Załącznik nr 2 do zarządzenia Nr 7/2019 z dnia 30.04.2019 r.
Dyrektora Instytucji Pośredniczącej Aglomeracji Wałbrzyskiej

Instrukcja Zarządzania Systemem Informatycznym IPAW

Spis treści

I. Cel

Celem instrukcji jest określenie sposobu zarządzania systemem informatycznym Instytucji Pośredniczącej Aglomeracji Wałbrzyskiej.

II. Zasady ogólne

Zawarte w instrukcji procedury i wytyczne są przekazywane osobom odpowiedzialnym za ich realizację stosownie do przyznanych uprawnień i zakresu obowiązków.

III. Definicje

Ilekroć w niniejszym dokumencie jest mowa o :

1. **IPAW** – należy przez to rozumieć Instytucję Pośredniczącą Aglomeracji Wałbrzyskiej;
2. **Administratorze Danych** – należy przez to rozumieć Dyrektora Instytucji Pośredniczącej Aglomeracji Wałbrzyskiej;
3. **Koordynatora Działu IT** – należy przez to rozumieć pracownika IPAW odpowiedzialnego za funkcjonowanie systemu informatycznego IPAW oraz stosowanie technicznych i organizacyjnych środków ochrony;
4. **administratorze systemu** – należy przez to rozumieć pracownika Działu IT, który posiada uprawnienia do administrowani określonymi zasobami informatycznymi IPAW. Czasowo, za zgodą Administratora Danych oraz Koordynatora Działu IT Administratorem Systemu może zostać inny pracownik IPAW lub przedstawiciela firmy współpracującej;
5. **użytkowniku systemu** – należy przez to rozumieć osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym IPAW. Użytkownikiem może być pracownik IPAW, osoba wykonująca pracę na podstawie umowy zlecenie lub innej umowy cywilnoprawnej, osoba odbywająca staż w IPAW lub wolontariusz;
6. **sieci lokalnej** – należy przez to rozumieć połączenie systemów informatycznych IPAW wyłącznie dla własnych jej potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnej;
7. **sieci rozległej** – należy przez to rozumieć publiczną sieć telekomunikacyjną w rozumieniu ustawy z dnia z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dziennik Ustaw z 2004 r. Nr 171 poz. 1800 ze zmianami) i nie będącą siecią lokalną;
8. **zasobie wspólnym** – należy rozumieć wydzieloną przestrzeń dysków serwerów z przeznaczeniem na służbowe dane i dokumenty elektroniczne. Zasoby te budowane są hierarchicznie zgodnie ze schematem organizacyjnym IPAW;

9. **uwierzytelnianiu** – należy przez to rozumieć proces rozpoznawania użytkownika w systemie komputerowym. W systemach komputerowych IPAW funkcjonują trzy sposoby uwierzytelniania:
    - login użytkownika,
    - karta mikroprocesorowa,
    - osobno zdefiniowane metody biometryczne;
10. **autoryzacji** – jest to proces identyfikacji uprawnień do systemu. Autoryzacja odbywa się za pomocą hasła użytkownika lub pinu karty mikroprocesorowej. Zasady uprawnień do systemów określa poszczególna polityka uprawnień w każdym systemie;
11. **portalu IPAW** – należy rozumie zespół stron www w zarządzie IPAW stanowiącym logicznie powiązany serwis informacyjny publikujący treści z zakresu działania IPAW;
12. **umowa użyczenia** – rozumie się przez to umowę użyczenia lokalu pomiędzy IPAW a Gminą Wałbrzych z dnia nr 1/07/2015 z dnia 02.03.2015r.;
13. **porozumienie** – rozumie się przez to „Porozumienie w przedmiocie dostępu do systemu informatycznego" pomiędzy IPAW a Gminą Wałbrzych z dnia 19.06.2015r.;
14. **infrastruktura UMW** – rozumie się przez to udostępniona na potrzeby Instytucji Pośredniczącej Aglomeracji Wałbrzyskiej Infrastrukturę Informatyczną Urzędu Miejskiego w Wałbrzychu, do której dostęp opisuje Porozumienie;
15. **dokumentacja UMW** – rozumie się przez to obowiązującą dokumentację przetwarzania danych osobowych w urzędzie miejskim wprowadzoną zarządzeniem prezydenta Miasta Wałbrzycha w sprawie wprowadzenia dokumentacji przetwarzania danych osobowych w Urzędzie Miejskim w Wałbrzychu;
16. **zasoby informatyczne** – rozumie się przez to zasoby informatyczne udostępniane w ramach Infrastruktury UMW takie jak programy merytoryczne, serwery wirtualne, serwery plików, oraz inne opisane w Dokumentacji UMW.

