INSTYTUCJA POŚREDNICZĄCA
AGLOMERACJI WAŁBRZYSKIEJ
ul. J. Słowackiego 23A
58-300 Wałbrzych
NIP: 886-298-60-61, R: 360712256
(1)

Załącznik Nr 2.1
do Zarządzenia Nr ...2...../2015
Dyrektora IPAW
z dnia 02.03.2015 r.

ZESTAWIENIE PROCEDUR POMOCNICZYCH

Spis treści

1. Definicje i używane skróty.

Niniejszy dokument jest załącznikiem do Instrukcji Zarządzania Systemem Informatycznym i stosowane są definicje i pojęcia wymienione w ww. opracowaniu.

Ilekroć w niniejszym dokumencie jest mowa o:

1. **Oprogramowaniu prywatnym** – należy przez to rozumieć programy komputerowe, które nie są własnością IPAW.
2. **Oprogramowaniu dodatkowym** – należy przez to rozumieć wszelkie oprogramowanie komercyjne/darmowe, które nie wchodzi w skład oprogramowania systemowego, instalowanego automatycznie oraz nie jest częścią systemów merytorycznych o osobno regulowanym trybie dostępu do sytemu.
3. **Dowodach legalności** – należy przez to rozumieć elementy dla potwierdzenia legalności posiadanego oprogramowania.
4. **Godzinach logowania** – należy przez to rozumieć przedział czasu, w którym użytkownicy mogą podjąć próbę autoryzacji w systemie.
5. **Standardowym zakresie czasu pracy** – jest to minimalny zakres czasu, zapewniający dostęp do systemu informatycznego ustalony na podstawie godzin pracy IPAW.
6. **Zamówieniu Publicznym** – należy przez to rozumieć, odpłatne umowy zawierane między zamawiającym a wykonawcą, których przedmiotem są usługi, dostawy lub roboty budowlane. Do zamówień publicznych znajduje zastosowanie ustawa z dnia 29 stycznia 2004 r. Prawo zamówień publicznych, (Tj. Dz. U. Dz.U. 2013 poz. 907 ze zm.) w zakresie regulującym sposób wyboru oferty.
7. **Zamówieniu poniżej progów** – należy przez to rozumieć, zamówienia i konkursy, których wartość nie przekracza wyrażonej w złotych równowartości kwoty 30 000 euro a dokonywane są na podstawie art. 4 ustawy Prawo zamówień publicznych.
8. **Dostępie zdalnym lub VPN** (ang. Virtual Private Network, Wirtualna Sieć Prywatna), jest to programowo realizowana sieć tworząca szyfrowane połączenie prywatne pomiędzy klientami końcowymi za pośrednictwem innej sieci (w tym publicznej np. Internet) w taki sposób, że węzły tej sieci są przezroczyste dla przesyłanych w ten sposób pakietów.

9. **Użytkowniku VPN** – Użytkownik Systemu Informatycznego IPAW posiadający uprawnienia do łączenia się z siecią IPAW z lokalizacji innych niż siedziba IPAW za pomocą sieci VPN.
10. **Odbiorcy danych** (OD) – należy przez to rozumieć osobę fizyczną lub prawną, która uzyskuje, w określonym zakresie, uprawnienia do przetwarzania danych z zasobów IPAW.
11. **KPE** – należy przez to rozumieć Kwalifikowany Podpis Elektroniczny.
12. **Komputerze zdalnym** – należy przez to rozumieć komputer służący do realizowania dostępu zdalnego.
13. **Szafie krosowniczej** – należy przez to rozumieć metalową szafę, w której umieszczane są serwery, aktywne i pasywne urządzenia będące elementami sieci komputerowej oraz urządzenia wspomagające.
14. **Serwerowni** – należy przez to rozumieć wydzielone pomieszczenie będące środowiskiem pracy komputerów pełniących rolę serwerów, a także aktywnych i pasywnych elementów sieci komputerowej.
15. **Sprzęcie komputerowym** – należy przez to rozumieć urządzenie elektroniczne służące do przetwarzania informacji i/lub urządzenia z nim współpracujące takie jak: drukarki, skanery, rzutniki, kamery, aparaty cyfrowe.
16. **Archiwizacji** - należy przez to rozumieć proces wykonywania kopii danych w celu zabezpieczenia ich przed utratą wskutek wystąpienia takich zdarzeń losowych jak powódź, pożar, włamanie, awaria sprzętu lub oprogramowania, czy skasowanie ich przez użytkownika.
17. **Dokumencie elektronicznym** – należy przez to rozumieć zbiór danych stanowiący odrębną całość znaczeniową i zapisany na nośniku danych.
18. **Kopii bezpieczeństwa** – należy przez to rozumieć dane, które mają służyć do odtworzenia oryginalnych danych w przypadku ich utraty lub uszkodzenia.
19. **Kopii pełnej** - należy przez to rozumieć sposób wykonania kopii polegający na skopiowaniu wszystkich wybranych plików.
20. **Kopii przyrostowej** - należy przez to rozumieć sposób wykonania kopii polegający na kopiowaniu jedynie tych plików, które zostały utworzone lub zmienione od czasu utworzenia ostatniej kopii przyrostowej lub normalnej.
21. **Kopii różnicowej** - należy przez to rozumieć sposób wykonania kopii polegający na

kopiowaniu jedynie tych plików, które zostały utworzone lub zmienione od czasu utworzenia ostatniej kopii normalnej.

