POLITYKA ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI

URZĘDU MIASTA RYBNIKA

WYCIĄG

2018

WSTĘP

Polityka Zarządzania Bezpieczeństwem Informacji Urzędu Miasta Rybnika została opracowana na zlecenie Administratora danych w celu spełnienia wymagań określonych:

a) ogólnym rozporządzeniem 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, zwanym dalej RODO,
b) wewnętrznymi przepisami krajowymi w zakresie ochrony danych osobowych.

CZĘŚĆ I

INFORMACJE OGÓLNE.

Polityka Zarządzania Bezpieczeństwem Informacji, zwana dalej Polityką lub PZBI, powstała w związku z wykorzystywaniem:

- danych osobowych w rozumieniu RODO,
- innych, niż dane osobowe, danych (informacji) podlegających ochronie,
- technologii informatycznych do realizacji zadań statutowych Urzędu Miasta.

Niniejszy dokument stanowi najwyższej rangi dokument polityki zarządzania bezpieczeństwem informacji, w tym przede wszystkim danych osobowych, przetwarzanych w systemach informatycznym i tradycyjnym wykorzystywanych w Urzędzie Miasta Rybnika oraz jest on wiążący dla pracowników wszystkich komórek organizacji wewnętrznej Urzędu Miasta, stażystów, praktykantów, wolontariuszy i radnych Rady Miasta Rybnika (zwanych dalej radnymi) korzystających z tych systemów oraz innych podmiotów (stron trzecich) mających do nich dostęp na podstawie odrębnych umów, określających zasady korzystania z tych systemów.
Na Politykę Zarządzania Bezpieczeństwem Informacji składają się: Polityka Bezpieczeństwa Informacji i Instrukcja Zarządzania Systemem Informatycznym.

Informacje niejawne nie zostały objęte zapisami niniejszego dokumentu. Zasady ochrony informacji niejawnych reguluje ustawa o ochronie informacji niejawnych oraz opracowane na jej podstawie wewnętrzne regulacje Urzędu.

CZĘŚĆ II

POLITYKA BEZPIECZEŃSTWA INFORMACJI

§ 1.
PODSTAWOWE DEFINICJE.

1. **ADMINISTRATOR DANYCH (AD)** - Prezydent Miasta Rybnika, właściciel i administrator zasobów danych osobowych i innych danych (w tym również tych, które zostały mu powierzone) przetwarzanych w Urzędzie Miasta Rybnika, decydujący o celach i środkach przetwarzania danych.
2. **ANONIMIZACJA DANYCH** - proces polegający na przekształceniu danych osobowych w sposób uniemożliwiający przyporządkowanie poszczególnych informacji

osobistych lub rzeczowych do określonej bądź możliwej do zidentyfikowania osoby fizycznej.