IV. Wymagania techniczne systemów informatycznych

1. Wszystkie środki sprzętowe i programowe, również nowo kupowane, służące do przetwarzania informacji elektronicznej podlegają autoryzacji przez Koordynatora Działu IT.
2. Wszystkie zasoby systemu informatycznego IPAW podlegają ewidencjonowaniu w Ewidencji Sprzętu Komputerowego prowadzonej przez Koordynatora Działu IT.
3. Każdorazowe zmiany w konfiguracji zarówno sprzętowej jak i programowej podlegają ewidencjonowaniu w ww. Ewidencji.

4. Każdy z wdrażanych systemów informatycznych podlega audytowi Działu IT i jego działanie oraz bezpieczeństwo przechowywania danych jest odbierane przez Koordynatora Działu IT.
5. W uzasadnionych przypadkach zastępowany system (tradycyjny lub informatyczny) prowadzony jest równolegle z nowo wdrażanym systemem informatycznym, a dane wejściowe i wyniki wyjściowe polegają weryfikacji.
6. Każdy system informatyczny musi mieć przynajmniej dwa poziomy autoryzacji. Użytkownika i Administracyjny. W trybie użytkownika nie może być dostępna kontrola pracy innych użytkowników, jak i zarządzanie ich uprawnieniami do systemu.
7. System informatyczny nie dopuszcza logowania anonimowego. Dane przechowywane w systemie informatycznym nie są dostępne dla klientów IPAW. Dane publikowane, dostępne dla klientów IPAW publikowane są w Biuletynie Informacji Publicznej i stronach internetowych IPAW.
8. Każdy serwer IPAW musi być zasilany za pośrednictwem urządzenia do awaryjnego zasilania (UPS). Urządzenie to w razie awarii zasilania ma bezpieczne i automatyczne zakończyć pracę serwera oraz powiadomić o tym fakcie administratora za pomocą poczty elektronicznej i lub wiadomości SMS.
9. Każdy komputer użytkownika musi być zasilany z wydzielonej linii energetycznej poprzez elektryczną listwę z zabezpieczeniem przeciwprzepięciowym.
10. Tam gdzie to możliwe, komputery użytkowników, zwłaszcza komputery przetwarzające dane osobowe i systemów merytorycznych przechowujących zasoby w bazach danych zgromadzonych na serwerach IPAW powinny być zasilane za pomocą zasilaczy awaryjnych (UPS). Urządzenia UPS powinny umożliwić bezpieczne zakończenie pracy w systemie w przypadku braku zasilania. Jeżeli urządzenie UPS to umożliwia, zamknięcie sytemu powinno odbywać się automatycznie.
11. Sprzęt informatyczny podlega konserwacji wg instrukcji stanowiącej procedurę *„Kontrola stanu urządzeń informatycznych”* w „Zestawieniu procedur pomocniczych” będącym Załącznikiem nr 2.1 do niniejszej instrukcji.
12. Nie rzadziej niż raz na 12 miesięcy Dział IT sporządza raport z wykorzystania posiadanych zasobów oraz plan ich wykorzystania na następne 12 miesięcy.
13. Zgłaszanie awarii:
    a) wszelkie nieprawidłowości w działaniu systemu informatycznego związane z Infrastruktura IPAW użytkownicy mają obowiązek zgłaszać do Działu IT za pomocą poczty elektronicznej na adres pomoc@ipwaw.walbrzych.eu;

- jeżeli nie można zrealizować zgłoszenia za pomocą poczty elektronicznej dopuszczalne jest zgłoszenie telefoniczne lub inne skuteczne;

b) wszelkie nieprawidłowości w działaniu systemu informatycznego związane z Zasobami Informatycznymi udostępnionymi w ramach Infrastruktury UMW użytkownicy mają obowiązek zgłaszać do Biura Informatyki Urzędu Miejskiego za pomocą specjalnej aplikacji QDesk, do której skrót znajduje na pulpicie każdego użytkownika;

- w przypadkach kiedy nie można uruchomić komputera, zgłoszenie awarii może nastąpić z dowolnego sąsiedniego, sprawnego komputera;
- jeżeli nie można zrealizować zgłoszenia systemem QDesk za pomocą powyższych punktów dopuszczalne jest zgłoszenie telefoniczne lub inne skuteczne.