22. **Serwerze plików** – należy przez to rozumieć wydzielony komputer (serwer), który udostępnia zasoby dyskowe.
23. **Nośniku danych** - należy przez to rozumieć urządzenie, na którym możliwe jest fizyczne zapisanie danego rodzaju informacji, i z którego możliwe jest późniejsze odczytanie (odtworzenie) tej informacji. Rodzaje nośników wykorzystywanych do tworzenia kopii bezpieczeństwa:
    - dyski magnetyczne,
    - dyski optyczne,
    - taśmy magnetyczne
24. **Złomowaniu** – należy przez to rozumieć uznawanie za nienadające się do dalszego użytkowania urządzenia zużyte lub uszkodzone, sklasyfikowane jako nie nadające się do naprawy lub remontu, ale także przestarzałe technicznie lub zbędne.
25. **Komisji likwidacyjnej** – należy przez to rozumieć komisję likwidacyjną powoływaną przez Dyrektora IPAW, która przeprowadza likwidację sprzętu komputerowego.
26. **Koncie** – należy przez to rozumieć zbiór zasobów i uprawnień w systemie przypisanych konkretnemu użytkownikowi. Konto posiada jednoznaczny identyfikator.
27. **Koncie systemowym** – należy przez to rozumieć specjalny rodzaj konta, nieprzypisany żadnemu użytkownikowi, wymagany do poprawnej pracy systemów informatycznych.
28. **Koncie wyłączonym** – należy przez to rozumieć konto, które zostało zablokowane przez administratora systemu i nie jest dostępne do użycia.
29. **Systemie merytorycznym** – należy przez to rozumieć dedykowany zespół aplikacji służący do przetwarzania określonych danych. System ten wykorzystywany jest przez komórki organizacyjne w celu wypełniania swoich zadań.
30. **Sumie kontrolnej** – należy przez to rozumieć liczbę uzyskaną w wyniku sumowania lub wykonania innych operacji matematycznych na przesyłanych danych, przesłaną razem z danymi i służącą do sprawdzania poprawności przetwarzanych danych.
31. **Logu** (plik dziennika, rejestr zdarzeń) – należy przez to rozumieć chronologiczny zapis

zawierający informację o zdarzeniach i działaniach dotyczących systemu komputerowego.

32. **Napędzie taśmowym** (lub streamerze) – należy przez to rozumieć urządzenie do przenoszenia danych z systemów komputerowych na taśmę magnetyczną w celu archiwizacji lub zabezpieczenia przed utratą danych.
33. **Stacji roboczej** – należy przez to rozumieć system komputerowy przy użyciu którego użytkownik dokonuje przetwarzania danych w systemie informatycznym.
34. **Licencji** – należy przez to rozumieć umowę określającą warunki korzystania z aplikacji komputerowej, zawieraną pomiędzy podmiotem, któremu przysługują majątkowe prawa autorskie do aplikacji, a podmiotem, który zamierza z danej aplikacji korzystać.
35. **KRI** - ROZPORZĄDZENIE 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
36. **Porozumienie** – rozumie się przez to „Porozumienie w przedmiocie dostępu do systemu informatycznego i powierzenia przetwarzania danych osobowych" pomiędzy IPAW a Urzędem Miasta Wałbrzycha z dnia ...
37. **Infrastruktura UMW** - rozumie się przez to udostępniona na potrzeby Instytucji Pośredniczącej Aglomeracji Wałbrzyskiej Infrastrukturę Informatyczną Urzędu Miejskiego w Wałbrzychu, do której dostęp opisuje Porozumienie.
38. **Dokumentacja UMW** - rozumie się przez to dokumentacje przetwarzania danych osobowych w urzędzie miejskim wprowadzona zarządzeniem nr 947/2014 Prezydenta Miasta Wałbrzycha z w sprawie wprowadzenia dokumentacji przetwarzania danych osobowych w Urzędzie Miejskim w Wałbrzychu,

2. Zasady ogólne

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

2.1. Procedury dotyczące zabezpieczeń użytkowników

2.1.1. Przydział uprawnień do systemów

Cel

Określenie sposobu przydziału uprawnień do systemów dla użytkowników systemu informatycznego.

Opis procedury

Nadanie uprawnień użytkownikowi dokonuje się każdorazowo na wniosek przełożonego Użytkownika poprzez złożenie Karty Uprawnień. Kartę Uprawnień można złożyć wyłącznie za pomocą Formularza złożonego do Działu IT. Karta uprawnień powinna zostać wypełniana przez bezpośredniego przełożonego, który określa w niej systemy merytoryczne, stanowiska komputerowe oraz sieci publiczne, do których dostęp ma mieć pracownik, np: (System OTAGO Moduł Kadry, lub też Internet wraz z pocztą internetową). Kartę uprawnień może wypełnić inna osoba. W takim przypadku wymagana jest akceptacja bezpośredniego przełożonego użytkownika lub osoby przełożonego zastępującej.

W uzasadnionych przypadkach realizujący zmianę uprawnień administrator może zweryfikować aktualności posiadanego przez użytkownika upoważnienia do przetwarzania danych osobowych.

Karta uprawnień służy również do modyfikacji jak i odbierania uprawnień pracownikom.

Przebieg czynności

1. Weryfikacja identyfikatora pracownika w przypadku nowego pracownika nadanie nowego identyfikatora z domyślnym hasłem „P@ssw0rd" (hasło zostaje zmienione przez pracownika przy pierwszym logowaniu do systemu).
2. Weryfikacja praw logowania do komputerów pracownika, w przypadku nowego pracownika nadanie uprawnień do logowania do konkretnych komputerów, w przypadku odebrania praw do logowania w systemie – zablokowanie konta pracownika.
3. Weryfikacja godzin logowania, w przypadku nowego pracownika nadanie domyślnych godzin logowania.

4. Weryfikacja adresu IP komputera – nadanie/odebranie dostępu do internetu.
5. Weryfikacja uprawnień dostępu do serwerów (nadanie/odebranie uprawnień).
6. Weryfikacja uprawnień dostępu do systemów merytorycznych (nadanie/odebranie uprawnień).
7. Powiadomienie pracownika o zmianach w konfiguracji – przekazanie odpowiednich danych.
8. Konfiguracja stanowiska komputerowego pracownika.

2.1.2. **Instalacja oprogramowania dodatkowego**

Cel

Celem instrukcji jest określenie sposobu instalacji oprogramowania dodatkowego.

Opis procedury

Na złożony pisemny wniosek pracownika zaakceptowany przez kierownika komórki organizacyjnej, koordynator Działu IT akceptuje bądź odrzuca prośbę instalacji oprogramowania dodatkowego. Dział IT w zależność od rodzaju oprogramowania (komercyjne/darmowe) dokonuje zakupu oprogramowania, bądź w przypadku oprogramowania darmowego, dokonuje weryfikacji dowodów legalności, następnie instaluje oprogramowanie na komputerze wnioskującego. Dowody legalności wraz z oprogramowaniem zostają złożone do Dziale IT, na czas w którym oprogramowanie będzie zainstalowane na komputerze IPAW. Dezinstalacja oprogramowania, odbywa się również na wniosek.

Osoba odpowiedzialna za wykonanie :

Administrator systemu informatycznego.