3. **BEZPIECZEŃSTWO INFORMACJI** – oznacza zachowanie poufności, integralności, dostępności informacji, a także jej autentyczności, rozliczalności, niezaprzeczalności, niezawodności. Informacje podlegające ochronie zabezpiecza się przed nieautoryzowanym dostępem, zmianą, utratą, uszkodzeniem, zniszczeniem lub zatajeniem.
4. **DOSTĘPNOŚĆ INFORMACJI** – oznacza, że osoby upoważnione mają dostęp do informacji i związanych z nią aktywów wtedy, gdy istnieje taka potrzeba (zapewnienie dostępu do danych, w każdym momencie żądanym przez użytkownika).
5. **ESOD** – elektroniczny system obiegu dokumentów funkcjonujący w Urzędzie Miasta Rybnika.
6. **HASŁO** – ciąg znaków znanych jedynie osobie posiadającej uprawnienia do pracy w systemie informatycznym służący, w połączeniu z identyfikatorem użytkownika, do uwierzytelnienia użytkownika w systemie informatycznym.
7. **IDENTYFIKATOR UŻYTKOWNIKA** – ciąg znaków jednoznacznie identyfikujący użytkownika systemu.
8. **INCYDENT BEZPIECZEŃSTWA INFORMACJI** – naruszenie bezpieczeństwa informacji przetwarzanej w Urzędzie Miasta ze względu na poufność, dostępność i integralność,
9. **INFORMACJE (DANE)** – to wszystko, co posiada logiczne znaczenie jako przekaz treści i nadaje się do praktycznego wykorzystania w procesach, skutkując osiągnięciem celu. Informacja może być przetwarzana na różnych typach nośników (m.in. papierowych, magnetycznych, optycznych itp.), w szczególności w systemach informatycznych.
10. **INSPEKTOR OCHRONY DANYCH (IOD) –** pracownik wyznaczony przez Administratora danych do nadzorowania i zapewnienia przestrzegania przepisów o ochronie danych osobowych, powoływany odrębnym Zarządzeniem Prezydenta Miasta.
11. **INTEGRALNOŚĆ INFORMACJI** – oznacza, że informacje są kompletne i dokładne oraz że są przetwarzane w kontrolowany sposób (uniknięcie nieautoryzowanych zmian w danych).
12. **JEDNOSTKA** – oznacza jednostkę organizacji wewnętrznej Urzędu, o której mowa w Regulaminie Organizacyjnym Urzędu Miasta Rybnika.
13. **KONTO UŻYTKOWNIKA SYSTEMU** – przestrzeń w systemie informatycznym przypisana konkretnemu użytkownikowi i opatrzona hasłem. Nazwę konta użytkownika stanowi identyfikator użytkownika.
14. **MIASTO** – Miasto Rybnik.
15. **NACZELNIK** – osoba kierująca jednostką organizacji wewnętrznej Urzędu lub osoba pełniąca samodzielne stanowisko kierownicze w Urzędzie.
16. **OSOBA TRZECIA** – każda osoba (podmiot) niebędąca pracownikiem Urzędu Miasta Rybnika, radnym, praktykantem, wolontariuszem bądź stażystą, która podejmuje z Urzędem Miasta współpracę na podstawie innej niż umowa o pracę (w tym m.in. umowa cywilnoprawna) i / lub prowadzi działania w imieniu i na rzecz Urzędu Miasta Rybnika.
17. **PODSTAWOWE ZASADY BEZPIECZEŃSTWA INFORMACJI I PRZETWARZANIA DANYCH OSOBOWYCH** – zbiór zasad opisanych w § 3 ust. 5.
18. **POUFNOŚĆ INFORMACJI** – oznacza, że dostęp do informacji mają tylko osoby upoważnione (uniemożliwienie dostępu do danych osobom postronnym).
19. **PRACOWNIK** – osoba zatrudniona przez Urząd Miasta Rybnika na podstawie umowy o pracę.
20. **PRAKTYKANT** - osoba niebędąca pracownikiem urzędu, odbywająca praktykę w Urzędzie Miasta Rybnika.

21. **PSEUDONIMIZACJA** - działanie ograniczające możliwości tworzenia powiązań danych osobowych z prawdziwą tożsamością osoby, której dane dotyczą. Pseudonimizacja polega na zastępowaniu w zapisie jednego atrybutu (z reguły atrybutu nietypowego) innym atrybutem.
22. **PZBI** – Polityka Zarządzania Bezpieczeństwem Informacji.
23. **STAŻYSTA** – osoba niebędąca pracownikiem urzędu, odbywająca staż w Urzędzie Miasta Rybnika.
24. **SYSTEM –** system przetwarzania (informacji) – zespół określonych komponentów fizycznych i logicznych, współpracujących ze sobą według określonych reguł, służący do przetwarzania informacji; system składa się z systemu informatycznego i systemu tradycyjnego.
25. **SYSTEM INFORMATYCZNY** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowanych zastosowanych w celu przetwarzania danych.
26. **SYSTEM TRADYCYJNY** – system przetwarzania informacji w postaci papierowej np. archiwum papierowe, kartoteka.
27. **URZĄD** – Urząd Miasta Rybnika.
28. **UODO** – Urząd Ochrony Danych Osobowych.
29. **UŻYTKOWNIK SYSTEMU** – osoba upoważniona do przetwarzania danych w systemie informatycznym, której utworzono konto użytkownika systemu.
30. **ZASÓB** - zespół aktywów mających wartość dla organizacji. Do zasobów zalicza się w szczególności: ludzi, budynki, oprogramowanie, zbiory elektroniczne i tradycyjne, sprzęt służący do przetwarzania danych, strony internetowe, dokumentację bezpieczeństwa.