V. Opis systemu informatycznego IPAW.

A. Struktura fizyczna.

System informatyczny IPAW działa w oparciu o sieć komputerową Ethernet w budynku należącym do Urzędu Miejskiego w Wałbrzychu. Opis sieci informatycznej zawarty jest w opracowaniu będącym załącznikiem nr 2.2 do niniejszej instrukcji.

B. Struktura logiczna

Logiczna struktura sieci informatycznej IPAW oparta jest na domenowej, hierarchicznej usłudze katalogowej Active Directory opracowanej przez firmę Microsoft. Składa się z warstwy fizycznej i logicznej.

Na warstwę fizyczną składają się Lokalizacje (Site), Kontrolery Domeny Actitve Directory oraz komputery do domeny Active Directory podłączone.

1. W sieci informatycznej IPAW wypromowano domenę Active Directory o nazwie um.local.
2. Dostęp do Active Directory jest realizowany przez Infrastrukturę UMW, której strukturę logiczną opisuje Dokumentacja UMW.
3. Stacje robocze pracujące w sieci informatycznej IPAW muszą poprawnie zalogować się do domeny Active Directory. W związku z tym ustala się jako minimalny system Windows 7, Windows 8.1 lub Windows 10 w wersji Professional.
4. Niedopuszczalne jest stosowanie systemów nie posiadających odpowiedniego systemu zabezpieczeń (np Windows 98, Windows 95, Windows) oraz systemów nie posiadających systemu logowania do domeny Windows (np Windows XP Home Edition, Windows Vista Home Basic, Windows 7 Home itp.).

5. Każdy użytkownik, aby pracować w systemie informatycznym IPAW, musi posiadać indywidualne konto.
6. Konta użytkowników w Active Directory stosują system zabezpieczeń i uprawnień nazywanych Polityką Zasad Grup (GPO), która jest określona jako podstawowa w domenie um.local.
7. Wszystkie stacje robocze synchronizują swoje wewnętrzne zegary czasu rzeczywistego z kontrolerem domeny, do którego zostały zalogowane. Użytkownik zalogowany do domeny nie ma uprawnień do zmiany czasu.
8. Dane osobowe przechowywanie na dyskach lokalnych komputerów IPAW podlegają szyfrowaniu. Certyfikat szyfrujący musi być na osobnym, zabezpieczonym przed dostępem fizycznym jak i zdalnym serwerze.
9. W ramach infrastruktury UMW przechowywane są 3 podstawowe grupy certyfikatów:
   a) certyfikaty identyfikacji komputerów przechowywane na serwerze, głównym kontrolerze domeny i replikowane na pozostałem kontrolery domeny,
   b) certyfikaty identyfikacji komputerów zdalnego dostępu VPN. Centrum Certyfikacji znajduje się na serwerze o nazwie ZEUS. Ze względów bezpieczeństwa musi to być inny serwer niż udostępniający połączenie VPN,
   c) certyfikaty – klucze szyfrujące – danych osobowych, które z przyczyn technicznych znajdują się na dyskach lokalnych. Certyfikaty te, zależnie od lokacji komputera, znajdują się na najbliższym serwerze będącym kontrolerem domeny.

VI. Stosowane metody i środki uwierzytelniania i autoryzacji.

A. Uwagi ogólne

1. W systemach komputerowych wspomagających czynności merytoryczne, a w szczególności przetwarzających dane osobowe, użytkownicy podlegają uwierzytelnieniu za pomocą identyfikatora użytkownika i autoryzacji z pomocą hasła.
2. Przy opuszczeniu stanowiska pracy na odległość uniemożliwiającą jego obserwację należy zablokować system kombinacją klawiszy [Windows] + [L].
3. Osoba udostępniająca stanowisko komputerowe innemu upoważnionemu pracownikowi zobowiązana jest wylogować się z systemu.
4. Przed wyłączeniem komputera należy bezwzględnie:
   a) zakończyć pracę uruchomionych programów,
   b) wykonać zamknięcie systemu połączone z wylogowaniem,

5. Niedopuszczalne jest wyłączenie komputera bez zamknięcia wszystkich użytkowanych programów i wylogowania się z systemu,
6. Niedopuszczalne są praktyki blokowania automatycznego włączania zabezpieczonego hasłem wygaszacza ekranu na czas nieobecności pracownika,
7. Dział Kadr i Płac najpóźniej do godziny 9:00 dnia następnego po nastąpieniu zdarzenia zawiadamia Dział IT o wszelkich zmianach dotyczących statusu zatrudnienia pracowników, a zwłaszcza o terminie rozwiązania umowy o pracę.