Przebieg czynności

1. Akceptacja wniosku o instalację/dezinstalację oprogramowania przez kierownika komórki organizacyjnej.
2. Złożenie wniosku o instalację/dezinstalację oprogramowania.
3. W przypadku akceptacji wniosku przez Działu IT, zakup oprogramowania, bądź zgromadzenie niezbędnych dowodów legalności.
4. W przypadku oprogramowania darmowego, zgromadzenie dowodów legalności.

5. Instalacja oprogramowania na stanowisku komputerowym wnioskodawcy.
6. W przypadku dezinstalacji programu, całkowite usunięcie oprogramowania ze stanowiska komputerowego wnioskodawcy.

2.1.3. **Instalacja oprogramowania prywatnego**

Cel

Celem instrukcji jest określenie sposobu instalacji oprogramowania prywatnego.

Opis procedury

Na złożony pisemny wniosek pracownika zaakceptowany przez kierownika komórki organizacyjnej, Koordynator Działu IT akceptuje bądź odrzuca prośbę instalacji oprogramowania prywatnego. Dział Informatyki po otrzymaniu i weryfikacji dowodów legalności oraz po złożeniu pisemnego oświadczenia użytkownika o przestrzeganiu warunków licencji oprogramowania, instaluje oprogramowanie na komputerze wnioskującego. Dowody legalności wraz z oprogramowaniem zostają złożone do Działu IT na czas, w którym oprogramowanie będzie zainstalowane na komputerze IPAW. Dezinstalacja oprogramowania oraz zwrot dowodów legalności wnioskodawcy, odbywa się również na wniosek.

Osoba odpowiedzialna za wykonanie :

Administrator systemu informatycznego.

Przebieg czynności

1. Akceptacja wniosku o instalację/dezinstalację oprogramowania przez kierownika komórki organizacyjnej.
2. Złożenie wniosku o instalację/dezinstalację oprogramowania.
3. W przypadku akceptacji wniosku dostarczenie oprogramowania wraz z dowodami jego legalności, oraz podpisanie oświadczenia o przestrzeganiu warunków licencyjnych.
4. Weryfikacja legalności oraz zgodności oprogramowania przez pracownika biura.
5. Instalacja oprogramowania na stanowisku komputerowym wnioskodawcy.
6. W przypadku dezinstalacji programu, dezinstalacja oprogramowania na stanowisku

komputerowym wnioskodawcy.

7. W przypadku dezinstalacji programu, zwrot dowodów legalności.

2.1.4. **Rozszerzanie czasu pracy**

Cel

Celem instrukcji jest określenie sposobu rozszerzania czasu pracy użytkowników w systemie informatycznym IPAW.

Opis procedury

Rozszerzenie wynikającego z regulaminu pracy zakresu czasu pracy, odbywa się na złożony za wniosek przełożonego kierowany do Dyrektora IPAW. Zaakceptowany wniosek kierowany jest do Działu Kadr i Płac skąd następnie kierowany jest do Działu IT. Pracownik Działu IT administrator systemu informatycznego zmienia godziny logowania w systemie.

Osoba odpowiedzialna za wykonanie :

Administrator systemu informatycznego.

Przebieg czynności

1. Otrzymanie wniosku zaakceptowanego przez Dyrektora IPAW,
2. Przekazanie wniosku przez Koordynatora Działu IT do realizacji,
   2.1 Zmiana godzin logowania w systemie,
   2.2 Ustawienie powiadomienia o wygaśnięciu dodatkowych godzin,
   2.3 W dniu wygaśnięcia dodatkowego czasu pracy, zmiana godzin logowania w systemie.

2.1.5. **Przydział uprawnień do dostępu zdalnego VPN**

Cel

Celem instrukcji jest określenie sposobu konfiguracji dostępu zdalnego do systemu informatycznego IPAW realizowanego Wirtualną Siecią Prywatną (VPN) dla uprawnionych pracowników IPAW.

Opis procedury

Na złożony pisemny wniosek pracownika zaakceptowany przez kierownika komórki organizacyjnej oraz Administratora Danych koordynator Działu IT wyznacza pracownika będącego jednocześnie Administratorem Systemu Informatycznego odpowiedzialnego za udzielenie dostępu zdalnego. Pracownik kontaktuje się z Użytkownikiem VPN dostarczając „Instrukcję konfiguracji połączenia VPN" oraz ustalając datę i godziny włączenia Centrum Certyfikacji oraz aktywowanie przekierowania. Użytkownik wg instrukcji instaluje certyfikat prywatny oraz zestawia połączenie wdzwaniane. Po przeprowadzeniu testów połączenia Centrum Certyfikacji jest wyłączane a przekierowanie zamykane.

Osoba odpowiedzialna za wykonanie

Koordynator Działu IT wyznacza Administratora Systemu Informatycznego będącego pracownikiem Działu IT odpowiedzialnego za przydzielenie dostępu zdalnego. Odpowiada on za włączenie i późniejsze wyłączenie na serwerach IPAW niezbędnych środków programowych pozwalających na uzyskanie certyfikatu zdalnego dostępu. Konfigurację dostępu zdalnego na zdalnym komputerze wykonuje Użytkownik VPN wg Instrukcji konfiguracji połączenia VPN. Konfigurację dostępu zdalnego na zdalnym komputerze może wykonać Administrator Systemu Informatycznego odpowiedzialny za przydzielenie dostępu zdalnego w przypadku dostarczenia komputera zdalnego do Działu IT(np. komputer typu notebook).

Przebieg czynności

1. Złożenie wniosku o dostęp zdalny.
2. Akceptacja wniosku i wyznaczenie pracownika Działu IT prowadzącego udostępnianie dostępu zdalnego.
3. Dodanie Użytkownika VPN do grupy zabezpieczeń „Użytkownicy VPN".
4. Dostarczenie Użytkownikowi VPN „Instrukcji konfiguracji połączenia VPN" i ustalenie daty i zakresu godzin pobierania certyfikatu.
5. Uruchomienie w ustalonym okresie czasowym Centrum Certyfikacji oraz przekierowania na routerze pozwalającego na zewnętrzny dostęp co Centrum Certyfikacji.
6. Potwierdzenie przez Użytkownika VPN poprawności instalacji certyfikatu dostępu zdalnego.

7. Zestawienie próbnego połączenia.
8. Potwierdzenie skutecznego nawiązania połączenia.
9. Wyłączenie przekierowania i Centrum Certyfikacji.
10. W przypadku udzielenia dostępu czasowego Pracownik Działu IT odpowiadający za jego udostępnienie zobowiązany jest unieważnić certyfikat w zadanym terminie.