§ 2.
PODSTAWOWE ZASADY BEZPIECZEŃSTWA INFORMACJI I PRZETWARZANIA DANYCH OSOBOWYCH.

1. Każdy, kto przetwarza informacje Urzędu zobowiązany jest do stosowania niżej opisanych zasad bezpieczeństwa.
2. Każdy przetwarzający dane osobowe posiada upoważnienie AD do przetwarzania danych osobowych. Zabrania się przetwarzania danych osobowych bez ważnego upoważnienia.
3. Podstawowe zasady bezpieczeństwa informacji i przetwarzania danych osobowych:
   1) **ZASADA WIEDZY KONIECZNEJ** - dostęp do informacji ograniczony jest do tych, które są niezbędne do prawidłowego wykonywania obowiązków na danym stanowisku. Za przestrzeganie tej zasady odpowiedzialni są kierownicy.
   2) **ZASADA ŚWIADOMOŚCI ZBIOROWEJ –** wszyscy są świadomi konieczności ochrony zasobów, zapewnienia ich dostępności, poufności, integralności i aktywnie w tym procesie uczestniczą.
   3) **ZASADA ŚWIADOMEJ KONWERSACJI –** polega na tym, że nie zawsze i wszędzie trzeba mówić co się wie, ale zawsze i wszędzie trzeba wiedzieć co, gdzie i do kogo się mówi.
   4) **ZASADA ODPOWIEDZIALNOŚCI ZA ZASOBY** – każdy, kto przetwarza informacje jest odpowiedzialny za zapewnienie ich dostępności, poufności i integralności poprzez przestrzeganie procedur ich bezpiecznego przetwarzania oraz ochronę przyznanych zasobów, w tym za szkody wyrządzone w systemie informatycznym przez nieautoryzowane oprogramowanie lub niewłaściwe korzystanie z urządzeń systemu informatycznego.
   5) **ZASADA CHRONIONEGO POMIESZCZENIA** – wyraża się tym, że pod nieobecność osoby uprawnionej w pomieszczeniach (poza ogólnodostępnymi typu korytarze) nie mogą przebywać osoby postronne, po opuszczeniu pomieszczenia osoba odpowiedzialna zamyka je na klucz (bez pozostawiania kluczy w zamkach – wyjątek stanowi

ewakuacja), szczegółowe zasady ochrony pomieszczeń zostały zawarte w „Zasadach ochrony Urzędu Miasta Rybnika" przyjętych Zarządzeniem Prezydenta Miasta.