B. Zasady nadawania identyfikatora

1. Identyfikator użytkownika jest unikalny w obrębie systemu, w którym jest stosowany.
2. Identyfikator konstruowany jest z pierwszej litery imienia oraz nazwiska użytkownika.
3. W przypadku dublowania się identyfikatora, identyfikator składa się z dwóch pierwszych liter imienia i nazwiska. Jeżeli nadal identyfikator by się dublował należy użyć trzech pierwszych liter imienia itd. Po wyczerpaniu algorytmu do imienia dodaje się kolejną cyfrę arabską.
4. Identyfikator użytkownika nie powinien być zmieniany bez wyraźnej przyczyny, a po wyrejestrowaniu użytkownika z systemu informatycznego nie może być przydzielony innej osobie.
5. Z przyczyn technicznych nie należy stosować identyfikatorów zawierających znaki diakrytyczne charakterystyczne dla języka polskiego (ę, ą, ż itp.).

C. Zasady zarządzania hasłami.

1. Nowe konto jest zakładane przez Administratora systemu zgodnie z procedurą *„Wdrożenie nowego stanowiska komputerowego”* zapisaną w „Zestawieniu procedur pomocniczych” będącym Załącznikiem nr 2.1 do niniejszej instrukcji.
2. W systemach umożliwiających samodzielną zmianę haseł przez użytkowników hasło powinno być zmienione przy pierwszym logowaniu do systemu.
3. Hasło użytkownika jest poufne, jest własnością użytkownika i zna je tylko dany użytkownik. Zabronione jest przekazywanie hasła innym lub w jakikolwiek sposób narażanie na poznanie hasła przez osoby postronne.
4. Za zachowanie poufności swoich haseł odpowiedzialni są użytkownicy.
5. Hasła użytkownika utrzymuje się w tajemnicy również po upływie ich ważności.

6. Wszystkie hasła są tajne. Nie mogą pojawiać się w formie elektronicznej otwartym tekstem bez bezpiecznego szyfrowania, a w oknach edycyjnych bez zaciemnienia. W formie papierowej może występować tylko w uzasadnionych i opisanych odrębnymi procedurami przypadkach.
7. Dla haseł grupowych, użytkownik nie ma prawa do udostępnienia haseł danej grupy osobom spoza grupy, dla której zostały one utworzone.
8. Hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie.
9. W sytuacji, kiedy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, pracownik zobowiązany jest do natychmiastowej zmiany hasła.
10. Przy wyborze hasła obowiązują zasady:
    a) minimalna długość hasła – 8 znaków,
    b) zakazuje się stosować:
        - haseł, które użytkownik stosował uprzednio w okresie minionego roku,
        - swojej nazwy użytkownika w jakiejkolwiek formie (pisanej dużymi literami, w odwrotnym porządku, dublując każdą literę, itp.),
        - swojego imienia, drugiego imienia, nazwiska, przezwiska, pseudonimu w jakiejkolwiek formie,
        - imion (w szczególności imion osób z najbliższej rodziny jak i zwierząt domowych),
        - ogólnie dostępnych informacji o użytkowniku takich jak: numer telefonu, numer rejestracji samochodu, jego marka, numer dowodu osobistego, nazwa ulicy na której mieszka lub pracuje, itp.
        - występujących pojedynczo wyrazów słownikowych,
        - przewidywalnych sekwencji znaków z klawiatury np.: „ QWERTY", „12345678", itp.
    c) należy stosować:
        - hasła zawierające kombinacje dużych i małych liter i cyfr,
        - hasła zawierające znaki specjalne zawarte w tabeli:

!	wykrzyknik
"	cudzysłów
#	kratka (hash)
$	dolar
%	procent
&	and
'	apostrof
(	nawias otwierający

)	nawias zamykający
*	gwiazdka
+	plus
,	przecinek
-	myślnik
.	kropka
/	ukośnik
:	dwukropek
;	średnik
<	znak mniejszości
>	znak większości
@	małpa
=	znak równości
[	nawias kwadratowy otwierający
\	odwrotny ukośnik
]	nawias kwadratowy zamykający
^	daszek
_	podkreślenie
{	nawias klamrowy otwierający
|	pałka pionowa
}	nawias klamrowy zamykający

- hasła, które można zapamiętać bez zapisywania,
- hasła łatwe i szybkie do wprowadzenia, po to by trudniej było podejrzeć je osobom trzecim,

11. Zmiany hasła nie wolno zlecać innym osobom.

D. Zasady wyrejestrowania użytkownika z systemu informatycznego

1. Wyrejestrowania użytkownika z systemu informatycznego dokonuje administrator systemu na wniosek kierownika Działu Kadr i Płac lub po zgłoszeniu się użytkownika z kartą obiegową z podanym terminem zakończenia pracy w IPAW.
2. Wyrejestrowanie, o którym mowa w ust. 1, może mieć charakter czasowy, trwały lub automatyczny.
3. Wyrejestrowanie następuje poprzez:

a) zablokowanie konta użytkownika do czasu ustania przyczyny uzasadniającej blokadę (wyrejestrowanie czasowe),
b) trwałe zablokowanie danych użytkownika w bazie użytkowników systemu (wyrejestrowanie trwałe),
c) upłynięcie terminu ważności konta w domenie Active Directory w przypadku zatrudnienia na czas określony.