2.1.6. **Przydział uprawnień do dostępu zdalnego VPN dla dostawców oprogramowania**

Cel

Celem instrukcji jest określenie sposobu konfiguracji dostępu zdalnego do systemu informatycznego IPAW realizowanego Wirtualną Siecią Prywatną (VPN) dla firm świadczących usługi informatyczne wewnątrz sieci IPAW.

Opis procedury

Na pisemny wniosek firmy zewnętrznej zaakceptowany przez Administratora Danych koordynator Działu IT wyznacza pracownika będącego jednocześnie Administratorem Systemu Informatycznego odpowiedzialnego za udzielenie dostępu zdalnego. Pracownik kontaktuje się z Użytkownikiem VPN dostarczając „Instrukcja konfiguracji połączenia VPN" oraz ustalając datę i godziny włączenia Centrum Certyfikacji oraz aktywowanie przekierowania. Użytkownik wg instrukcji instaluje certyfikat prywatny oraz zestawia połączenie wdzwaniane. Po przeprowadzeniu testów połączenia Centrum Certyfikacji jest wyłączane a przekierowanie zamykane. Wyłączane jest też konto Active Directory Użytkownika VPN do czasu, kiedy zażąda on dostępu do systemu.

Osoba odpowiedzialna za wykonanie

Koordynator Działu IT wyznacza Administratora Systemu Informatycznego będącego pracownikiem Działu IT odpowiedzialnego za przydzielenie dostępu zdalnego. Odpowiada on za włączenie i późniejsze wyłączenie na serwerach IPAW niezbędnych środków programowych pozwalających na uzyskanie zdalnego dostępu. Konfigurację dostępu zdalnego na zdalnym komputerze wykonuje Użytkownik VPN wg Instrukcji konfiguracji połączenia VPN. Konfigurację dostępu zdalnego na zdalnym komputerze może wykonać Administrator Systemu Informatycznego odpowiedzialny za przydzielenie dostępu zdalnego w przypadku dostarczenia komputera zdalnego

do Działu IT (np. komputer typu notebook).

Przebieg czynności

1. Złożenie wniosku o dostęp zdalny i akceptacja regulaminu dostępu zdalnego dla firm zewnętrznych.
2. Akceptacja wniosku i wyznaczenie pracownika Działu IT prowadzącego udostępnianie dostępu zdalnego.
3. Konfiguracja i odblokowanie konta użytkownika Active Directory dla Użytkownika VPN. Dodanie do grupy zabezpieczeń „Użytkownicy VPN".
4. Dostarczenie Użytkownikowi VPN „Instrukcji konfiguracji połączenia VPN" i ustalenie daty i zakresu godzin pobierania certyfikatu.
5. Uruchomienie w ustalonym okresie czasowym Centrum Certyfikacji oraz przekierowania na routerze pozwalającego na zewnętrzny dostęp co Centrum Certyfikacji.
6. Potwierdzenie przez Użytkownika VPN poprawności instalacji certyfikatu dostępu zdalnego.
7. Zestawienie próbnego połączenia.
8. Potwierdzenie skutecznego nawiązania połączenia.
9. Wyłączenie przekierowania i Centrum Certyfikacji.
10. Wyłączenie konta Active Directory użytkownika VPN.
11. W przypadku udzielenia dostępu czasowego ustawienie zdarzenia w terminarzu „BI wspólny" przypominającego konieczność likwidacji konta i unieważnienia certyfikatu w zadanym terminie.

2.1.7. **Wdrożenie nowego stanowiska komputerowego**

Cel

Celem instrukcji jest określenie sposobu wdrażania nowego stanowiska komputerowego.

Opis

Wdrożenia nowego stanowiska komputerowego odbywa się na złożony pisemny wniosek przełożonego kierowany do Dyrektora IPAW. Zaakceptowany przez Dyrektora IPAW wniosek kierowany jest do Działu IT. Po zaakceptowaniu wniosku przez Koordynatora Działu IT, w

zależności od ilości posiadanego sprzętu, licencji oraz możliwości ewentualnego ich zakupu, Dział IT wybiera rodzaj odpowiedniego sprzętu do wydania.

Osoba odpowiedzialna za wykonanie :

Administrator systemu informatycznego.

Przebieg czynności

1. Złożenie wniosku zaakceptowanego przez Dyrektora IPAW w Dziale IT,
2. W przypadku braku akceptacji przez Koordynatora Działu poinformowanie wnioskującego,
3. Akceptacja wniosku przez Koordynatora Działu,
   3.1. Sprawdzenie czy są możliwości techniczne podłączenia od sieci nowego sprzętu,
   3.2. Sprawdzenie czy na stanie Działu IT znajduje się odpowiedni sprzęt,
   3.3. Sprawdzenie czy Dział posiada odpowiednią liczbę wymaganych na danym stanowisku licencji,
   3.4. W przypadku braku sprzętu lub licencji na stanie określenie możliwości i zasadności zakupu ich poniżej progów,
   3.5. Określenie możliwości finansowych zakupu sprzętu i ewentualnych licencji,
   3.6. W przypadku braku możliwości zakupu sprzętu powiadomienie wnioskującego o zaistniałych okolicznościach,
   3.7. Wybór odpowiedniego sprzętu lub licencji do zakupu,
   3.8. Zakup poniżej progów lub też dołączenie zakupu sprzętu do następnego zamówienia publicznego,
   3.9. Zakup sprzętu,
   3.10. Wdrożenie sprzętu.
   3.11. Aktualizacja Ewidencji Sprzętu Komputerowego.
   3.12. Zamknięcie sprawy.

2.1.8. **Zmiana miejsca użytkowania sprzętu komputerowego**

Cel

Celem instrukcji jest określenie sposobu zmiany lokalizacji sprzętu i urządzeń komputerowych,

zmiany użytkownika komputera, czy tez przeniesienie sprzętu między jednostkami.

Opis procedury

Jakakolwiek zmiana lokalizacji sprzętu i urządzeń komputerowych, zmiana użytkownika komputera, czy też przeniesienie sprzętu między jednostkami jest możliwa jedynie na złożony pisemny wniosek kierowany do Działu IT. Po rozpatrzeniu zasadności wniosku, jego akceptacji przez koordynatora Działu IT, oraz istniejących możliwościach technicznych zmiany lokalizacji sprzętu komputerowego, pracownicy biura dokonują zmiany miejsca użytkowania sprzętu.