6) **ZASADA NADZOROWANIA KLUCZY –** pobrane klucze do pomieszczeń powinny być w każdym czasie pod kontrolą; zasady pobierania i zdawania kluczy zawarto w „Zasadach ochrony Urzędu Miasta Rybnika" przyjętych Zarządzeniem Prezydenta Miasta. Ponadto pracownicy odpowiedzialni są za należyte zabezpieczenie kluczy do ich biurek stanowiskowych oraz szaf biurowych, w których przechowywane są dokumenty; ostatni pracownik opuszczający dane pomieszczenie po zakończeniu pracy zamyka szafy i chowa klucze w bezpieczne, ustalone z pozostałymi współpracownikami miejsce.
7) **ZASADA CZYSTEGO BIURKA** – wyraża się tym, że zarówno dokumentów papierowych, jak i jakichkolwiek innych nośników informacji (płyt CD, DVD, pamięci flash, USB itp.), nie pozostawia się bez nadzoru.
8) **ZASADA CZYSTEGO EKRANU** – każdorazowe opuszczenie pomieszczenia w godzinach pracy powinno zostać poprzedzone zablokowaniem komputera. Każdy użytkownik systemu zobowiązany jest zadbać, aby po zakończeniu pracy sprzęt został poprawnie wyłączony.
9) **ZASADA CZYSTEGO KOMPUTERA** – osoby korzystające z komputerów przenośnych wypożyczonych z Wydziału Informatyki zobowiązane są po zakończeniu na nich pracy usunąć wszystkie skopiowane bądź utworzone na nich informacje.
10) **ZASADA CZYSTEJ DRUKARKI** – wszyscy pracownicy, praktykanci i stażyści zobowiązani są do zabierania dokumentów z drukarek zaraz po ich wydrukowaniu (dotyczy to zwłaszcza drukarek usytuowanych w miejscach ogólnie dostępnych).
11) **ZASADA CZYSTEGO KOSZA** – nieprzydatne dokumenty, brudnopisy, zbędne kopie muszą zostać trwale zniszczone w sposób uniemożliwiający odtworzenie zawartych w nich informacji. Zasada ta dotyczy również informacji zapisanych w innej niż papierowa formie – na nośnikach elektronicznych. Do kosza na śmieci nie wyrzuca się płyt CD/DVD oraz innych nośników, powinny one zostać zniszczone w specjalistycznych niszczarkach. W przypadku, gdy będzie to niemożliwe nośniki te należy przekazać do Wydziału Informatyki celem ich utylizacji.
12) **ZASADA CZYSTEJ TABLICY** – w przypadku korzystania z tablic w salach ogólnodostępnych osoba organizująca spotkanie musi uprzątnąć wszystkie pozostałe tam materiały i wyczyścić tablice; pracownicy korzystający z tablic w biurach zobowiązani są do nie zamieszczania na tablicach informacji podlegających ochronie.
13) **ZASADA LEGALNOŚCI OPROGRAMOWANIA** – zabrania się samodzielnego instalowania oprogramowania, a także przechowywania na komputerach treści naruszających prawo.
14) **ZASADA WERYFIKACJI PRZENOŚNYCH NOŚNIKÓW DANYCH** (np. pendrive, CD, DVD) – każdy komputer wymusza przeprowadzenie skanowania przez system antywirusowy zewnętrznych nośników danych przed ich uruchomieniem. W Urzędzie dopuszczalne jest stosowanie tylko i wyłącznie zaszyfrowanych zewnętrznych nośników danych stanowiących własność Urzędu.
15) **ZASADY ZGŁASZANIA INCYDENTÓW NARUSZENIA BEZPIECZEŃSTWA INFORMACJI ORAZ ZAGROŻEŃ PRAWIDŁOWEJ REALIZACJI ZAŁOŻEŃ PZBI** – każdy użytkownik systemu zobowiązany jest do zgłaszania wszelkich zauważonych incydentów; zasady te zawarte są w PZBI.
16) **ZASADA MONITORINGU** – każde stanowisko komputerowe może zostać objęte monitorowaniem działania użytkowników i oprogramowania.
17) **ZASADA ZGODNOŚCI Z PRAWEM, RZETELNOŚCI I PRZEJRZYSTOŚCI** – dane powinny być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dotyczą.

18) **ZASADA OGRANICZENIA CELU** – dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane, za niezgodne z pierwotnymi celami.
19) **ZASADA MINIMALIZACJI DANYCH** – zebrane dane muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane.
20) **ZASADA PRAWIDŁOWOŚCI** – dane muszą być prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały usunięte lub sprostowane.
21) **ZASADA OGRANICZENIA PRZECHOWYWANIA** – dane muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, de celów badań naukowych lub historycznych lub do celów statystycznych z zastrzeżeniem że wdrożone zostają odpowiednie środki techniczne i organizacyjne wymagane na podstawie tego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą.
22) **ZASADA INTEGRALNOŚCI I POUFNOŚCI** – dane osobowe muszą być przetwarzane w sposób zapewniający odpowiednie ich bezpieczeństwo, w tym ochronę przed niedozwolonym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.
23) **ZASADA ROZLICZALNOŚCI** – Administrator jest odpowiedzialny za przestrzeganie podstawowych zasad przetwarzania danych osobowych, zawartych i musi być w stanie wykazać ich przestrzeganie.

4. Poza podstawowymi zasadami bezpieczeństwa informacji i przetwarzania danych osobowych należy stosować reguły opisane w „Zasadach ochrony Urzędu Miasta Rybnika” przyjętych Zarządzeniem Prezydenta Miasta.
5. Za monitorowanie przestrzegania zasad PZBI odpowiada IOD.

§ 3.
OGÓLNE CELE I ZAKRES ORAZ ZNACZENIE BEZPIECZEŃSTWA JAKO MECHANIZMU UMOŻLIWIAJĄCEGO WSPÓŁUŻYTKOWANIE INFORMACJI.

Celem zapewnienia bezpieczeństwa informacji jest w szczególności:
1. ochrona zasobów informacji,
2. zapewnienie ciągłości działania Urzędu i sprawnej obsługi jego klientów i partnerów,
3. zgodność procesu przetwarzania informacji z przepisami prawa,
4. ochrona wizerunku Urzędu.

Spełnienie powyższych celów poprzez zachowanie poufności, integralności, dostępności, rozliczalności, autentyczności, niezaprzeczalności danych w ramach PZBI umożliwia współużytkowanie informacji.

§ 4.

OŚWIADCZENIE O INTENCJACH KIEROWNICTWA POTWIERDZAJĄCE CELE I ZASADY BEZPIECZEŃSTWA INFORMACJI.

Prezydent Miasta, jako Administrator danych, mając świadomość potrzeby ochrony informacji przetwarzanych w Urzędzie, która wynika nie tylko z przepisów prawa, ale również z konieczności zapewnienia sprawnej i bezpiecznej realizacji usług i zadań publicznych oraz dbałości o wizerunek Urzędu, deklaruje zaangażowanie w tworzenie odpowiednich warunków organizacyjnych i technicznych i zapewnienie zasobów niezbędnych do osiągnięcia celów wynikających z PZBI. Wszelkie przetwarzanie danych osobowych powinno być zgodne z prawem i rzetelne. Dane osobowe powinny być adekwatne, stosowne i ograniczone do tego, co niezbędne do celów, dla których są one przetwarzane. Okres przechowywania danych powinien ograniczyć się do ścisłego minimum.
Urząd chroni zarówno dane osobowe oraz informacje własne jak i powierzone. Założenie to jest podstawą do wszystkich dalszych regulacji.
Wszystkie zagadnienia związane z przetwarzaniem i przechowywaniem informacji w Urzędzie podlegają uregulowaniom zawartym w PZBI. Działania niezgodne z PZBI są bezwzględnie zakazane i pociągają za sobą skutki dyscyplinarne lub finansowe.

PZBI jest w sposób ciągły aktualizowana tak, aby jej postanowienia odzwierciedlały zmiany prawa, bieżące wymogi techniczne jak i zmieniające się realia pracy Urzędu.

§ 5. (...)
§ 6. (...)
§ 7. (...)
§ 8. (...)
§ 9. (...)
§ 10. (...)

§ 11.

TRANSGRANICZNY PRZEPŁYW DANYCH OSOBOWYCH W UNII EUROPEJSKIEJ ORAZ ICH PRZEKAZYWANIE DO PAŃSTW TRZECICH.

Przekazywanie danych osobowych do innych państw członkowskich Unii musi odbywać się zgodnie z wymogami prawa. W przypadku konieczności przekazywania danych do państwa trzeciego każdorazowo musi zostać uzyskana opinia IOD i Naczelnika Wydziału Informatyki oraz zgoda Administratora danych na przekazanie danych pod warunkiem wcześniejszego uzyskania informacji niezbędnych do bezpiecznego przekazania danych.

§ 12. (...)
§ 13. (...)
§ 14. (...)
§ 15.

(...)

14. W Urzędzie dopuszczalny jest zdalny dostęp do zasobów sieci wewnętrznej systemu informatycznego tylko i wyłącznie w celach:
    a) administracyjnych – dotyczy to pracowników Wydziału Informatyki, którzy realizują swoje zadania,
    b) realizacji umów – dotyczy to upoważnionych pracowników firm zewnętrznych.
15. Warunki korzystania ze zdalnego dostępu zostały określone w odrębnej procedurze pn. „Zdalny dostęp” stanowiącej załącznik nr 10 do PZBI.

(...)

§ 16.
INFORMACJE O ZALECANYCH ZAPISACH W UMOWACH SERWISOWYCH PODPISYWANYCH ZE STRONAMI TRZECIMI GWARANTUJĄCYCH ODPOWIEDNI POZIOM BEZPIECZEŃSTWA INFORMACJI.

Aby zapewnić maksymalne bezpieczeństwo informacji oraz spójność stosowanych rozwiązań, umowy dotyczące systemu teleinformatycznego, sprzętu, oprogramowania czy dostępu do danych chronionych zawierane z osobami trzecimi powinny być akceptowane przez IOD lub osobę przez niego wyznaczoną. Wzorcowe zapisy do specyfikacji przedmiotu zamówienia i umów zawarto w załączniku nr 9 do PZBI.

§ 17.
UMOWY POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH. WSPÓŁADMINISTROWANIE PRZETWARZANIA.

W celu zapewnienia zgodności przetwarzania danych z zapisami wynikającymi z przepisów prawa w zakresie ochrony danych osobowych stosuje się umowę powierzenia przetwarzania danych osobowych, której wzór stanowi załącznik nr 11 do PZBI.

§ 18.
PODSTAWY PRZETWARZANIA DANYCH OSOBOWYCH

Aby przetwarzanie danych osobowych było zgodne z prawem, powinno się odbywać na podstawie zgody osoby, której dane dotyczą, lub na innej uzasadnionej podstawie przewidzianej prawem. W przypadku przetwarzania danych osobowych wynikającego z realizacji ustawowych zadań nie ma konieczności odbierania zgód na ich przetwarzanie.
Zarządzający zasobami są zobowiązani do uzyskania pisemnej zgody na przetwarzanie danych osobowych od osób, których dane osobowe będą przetwarzane w związku z realizacją wszelkich zadań wykraczających poza nakazane prawem zadań (np. konsultacje, spotkania, wydarzenia o charakterze promocyjnym, itp.). Zgoda na przetwarzanie danych osobowych może zostać pisemnie wycofana przy czym wycofanie zgody nie przekreśla legalności przetwarzania danych przed ich wycofaniem.
Wzór ramowy zgody na przetwarzanie danych osobowych stanowi załącznik nr 12 do PZBI.

§ 19.
OBOWIĄZEK INFORMACYJNY.

W celu spełnienia obowiązku informacyjnego opracowano wzór ramowy obowiązku informacyjnego stanowiący załącznik nr 13 do PZBI.

§ 20. (...)
§ 21. (...)
§ 22. (...)
§ 23. (...)
§ 24. (...)
§ 25. (...)
§ 26. (...)
§ 27. (...)
§ 28. (...)
§ 29. (...)
§ 30. (...)
§ 31. (...)

ZAŁĄCZNIKI DO PZBI.

Integralną częścią Wyciągu z PZBI są opisane w jej treści niżej wyszczególnione załączniki:
Wzór ramowy zgody na przetwarzanie danych osobowych;

załącznik nr 1: (...);
załącznik nr 2: (...);
załącznik nr 3: (...);
załącznik nr 4: (...);
załącznik nr 5: (...);
załącznik nr 6: (...);
załącznik nr 7: (...);
załącznik nr 8: (...);
załącznik nr 9: (...);
załącznik nr 10: Zdalny dostęp;
załącznik nr 11: (...);
załącznik nr 12: (...);
załącznik nr 13: (...);
załącznik nr 14: (...).

Załącznik nr 10 do PZBI

Procedura

„Zdalny dostęp”

1. Cel

Dostęp zdalny do zasobów sieci wewnętrznej Urzędu Miasta Rybnika (UM) wykorzystywany jest w celu skrócenia czasu reakcji na awarie i obniżenia kosztów realizacji podpisanych umów. Przydzielany jest na potrzeby:

1) administracyjne – dla pracowników Wydziału Informatyki realizujących swoje zadania,
2) realizacji podpisanych umów - dla pracowników wybranych firm zewnętrznych.

2. Warunki ogólne realizacji usługi zdalnego dostępu

1) Użytkownicy usługi zdalnego dostępu (Użytkownicy) przed uruchomieniem usługi muszą uzyskać zgodę Naczelnika Wydziału Informatyki i akceptację Inspektora Ochrony Danych (IOD) zgodnie z opisanymi niżej procedurami.
2) Rozwiązanie techniczne udostępnienia zdalnego dostępu nie może obniżać znacząco poziomu bezpieczeństwa sieci UM i przetwarzanych tam danych.
3) Szczególnie należy zadbać o ograniczenie i ochronę dostępu z zewnątrz do konsoli zarządzania systemu zabezpieczeń (firewall, routery, ISA, kontrolery domeny).
4) Zdalny dostęp musi umożliwiać identyfikację:
   - osoby nawiązującej zdalne połączenie,
   - czasu dostępności ww. usługi,
   - zasobów, które zostaną udostępnione poprzez zdalny dostęp.

3. Procedura uzyskania zdalnego dostępu przez pracowników Wydziału Informatyki

1) Pracownik Wydziału Informatyki przygotowuje wniosek o nadanie uprawnień do ww. usługi.
2) Naczelnik Wydziału Informatyki po pozytywnym rozpatrzeniu wniosku uzyskuje akceptację IOD dla udostępnienia ww. usługi.
3) Po akceptacji ze strony IOD Administrator zdalnego dostępu generuje certyfikat i konfiguruje usługę dostępu zgodnie z wnioskiem.
4) Pracownik posiadający uprawnienie zdalnego dostępu jest zobowiązany do kontroli ważności wydanego certyfikatu i jego odnowienia w celu zapewnienia ciągłości działania ww. usługi.

4. Procedura uzyskania zdalnego dostępu przez pracowników firm zewnętrznych

1) Pracownik wydziału merytorycznego przekazuje Naczelnikowi Wydziału Informatyki wzór umowy i opis przedmiotu zamówienia w celu określenia warunków technicznych korzystania z usługi zdalnego dostępu dla pracowników przyszłego Wykonawcy.
2) Opis przedmiotu zamówienia oraz wzór umowy wymaga ostatecznej akceptacji Naczelnika Wydziału Informatyki oraz IOD.
3) Po podpisaniu umowy Wykonawca występuje z pisemną prośbą o uruchomienie ww. usługi dla wskazanych przez siebie pracowników.
4) Pracownicy Wykonawcy, przed uzyskaniem zdalnego dostępu, muszą zapoznać się i zaakceptować „Regulamin zdalnego dostępu” stanowiący załącznik do niniejszej procedury.
5) Naczelnik wydziału merytorycznego przygotowuje w ESOD wniosek o nadanie uprawnień dla pracowników Wykonawcy ze wskazaniem zdalnego dostępu.
6) Po pozytywnym rozpatrzeniu wniosku przez IOD, Naczelnik Wydziału Informatyki lub wskazana przez niego osoba, uruchamia usługę zgodnie z wnioskiem o nadanie uprawnień.

Załącznik do Procedury „Zdalny dostęp”

Regulamin zdalnego dostępu

1. Użytkownikiem jest pracownik Wykonawcy, z którym została podpisana umowa dopuszczająca zdalny dostęp.
2. Użytkownik korzystający ze zdalnego dostępu do systemów Urzędu Miasta Rybnika ponosi pełną odpowiedzialność za swoje działania i zobowiązany jest do stosowania wszelkich środków bezpieczeństwa, tak aby nie naruszyć bezpieczeństwa systemów i danych przetwarzanych w Urzędzie Miasta (UM).
3. Informacje i dane przetwarzane w systemie UM są chronione. Użytkownik zobowiązuje się nie przekazywać innym osobom żadnych informacji i danych jakie uzyska z systemów UM.
4. Zdalny dostęp Użytkownika do systemów Urzędu może być wykorzystywany jedynie w celu i zakresie wynikającym z zakresu prac opisanego we właściwej umowie, podpisanej wcześniej pomiędzy Zamawiającym (Urząd Miasta Rybnika) a Wykonawcą (firma zatrudniająca Użytkownika).
5. Zdalny dostęp dla użytkowników przydzielany jest na czas realizacji umowy. W wyjątkowych okolicznościach (np. prace serwisowe, awarie, podejrzenie/wykrycie incydentu naruszenia bezpieczeństwa danych) zdalne połączenie może być zakończone wcześniej lub wyłączone czasowo na polecenie Naczelnika Wydziału Informatyki.
6. Na potrzeby połączenia Użytkownik otrzymuje indywidualny certyfikat konieczny do nawiązania połączenia VPN z siecią UM, login i hasło oraz oprogramowanie klienckie VPN. Certyfikat musi zostać odebrany osobiście przez Użytkownika w siedzibie UM.
7. Certyfikat jest wydawany na okres trwania umowy Wykonawcą, lecz nie dłużej niż na okres 1 roku. Do obowiązku użytkownika należy zgłoszenie do Wydziału Informatyki, z odpowiednim wyprzedzeniem konieczności odnowienia certyfikatu, jeżeli utraci on ważność w trakcie trwania umowy.
8. Użytkownik zobowiązuje się nie przekazywać innym osobom certyfikatu, hasła ani żadnych innych informacji związanych z procesem autoryzacji i zdalnego dostępu do systemów UM.
9. Brak możliwości skorzystania ze zdalnego dostępu, spowodowany np. problemami technicznymi, nie zwalnia Wykonawcy z konieczności terminowego wywiązania się z obowiązków określonych w umowie.
10. Użytkownik zobowiązuje się nie uruchamiać w systemach UM, innego oprogramowania niż to udostępnione przez Zamawiającego. W razie konieczności użycia innego oprogramowania, użytkownik każdorazowo uzyska wcześniej zgodę Naczelnika Wydziału Informatyki.
11. O wszelkich nieprawidłowościach w działaniu zdalnego dostępu, podejrzeniach związanych z możliwością naruszenia bezpieczeństwa Użytkownik niezwłocznie informuje Naczelnika Wydziału Informatyki lub wyznaczonego pracownika Wydziału Informatyki, lub Inspektora Ochrony Danych.
12. Nie stosowanie się do zasad określonych niniejszym regulaminem, spowoduje zablokowanie możliwości korzystania ze zdalnego dostępu.
13. Urząd Miasta zastrzega sobie prawo zmiany postanowień niniejszego regulaminu, o czym poinformuje wszystkie zainteresowane strony.