4. Czasowe wyrejestrowanie użytkownika z systemu informatycznego musi nastąpić w razie:
   a) nieobecności użytkownika w pracy trwającej dłużej niż 21 dni kalendarzowych,
   b) zawieszenia w pełnieniu obowiązków służbowych,
   c) wypowiedzenie umowy o pracy,
   d) wszczęcie postępowania dyscyplinarnego względem osoby upoważnionej do przetwarzania danych osobowych,
   e) incydentu bezpieczeństwa z udziałem konta nieobecnego w danej chwili użytkownika systemu informatycznego
5. Przyczyną trwałego wyrejestrowania użytkownika z systemu informatycznego jest rozwiązanie lub wygaśnięcie stosunku pracy lub innego stosunku prawnego, w ramach którego zatrudniony był użytkownik.

E. Zasady zarządzania uprawnieniami.

1. Nowy użytkownik systemu może dostać uprawnienia do systemu komputerowego po:
   a) otrzymaniu upoważnienia do przetwarzania danych osobowych,
   b) zapoznaniu się z niniejszą Instrukcją Zarządzania Systemem Informatycznym IPAW i potwierdzeniu na piśmie faktu zapoznania się z ww. dokumentami oraz złożyć stosowne oświadczenie, potwierdzające znajomość jego treści.
2. Użytkownik systemu nie może uruchamiać innego oprogramowania niż zainstalowane przez Dział IT do którego ma przyznane kartą uprawnień uprawnienia. W szczególności nie może samodzielnie instalować oprogramowania i w jakikolwiek sposób obchodzić zabezpieczenia uniemożliwiające instalację lub uruchomienie innego oprogramowania.
3. Administrator systemu ma dostęp do całości systemu informatycznego w tym uprawnienia do nadawania i odbierania uprawnień, zakładania kont użytkowników, zakładania i zmiany haseł.
4. Użytkownik systemu może mieć dostęp tylko do tych zasobów sieci informatycznej IPAW do której posiada przyznane mu przez Administratora uprawnienia.

5. Zmiany uprawnień dokonuje się każdorazowo na wniosek przełożonego Użytkownika poprzez złożenie Karty Uprawnień Jednostkowych do Działu IT. Kartę Uprawnień należy złożyć za pomocą Formularza, którego wzór stanowi załącznik nr 2.4 do niniejszego dokumentu.
6. Osoby trzecie wykonujące zadania w sieci IPAW muszą każdorazowo uzyskać pozwolenie Administratora Danych lub osób przez niego upoważnionych. W przypadku pracy na – czasowo nadanych – uprawnieniach administracyjnych, praca taka musi przebiegać pod nadzorem przynajmniej jednego administratora systemu.
7. Każde oprogramowanie konieczne do uruchomienia lub instalacji przez osoby trzecie musi być sprawdzone przez Administratora Systemu i zatwierdzone przez Koordynatora Działu IT.

VII. System tworzenia kopii bezpieczeństwa.

System tworzenia kopii bezpieczeństwa jest zapewniony w ramach Infrastruktury UMW i został on opisany w procedurze „Tworzenie, dystrybucja i przechowywanie kopii bezpieczeństwa" w załączniku nr 2.1 „Zestaw procedur pomocniczych" do Dokumentacji UMW oraz w Porozumieniu.

VIII. Środki ochrony systemu przed wirusami i innym złośliwym oprogramowaniem.

1. Na każdym stanowisku komputerowym musi być zainstalowane oprogramowanie antywirusowe pracujące i wychwytujące wirusy jak i inne złośliwe oprogramowanie.
2. Każdy odbierana wiadomości przychodząca drogą elektroniczną musi być sprawdzona pod względem występowania ww. oprogramowania. Zarówno treść jak i załączniki włączając te spakowane popularnymi algorytmami (zip, rar).
3. Definicje wzorców wirusów aktualizowane są przy każdym starcie systemu nie rzadziej niż raz na 3 dni. Aktualizacja odbywa się automatycznie z określonego serwera w ramach Infrastruktury UMW.
4. Komputery przenośne, przebywające często poza siecią IPAW, mają zdefiniowany inny, globalny serwer aktualizacji. Sprawdzenie aktualności i ewentualna aktualizacja sygnatur musi się odbywać przy każdym podłączeniu komputera do sieci internet.
5. Aktualność sygnatur programów antywirusowych jest zapewniona w ramach Infrastruktury UMW.

6. Każdy nośnik wymienny (dyskietka, pamięć Flash) po podłączeniu powinna być sprawdzona na obecność występowania ww. oprogramowania. Niedopuszczalne jest użytkowanie nośnika bez sprawdzenia jeżeli był poprzednio użyty w innym systemie, zarówno komputerowym jak i innym.
7. Zabrania się pobierania z Internetu plików niewiadomego pochodzenia. Każdy plik pobrany z Internetu musi być sprawdzony programem antywirusowym. Sprawdzenia dokonuje użytkownik, który pobrał plik. Za sprawdzenie odpowiada Użytkownik. Kontrola antywirusowa przeprowadzana jest na komputerach, co do których istnieje podejrzenie, że nieprawidłowości w działaniu mogą być przyczyną ww. oprogramowania.
8. W przypadku wykrycia wirusów komputerowych sprawdzane jest:
   a) stanowisko komputerowe na którym wirusa wykryto,
   b) wszystkie nośniki wymienne i zapisywalne posiadane przez użytkowników pracującym na ww. stanowisku komputerowym,
   c) komputery wszystkich osób logujących się na danej stacji,
   d) zasoby i użytkownicy wspólnych grup uprawnień dzielących zasoby,

IX. Dokumenty elektroniczne.

A. Zasady przechowywania dokumentów elektronicznych.

1. Podczas logowania tworzony jest na pulpicie dynamicznie skrót do zasobu wspólnego właściwego dla komórki organizacyjnej użytkownika.
2. Wszystkie dokumenty elektroniczne danej komórki należy przechowywać na zasobach wspólnych.
3. Przydział uprawnień do czynności wykonywanych na zasobach wspólnych dokonuje się za pomocą kart uprawnień.

B. Zasada „czystego ekranu"

1. Dokumenty elektroniczne powinny być przechowywane w sposób zapewniający im bezpieczeństwo.
2. Dokumenty zawierające dane poufne lub osobowe winny być wyświetlane na monitorze w sposób uniemożliwiający ich odczyt przez osoby nieuprawnione.
3. Po zakończeniu pracy na pulpicie oraz w folderach umieszczonych na nim nie wolno przechowywać żadnych dokumentów lub bezpośrednich skrótów do nich.

4. Dokumenty wolno przechowywać na pulpicie tylko podczas bezpośredniej edycji. Po zakończeniu pracy winny zostać przeniesione na zasób wspólny, a z pulpitu usunięte.

X. Nośniki mobilne.

A. Rodzaje nośników mobilnych.

Do nośników mobilnych zalicza się: dyskietki, płyty CD, DVD i Bluray, taśmy streamerów, masowe urządzenia magazynujące podłączane pod port USB, FireWire lub inny port wymiany danych komputera, pamięć wewnętrzna komputerów przenośnych i innych urządzeń taką pamięć posiadających takie jak odtwarzacze mp3 i mp4, palmtopy, telefony komórkowe, smartfony, nawigacje satelitarne i podobne.

B. Zasady użytkowania nośników mobilnych

1. Uprawnienia do użytkowania nośników mobilnych nadawane są i odbierane za pomocą karty uprawnień jednostkowych.
2. Nośniki USB są imiennie rejestrowane i tylko zarejestrowane nośniki mogą być użytkowane w Systemie Informatycznym.
3. Rejestr użytkowników posiadających uprawnienia do zapisywania danych na nośnikach mobilnych oraz ich ewentualnego wynoszenia poza teren IPAW prowadzi Dział IT.
4. Nośniki mobilne muszą być w sposób trwały oznaczone:
   a) środki trwałe posiadające wbudowane nośniki mobilne powinny być oznaczone etykietą wg. oznaczeń środków trwałych IPAW,
   b) inne nośniki powinny być oznaczone bądź pieczątką IPAW (dyskietki, taśmy streamerów) bądź niezmywalnym markerem,
   c) minimalne oznaczenie to napis „IPAW",
   d) nie wolno dokonywać zapisu i odczytu nośników danych innych niż oznaczone z wyjątkiem nośników obrotu danymi podlegających regulacjom za pomocą odrębnych umów.
5. Dane osobowe i dane uznawane za wrażliwe powinny być przechowywane na nośnikach mobilnych w sposób bezpieczny. Chronione programem pozwalającym na szyfrowanie oparte na algorytmach AES (symetryczny) lub RSA (niesymetryczny) i kluczem minimum 128 bitowym. Można posłużyć się innym nieskompromitowanym algorytmem lecz należy wówczas zwiększyć bezpieczeństwo szyfrowania do 256 bitowego klucza.

6. Niepotrzebne lub uszkodzone mobilne nośniki danych oddawane są do Działu IT, gdzie podlegają zniszczeniu w niszczarce płyt w przypadku nośników optycznych i dyskietek lub poprzez fizyczne zniszczenie w przypadku innego nośnika.
7. Użytkownik nośników mobilnych podlega wstępnemu i okresowemu szkoleniu z zasad bezpiecznego przechowywania danych, zasad ich udostępniania oraz bezpiecznej pracy na urządzeniach mobilnych zawierających nośniki danych.

XI. Posługiwania się pocztą e-mail.

1. Serwer poczty elektronicznej funkcjonuje w wewnętrznej sieci w ramach Infrastruktury UMW i zajmuje się dystrybucją wiadomości email zarówno w sieci wewnętrznej jak i na serwery zewnętrzne.
2. Wysyłanie poczty elektronicznej w IPAW działa w oparciu o protokół SMTP (ang. Simple Mail Transfer Protocol).
3. Pobierania wiadomości z serwera poczty elektronicznej wykonuje się w oparciu o protokół POP3 (Post Office Protocol version 3) lub IMAP (Internet Message Access Protocol).
4. Ustawienia serwera wymagają uwierzytelnienia wysyłania wiadomości tj. przed wysłaniem każdej wiadomości pocztowej program pocztowy musi podać dane uwierzytelniające - login i hasło.
5. Konta pocztowe poczty elektronicznej przydzielane są na podstawie modyfikacji uprawnień za pomocą karty uprawnień jednostkowych.
6. Konta poczty elektronicznej przydzielane każdorazowo są według następującego klucza *pierwsza_litera_imienia.nazwisko@ipaw.walbrzych.eu* Jeżeli taka nazwa konta pocztowego jest już zajęta, używa się pierwszych dwóch liter imienia. Jeżeli nadal nazwa nie jest unikalna używa się trzech pierwszych liter imienia itd. Po wyczerpaniu algorytmu do imienia dodaje się kolejną cyfrę arabską.
7. Hasła do poczty elektronicznej generują i konfigurację programu pocztowego przeprowadzają pracownicy Działu IT.
8. Ponieważ wiadomość pocztowa jest wysyłana i odbierana nieszyfrowanym połączeniem oraz otwartym tekstem nie wolno jej stosować do korespondencji zawierającej dane poufne oraz zawierającej dane osobowe bez odpowiednich procedur szyfrowania załączników.
9. Procedurę wysyłania danych poufnych oraz zawierających dane osobowe reguluje procedura *„Udostępnianie i przekazywanie danych, w tym danych poufnych i osobowych”* opisana w „Zestawieniu procedur pomocniczych” stanowiącym załącznik nr 2.1 do niniejszej instrukcji.

10. W przypadku wysyłania wiadomości wielu odbiorców, zwłaszcza na adresy prywatne lub instytucji innych niż administracja publiczna zabrania się podawania adresów w sposób jawny tj. w polu „DO" lub „DW". Należy wówczas użyć pola ukrytego (UDW).

XII. Zasady i sposób odnotowywania w systemie informacji o udostępnianiu danych osobowych.

1. Dane osobowe z eksploatowanych systemów mogą być udostępniane wyłącznie osobom upoważnionym.
2. Udostępnianie danych osobowych, w jakiejkolwiek postaci wymaga pisemnego upoważnienia Administratora Danych.
3. Udostępnienie danych osobowych osobom nie może być realizowane drogą telefoniczną.
4. Udostępnienie danych osobowych może nastąpić wyłącznie po przeanalizowaniu podstawy ich udostępnienia.
5. Udostępnienia danych osobowych może być realizowane drogą elektroniczną za pomocą procedury *„Udostępnianie i przekazywanie danych, w tym danych poufnych i osobowych"* opisanej w „Zestawieniu procedur pomocniczych" stanowiącym załącznik nr 2.1 do niniejszej instrukcji.
6. Kierownicy komórek organizacyjnych, prowadzą rejestry udostępnionych danych osobowych zawierające co najmniej: datę udostępnienia, podstawę, zakres udostępnionych informacji oraz osobę lub instytucje, której dane udostępniono.

XIII. Publikacja treści na stronach internetowych IPAW

1. Publikacja treści zajmują się uprawnione osoby będące Redaktorami Portalu www IPAW.
2. Uprawnienia Redaktorów Portalu mogą dotyczyć całości lub wydzielonej części tematycznej stron www IPAW.
3. Za publikowane treści w części Głównej portalu odpowiada Kierownika Działu Naborów i Promocji.
4. Za publikowane treści w części portalu dotyczącej Biuletynu Informacji Publicznej odpowiada Kierownika Działu Organizacyjnego i Pomocy Technicznej.
5. Redaktor Główny portalu prowadzi listę osób i podmiotów – uzgodnionych dostawców treści – do Portalu IPAW.
6. Wnioski o publikację, zmianę lub usunięcie treści na stronach internetowych IPAW należy kierować bezpośrednio do Kierowników odpowiedzialnych za powyższe części portalu.

7. Kierownicy działów odpowiedzialnych za publikowanie treści na stronach internetowych IPAW, prowadzą rejestr zmian, dokonywanych w części portalu WWW, za który odpowiadaj.

XIV. Zasady użytkowania komputerów przenośnych

1. Osoba użytkująca przenośny komputer, służący do przetwarzania danych osobowych, obowiązana jest zachować szczególną ostrożność podczas transportu i przechowywania tego komputera poza obszarem, przeznaczonym do przetwarzania danych osobowych wskazanym w Polityce Bezpieczeństwa.
2. W celu zapobieżenia dostępowi do tych danych osobie niepowołanej, należy:
   a) użytkować wyłącznie urządzenie zarejestrowane w domenie Acitve Directory um.local stosującej nieodwracalne szyfrowanie haseł i zasady GPO kontenera przeznaczonego dla komputerów przenośnych zwiększających liczbę logowań z bufora do 50,
   b) dane osobowe i dane z baz danych programów merytorycznych użytkowanych w systemie informatycznym IPAW przetwarzać za pomocą zdalnego dostępu do bazy danych użytkując aplikacje trójwarstwowe (przeglądarkowe lub tzw. cienkiego klienta),
   c) w przypadku aplikacji dwu lub jednowarstwowych używać usług terminalowych (protokół RDP) realizowanych za pomocą serwera terminali Iris,
   d) nie zezwalać na używanie komputera osobom nieupoważnionym do dostępu do danych osobowych.
   e) w przypadku konieczności przechowywania danych osobowych lub innych, poufnych na dysku lokalnym komputera przenośnego należy takie dane zaszyfrować,
   f) wprowadzenie w BIOS/UEFI następujących ustawień:
      - wejście i zmiana ustawień BIOS/UEFI wymaga podania hasła;
      - wyłączona jest możliwość uruchamiania systemu z sieci lub innych nośników niż dysk twardy komputera;
      - długość hasła BIOS/UEFI zgodne z polityką haseł z p. VI.C
3. W przypadku kradzieży sprzętu komputerowego przenośnego użytkowanego poza siedzibą IPAW użytkownik powinien niezwłocznie zawiadomić organy policji celem sporządzeniu stosownego protokołu/zgłoszenia. Następnie powiadomić o tym fakcie i przedstawić protokół z policji w dziale OPT celem zgłoszenia tego faktu do ubezpieczyciela oraz w dziale DF.

XV. Sposób postępowania w sytuacji naruszenia ochrony danych osobowych.

Sposób postępowania w sytuacji stwierdzenia naruszenia ochrony danych osobowych określa Instrukcja Postępowania w Sytuacji Naruszenia Ochrony Danych Osobowych Załącznik Nr 2.3 do niniejszej instrukcji.

XVI. Postanowienia końcowe

1. W sprawach nieuregulowanych niniejszą instrukcją należy stosować instrukcje obsługi i zalecenia producentów aktualnie wykorzystywanych urządzeń i programów.
2. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest zapoznać się przed dopuszczeniem do przetwarzania danych z niniejszą instrukcją oraz złożyć stosowne oświadczenie, potwierdzające znajomość jej treści.
3. Niezastosowanie się do procedur określonych w niniejszej instrukcji i załącznikach przez pracowników upoważnionych do przetwarzania danych osobowych może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, skutkujące rozwiązaniem stosunku pracy bez wypowiedzenia na podstawie art. 52 kodeksu pracy.

DYREKTOR
INSTYTUCJI POŚREDNICZĄCEJ
AGLOMERACJI WAŁBRZYSKIEJ
Bożena Dróżdż