Osoba odpowiedzialna za wykonanie :

Administrator systemu informatycznego.

Przebieg czynności

1. Złożenie wniosku zatwierdzonego przez kierownika komórki organizacyjnej.
2. Sprawdzenie możliwości technicznych przeniesienia sprzętu.
3. Akceptacja wniosku przez Koordynatora Działu IT.
4. Przeniesienie sprzętu/zmiana użytkownika/przeniesienie między jednostkami.

2.2. Procedury dotyczące zabezpieczeń systemów

2.2.1. Tworzenie, kopii bezpieczeństwa na żądanie.

Cel

Określenie sposobu i zakresu tworzenia kopii bezpieczeństwa na żądanie.

Opis procedury

Termin :

Kopie są wykonywane regularnie zgodnie z ustalonym harmonogramem tworzenia kopii opisanym w dokumentacji UMW. Dział IT może zażądać od Biura Informatyki IPAW Miejskiego wykonania i udostępnienia kopi zapasowej z wskazanych zasobów.

Osoba odpowiedzialna za wykonanie :

Administrator systemu informatycznego

Przebieg czynności

1. Złożenie prośby o usługę w systemie Qdesk Urzędu Miejskiego w Wałbrzychu do którego skrót znajduje się na pulpicie. W prośbie o usługę należy wskazać:
   - Zasoby danych których kopię chcemy wykonać,
   - Sposób zabezpieczenia danych (szyfrowania)
   - Miejsce w zasobach wspólnych w którym kopia ma zostać udostępniona Administratorowi systemu informatycznego.
2. Pracownik Biura Informatyki Realizujący zgłoszenie, przekaże kopie wskazanych zasobów, oraz poświadczenia niezbędne do ich odtworzenia.

2.2.2. **Odtworzenie, kopii bezpieczeństwa na żądanie.**

Cel

Określenie sposobu i zakresu odtworzenia kopii bezpieczeństwa na żądanie.

Opis procedury

Termin :

Kopie są wykonywane regularnie zgodnie z ustalonym harmonogramem tworzenia kopii opisanym w dokumentacji UMW. Dział IT może zażądać od Biura Informatyki IPAW Miejskiego odtworzenia i udostępnienia kopi zapasowej z wskazanych zasobów.

Osoba odpowiedzialna za wykonanie :

Administrator systemu informatycznego

Przebieg czynności

1. Złożenie prośby o usługę w systemie Qdesk Urzędu Miejskiego w Wałbrzychu do którego skrót znajduje się na pulpicie. W prośbie o usługę należy wskazać:
   - Zasoby danych których kopię chcemy odtworzyć,

- Datę okresu z którego dane chcemy odtworzyć.
- Sposób zabezpieczenia danych (szyfrowania)
- Miejsce w zasobach wspólnych w którym kopia ma zostać udostępniona Administratorowi systemu informatycznego.

2. Pracownik Biura Informatyki Realizujący zgłoszenie, przekaże kopie wskazanych zasobów, oraz poświadczenia niezbędne do ich odtworzenia.

2.2.3. **Dostęp do pomieszczeń, szaf i urządzeń informatycznych**

Cel

Określenie sposobu dostępu, rodzajów zabezpieczeń oraz osób uprawnionych do pomieszczeń, w których eksploatowane są urządzenia informatyczne.

Opis procedury

Osoba odpowiedzialna za wykonanie :

Nadzór i kontrolę dostępu do pomieszczeń, wyposażonych w urządzenia i sprzęt informatyczny sprawuje Koordynator Działu IT.

Przebieg czynności

1. Osobami uprawnionymi do przebywania w pomieszczeniach są wyłącznie pracownicy wyznaczeni przez Koordynatora Działu IT.
2. Przebywanie osób uprawnionych w pomieszczeniach poza godzinami pracy jest dozwolone tylko za zgodą lub na polecenie Koordynatora Działu IT, zaakceptowane przez Dyrektora IPAW.
3. Dostęp do pomieszczeń oraz szaf i urządzeń informatycznych jest zabezpieczony zamkami patentowymi i/lub kratą.
4. Klucze do pomieszczeń Działowych są każdorazowo przed rozpoczęciem pracy pobierane za potwierdzeniem z portierni.
5. Klucze do pomieszczeń serwerowni oraz szaf krosowniczych i innych urządzeń informatycznych są przechowywane w Dziale IT. Dodatkowo na portierni przechowywane są

klucze zapasowe, wydawane tylko pracownikom Działu IT

6. Nadzór i kontrolę nad kluczami będącymi w dyspozycji Działu IT pełni Koordynator Działu IT.
7. Pomieszczenia oraz szafy, w których znajdują się urządzenia i sprzęt informatyczny należy zamykać na czas nieobecności w nich osób uprawnionych, w sposób uniemożliwiający dostęp do nich osób trzecich.
8. Dostęp do pomieszczeń i/lub urządzeń osób nieuprawnionych musi być każdorazowo zgłoszony Koordynatorowi Działu IT.
9. Koordynator Działu IT uzgadnia ze zgłaszającym termin i rodzaj wykonywanych prac oraz wyznacza osobę, która będzie nadzorować przebieg prac w tym czasie.
10. Przebywanie w pomieszczeniach osób trzecich jest możliwe tylko w obecności i pod nadzorem osoby uprawnionej.

2.2.4. **Udostępnianie sprzętu firmom zewnętrznym**

Cel

Określenie zasad użyczania sprzętu komputerowego będącego w posiadaniu IPAW w Wałbrzychu.

Opis procedury

Osoba odpowiedzialna za wykonanie :

Administrator systemu informatycznego

Założenia wstępne

Udostępnianie sprzętu poza siedzibę IPAW ma miejsce w następujących przypadkach:

1. Sprzęt uległ uszkodzeniu
   - urządzenie jest na gwarancji i podlega naprawie gwarancyjnej,
   - urządzenie nie może być naprawione w siedzibie IPAW z powodu braku części i/lub wymaganych narzędzi,
2. Sprzęt jest elementem zasobów IPAW podlegających udostępnieniu.

Przebieg czynności

1. Urządzenie przeznaczone do naprawy jest każdorazowo weryfikowane w celu identyfikacji obecności danych podlegających ochronie.
2. Zabezpieczenie danych zawartych na nośnikach informacji jest realizowane poprzez fizyczne usunięcie nośnika z urządzenia. W przypadku uszkodzenia nośnika lub braku możliwości jego demontażu, dane z naprawianego urządzenia są bezwzględnie, w sposób trwały, usuwane.
3. Udostępnienie sprzętu odbywa się na podstawie zgłoszenia. Zgłoszenie powinno zawierać następujące informacje :
   - rodzaj sprzętu (nazwa),
   - dane wnioskodawcy oraz osoby odpowiedzialnej za sprzęt,
   - wskazanie przeznaczenia sprzętu,
   - wskazanie miejsca użytkowania sprzętu,
   - termin (w jakim okresie sprzęt będzie używany).
4. Na podstawie zgłoszenia pracownik Działu IT określa dostępność urządzenia.
5. Przekazanie oraz zwrot sprzętu odbywa się na podstawie listu przewozowego, wpisu w zeszyt wypożyczeń, protokołu serwisowego lub innego dokumentu pozwalającego zdefiniować odpowiedzialność za sprzęt poza urzędem.
6. Pracownik Działu IT dokonuje przeglądu sprzętu przed każdym wydaniem / zwrotem urządzenia pod kątem sprawności i kompletności.
7. Fakt uszkodzenia sprzętu, z wyjątkiem sprzętu przekazanego do naprawy, jest odnotowywany na dokumencie z pkt. 6.

2.2.5. **Złomowanie zużytego sprzętu komputerowego**

Cel

Celem instrukcji jest zdefiniowanie zasad kwalifikacji i przeprowadzenia złomowania zużytego sprzętu komputerowego.

Opis procedury

Termin :

Złomowanie sprzętu jest przeprowadzane w miarę potrzeb

Osoba odpowiedzialna za wykonanie :

Administrator systemu informatycznego

Przebieg czynności

1. Pracownik Działu IT przygotowuje urządzenie zakwalifikowane do złomowania poprzez :
   - trwałe usunięcie danych zawartych na nośnikach informacji,
   - umieszczenie etykiety „do złomowania" w widocznym miejscu urządzenia,
   - dodanie urządzenia do listy sprzętu przeznaczonego do złomowania
2. Sprzęt może być przekazywany tylko firmie posiadającej uprawnienia do utylizacji sprzętu elektronicznego.
3. Termin, miejsce oraz wykaz sprzętu przeznaczonego do złomowania jest zgłaszany komisji likwidacyjnej.
4. Przekazanie sprzętu do złomowania jest możliwe wyłącznie w obecności i pod nadzorem przynajmniej jednego członka komisji likwidacyjnej.
5. Przekazanie sprzętu uprawnionej firmie jest potwierdzone protokołem.
6. Usunięcie sprzętu jest każdorazowo rejestrowane w ewidencji sprzętu i oprogramowania.

2.2.6. **Udostępnianie i przekazywanie danych, w tym danych poufnych i osobowych**

Cel

Określenie zasad udostępniania danych oraz sposobu na bezpieczne przekazywanie danych.

Opis procedury

Osoba odpowiedzialna za wykonanie :

Administrator Danych

Przebieg czynności

1. Dane udostępniane są na pisemny lub elektroniczny, podpisany kwalifikowanym podpisem elektronicznym, wniosek.
2. Wniosek akceptuje Administrator Danych.
3. W przypadku danych osobowych lub o charakterze poufnym zachodzi konieczność podpisania umowy o powierzaniu danych pomiędzy IPAW a Odbiorcą danych.
4. W przypadku udostępniania danych jawnych pracownik udostępniający może podjąć decyzję o ich szyfrowaniu. W przypadku danych osobowych i poufnych szyfrowanie jest obligatoryjne.
5. W przypadku kiedy Odbiorca danych posiada odpowiednie środki, szyfrowanie może odbywać się za pomocą certyfikatu klucza publicznego podpisu kwalifikowanego Odbiorcy danych. W pozostałych przypadkach dane zabezpiecza się na czas dostarczenia w następujących reguł:
   - Dane szyfruje się za pomocą losowo wygenerowanego klucza i dostarcza Odbiorcy danych,
   - Wytyczne algorytmów szyfrowania i długości klucza znajdują się w dokumencie nadrzędnym – Instrukcja zarządzania systemem informatycznym.
   - Innym kluczem, w postaci hasła, szyfrowany jest klucz szyfrujący,
   - Odbiorca danych odbiera zaszyfrowane dane i potwierdza ich odbiór,
   - Odbiorca danych odbiera zaszyfrowany klucz szyfrujący i potwierdza jego odbiór,
   - Pracownik udostępniający przekazuje, innym kanałem niż dane i klucz szyfrujący, hasło do odszyfrowania klucza szyfrującego,
   - Odbiorca danych deszyfruje klucz szyfrujący oraz dane i potwierdza poprawność deszyfracji.

2.3. Procedury cykliczne dotyczące zabezpieczeń

2.3.1. Kontrola godzin logowania

Cel

Celem instrukcji jest określenie sposobu cyklicznej kontroli ustawień czasu logowania do systemu informatycznego IPAW.

Opis procedury

Termin :

Kontrola ustawienia godzin logowania do systemu informatycznego przeprowadzana jest w ostatnim tygodniu każdego kwartału.

Osoba odpowiedzialna za wykonanie :

Administrator systemu informatycznego.

Przebieg czynności

1. Administrator przy użyciu narzędzi systemowych określa konta użytkowników, których atrybut logowania w określonych godzinach nie jest zgodny z przyjętym standardowym zakresem czasu pracy w systemie informatycznym.
2. Administrator dla każdego otrzymanego w wyniku konta sprawdza rodzaj i uprawnienia konta:
   - Jeśli konto jest kontem systemowym weryfikacja godzin logowania dla tego konta kończy się.
   - Jeśli konto jest wyłączone wszystkie dostępne godziny logowania są usuwane.
3. Administrator, na podstawie karty uprawnień oraz wniosków o przedłużenie czasu pracy weryfikuje i aktualizuje ustawienia godzin logowania dla tego konta.

2.3.2. **Kontrola uprawnień do systemów merytorycznych**

Cel

Celem procedury jest określenie sposobu i warunków cyklicznej kontroli uprawnień do systemów merytorycznych wykorzystywanych w systemie informatycznym IPAW.

Opis procedury

Termin :

Kontrola uprawnień do wszystkich systemów merytorycznych wykonywana jest względem każdego użytkownika raz na 12 miesięcy.

Osoba przeprowadzająca kontrolę:

Administrator systemów informatycznych.

Systemy podlegające kontroli :

Kontroli podlegają wszystkie systemy wchodzące w skład systemu informatycznego IPAW, w szczególności służące do prowadzenia wszelkiego rodzaju rejestrów i ewidencji, wykorzystywane do przetwarzania danych osobowych, finansowych i innych wymaganych przez daną jednostkę organizacyjną do sprawnego działania i realizacji powierzonych jej zadań.

Zakres kontroli

Kontrola przeprowadzana jest w zakresie określenia czy użytkownik posiada uprawnienia wymagane do pracy w systemie informatycznym IPAW zgodnie z kartą uprawnień jednostkowych.

Przebieg czynności

1. Kontrola uprawnień do systemów merytorycznych na podstawie indywidualnych kart uprawnień jednostkowych użytkowników:
   - kontrola ważności konta,
   - kontrola uprawnień w systemach, do których dostęp został przyznany na podstawie karty uprawnień jednostkowych,
   - kontrola uprawnień w systemach, do których dostęp nie został przyznany na podstawie karty uprawnień jednostkowych, ale które są zainstalowane na stacji roboczej i jest możliwe ich uruchomienie.
2. Jeśli przeprowadzona kontrola wykazała odstępstwa rzeczywistych uprawnień od tych określonych w karcie uprawnień jednostkowych dostęp do systemu lub danej jego funkcji zostaje niezwłocznie zablokowany.
3. Tworzony jest zbiorczy raport z przebiegu kontroli uprawnień do systemów merytorycznych.

2.3.3. Kontrola przestrzegania procedur zabezpieczeń

Cel

Celem procedury jest określenie sposobu i warunków wyrywkowej kontroli przestrzegania procedur zabezpieczeń w systemie informatycznym IPAW.

Opis procedury

Termin :

Kontrola przestrzegania procedur zabezpieczeń wykonywana jest w sposób wyrywkowy, poza godzinami pracy IPAW, bez uprzedniego określania planu jej przeprowadzania i bez powiadamiania o niej użytkowników.

Osoba przeprowadzająca kontrolę :

Administrator systemów informatycznych.

Systemy podlegające kontroli :

Kontroli podlegają wszystkie systemy komputerowe użytkowników, miejsca instalacji oraz ich najbliższe otoczenie.

Zakres kontroli

W ramach kontroli przestrzegania procedur zabezpieczeń przeprowadzane są działania określone w:

- procedurze kontroli uprawnień do systemów merytorycznych,
- procedurze kontroli godzin logowania do systemu informatycznego,
- procedurze przeprowadzania audytów oprogramowania (z wyłączeniem warunku obecności użytkownika stacji roboczej w trakcie przeprowadzania audytu).

Dodatkowo przeprowadzane są działania mające na celu:

- kontrolę czy hasła, numery PIN, karty inteligentne lub inne elektroniczne środki uwierzytelniania w systemie informatycznym IPAW nie zostały udostępnione innym osobom oraz czy sposób ich przechowywania może doprowadzić do ich kompromitacji,
- kontrolę czy sposób ustawienia monitorów ekranowych, drukarek lub innych urządzeń służących do prezentacji danych nie powodują możliwości uzyskania lub przejęcia danych

przez osoby nieupoważnione,

- kontrolę czy nie naruszono pozostałych zasad i procedur zabezpieczeń.

Przebieg czynności

1. Kontrola przestrzegania procedur zabezpieczeń wykonywana jest na wybranych systemach komputerowych użytkowników poprzez:
   - kontrolę uprawnień do systemów merytorycznych zgodnie z obowiązującą procedurą,
   - kontrolę godzin logowania do systemu informatycznego zgodnie z obowiązującą procedurą,
   - przeprowadzenie audytu oprogramowania zgodnie z obowiązującą procedurą,
   - kontrolę stanowiska pracy w celu wykrycia naruszeń zasad bezpieczeństwa.
2. W przypadku stwierdzenia nieprawidłowości osoba przeprowadzająca kontrolę niezwłocznie podejmuje wszystkie niezbędne kroki określone w odpowiednich procedurach zmierzające do ich usunięcia.
3. W pierwszy dzień roboczy przepadający po dniu kontroli, przełożony użytkowników, których systemy i stanowiska komputerowe podlegały kontroli, zostaje powiadomiony o jej wynikach i wykrytych nieprawidłowościach.

2.3.4. **Kontrola stanu urządzeń informatycznych**

Cel

Celem procedury jest określenie stanu wyeksploatowania oraz wymaganych konserwacji urządzeń informatycznych IPAW.

Opis procedury

Termin :

Kontrolę stanu urządzeń informatycznych przeprowadzana jest na podstawie harmonogramu przeglądów przygotowywanego na rok przez Dział IT i zatwierdzonego przez Koordynatora Działu IT.

Osoby przeprowadzające przegląd

1. Administrator systemów informatycznych.
2. Pracownicy firm zewnętrznych posiadający wymagane uprawnienia (pod nadzorem administratora systemów informatycznych).

Urządzenia podlegające przeglądowi.

1. Aktywne urządzenia sieciowe.
2. Systemy komputerowe pełniące rolę serwerów.
3. Urządzenia składowania danych.
4. Urządzenia zapewniające ciągłość zasilania.
5. Urządzenia zapewniające optymalne warunki środowiskowe miejsca instalacji pozostałych urządzeń.
6. Okablowanie informatyczne i zasilające sieć informatyczną.
7. Wszelkie urządzenia informatyczne w stosunku do których administrator systemu zlecił lub przeprowadził czynności serwisowe.

Warunki przeprowadzenia przeglądu

1. Przegląd danego urządzenia może zostać przeprowadzony pod warunkiem, że nie zakłóci ciągłości pracy IPAW. Wyjątkiem jest sytuacja, w której urządzenie w wyniku dalszej swojej pracy może ulec uszkodzeniu lub doprowadzić do uszkodzenia innych urządzeń.
2. Warunki i zakres przeglądu oraz uprawnienia pracowników firm zewnętrznych przeprowadzających przegląd i/ ewentualną konserwację określa stosowna umowa.
3. Warunki na których firmy zewnętrzne i ich pracownicy uzyskują dostęp do pomieszczeń i urządzeń definiują:
   - Procedura udostępniania sprzętu firmom zewnętrznym,
   - Procedura dostępu do pomieszczeń, szaf i urządzeń informatycznych.

Zakres przeglądu

1. Kontrola warunków środowiskowych w miejscu pracy urządzenia (temperatura i wilgotność powietrza, zapylenie).
2. Kontrola poprawności zasilania urządzenia.

3. Kontrola czynników, które mogą doprowadzić do uszkodzenia urządzenia lub negatywnie wpłynąć na poprawność jego działania.
4. Kontrola podłączenia i działania komponentów urządzenia.
5. Test odporności urządzenia na awarię systemu zasilania.

Przebieg czynności

1. Administrator systemu opracowuje plan przeglądu zgodny z zakresem i warunkami jej przeprowadzenia.
2. Jeżeli administrator systemu uzna w trakcie przeglądu, że jedno lub wiele urządzeń wymaga naprawy lub konserwacji w miarę możliwości wykonuje się te czynności bez zbędnej zwłoki.
3. Jeśli administrator systemu posiada odpowiednie uprawnienia wymagane do ingerencji w wewnętrzną budowę urządzenia, przystępuje do wykonania naprawy lub konserwacji. Jeśli do przeprowadzenia naprawy lub konserwacji urządzenia wymagane są specjalne uprawnienia, przeprowadzana jest ona przez pracownika firmy zewnętrznej, który nabył odpowiednie uprawnienia.
4. Jeśli naprawa lub konserwacja dokonywana jest w miejscu instalacji urządzenia, następuje ona zgodnie z procedurą dostępu do pomieszczeń, szaf i urządzeń informatycznych. Jeśli na czas naprawy lub konserwacji wymagane jest wydanie urządzenia firmie zewnętrznej, następuje ono zgodnie z procedurą udostępniania sprzętu firmom zewnętrznym.
5. Po przeglądzie urządzenia tworzony jest jednostkowy raport z jej przebiegu.
6. Po wykonaniu planu przeglądów urządzeń administrator systemu na podstawie raportów jednostkowych tworzy raport zbiorczy zawierający m.in:
   - listę przeglądanych urządzeń,
   - wykaz stwierdzonych nieprawidłowości,
   - wykaz napraw i konserwacji, wykonanych podczas przeglądu,
   - listę zaleceń pokontrolnych osoby przeprowadzającej przegląd.

2.3.5. **Audyty oprogramowania**

Cel

Celem procedury jest określenie sposobu i warunków cyklicznego przeprowadzania audytów oprogramowania wykorzystywanego w systemie informatycznym IPAW.

Opis procedury

Termin:

Audyty oprogramowania wykorzystywanego w systemie informatycznym IPAW wykonywane są raz do roku.

Osoba przeprowadzająca audyt

1. Administrator systemów informatycznych.
2. Pracownicy firm zewnętrznych posiadający wymagane uprawnienia (pod nadzorem administratora systemów informatycznych).

Audytowi podlegają

1. Systemy komputerowe wszystkich pracowników IPAW.
2. Systemy komputerowe pełniące rolę serwerów.

Warunki przeprowadzenia

1. Audyt oprogramowania serwerów może zostać przeprowadzony wyłącznie w obecności administratora systemów informatycznych.
2. Audyt nie może zostać przeprowadzony jeśli zakłóciłby działanie newralgicznych elementów systemu informatycznego lub utrudnił wykonywanie pełnionych przez IPAW zadań.
3. Warunki i zakres przeprowadzenia audytu oprogramowania przez pracowników firm zewnętrznych określa stosowna umowa.
4. Warunki na których pracownicy firm zewnętrznych uzyskują dostęp do pomieszczeń i urządzeń w celu przeprowadzenia audytu definiują:
   - Procedura udostępniania sprzętu firmom zewnętrznym,
   - Procedura dostępu do pomieszczeń, szaf i urządzeń informatycznych.

Zakres

Czynności wykonywane w ramach audytu oprogramowania:

Audyt wykonywany jest zdalnie, bez konieczności informowania pracowników.

Przy użyciu programu do audytu identyfikowana jest liczba zainstalowanych aplikacji w systemach komputerowych i porównywana ze stanem ewidencji sprzętu i oprogramowania.

Niezgodności są weryfikowane poprzez porównanie wyników skanowania ze spisem zainstalowanych aplikacji wyeksportowanym z rejestru każdej stacji. Następnie sprawdzana jest poprawność instalacji oprogramowania, celem wyeliminowania oprogramowania, które zostało „fizycznie" usunięte z komputera.

W przypadku stwierdzenia niezgodności, bądź problemów z przeprowadzeniem audytu zdalnie, audyt jest wykonywany przez Administratora Systemu na stacji klienckiej, bądź w oparciu o dane wyeksportowane z rejestru systemowego.

Dodatkowo zdalnie sprawdzana jest zawartość dysków twardych w poszukiwaniu treści chronionych prawem autorskim, lub zawierających dane osobowe, które powinny być szyfrowane.

Przebieg czynności

1. Administrator systemu opracowuje plan przeprowadzenia audytu oprogramowania zgodny z zakresem i warunkami jego przeprowadzenia.
2. Jeśli audyt przeprowadzany jest przez pracowników firmy zewnętrznej, następuje on zgodnie z procedurą dostępu do pomieszczeń, szaf i urządzeń informatycznych oraz procedurą udostępniania sprzętu firmom zewnętrznym.
3. Przeprowadzenie audytu zgodnie z zakresem.
4. Po wykonaniu planu przeprowadzenia audytu administrator tworzy raport zbiorczy zawierający m. in:
   - listę stwierdzonych nieprawidłowości,
   - wykaz czynności podjętych z celu ich usunięcia,
   - listę zaleceń pokontrolnych osoby przeprowadzającej audyt.

TYTUŁ OPRACOWANIA:	**Opis sieci komputerowej IPAW.**		
OPRACOWAŁ:	***Sebastian Węgrzynkiewicz*** Imię i nazwisko	Podpis	Data
SPRAWDZIŁ:	Imię i nazwisko	Podpis	Data
		Podpis	Data
OBOWIĄZUJE OD DNIA:			

Spis treści

1. Definicje

1. **Sieć LAN** - Przez sieć LAN (ang. Local Area Network stąd używany także w języku polskim skrót LAN) należy rozumieć lokalna (wewnętrzną) sieć komputerową Urzędu Miejskiego. