować infekcję lub inne naruszenie bezpieczeństwa, Administrator zastrzega możliwość zablokowania strony, do czasu usunięcia luk bezpieczeństwa. Po blokadzie Administrator informuje o ww. fakcie użytkownika.

Zalecenia techniczne

1. Rekomenduje się stosowanie responsywnych stron internetowych (RWD), przyjaznych dla urządzeń mobilnych.

2. Zamieszczane materiały powinny być zoptymalizowane pod względem formatu i rozdzielczości, stosownie do celu ich wykorzystania (np. prezentacja, druk).

3. Rekomendowane jest bieżące aktualizowanie oprogramowania.

4. Rekomendowane jest stosowanie jak najwyższej aktualnie wspieranej wersji PHP.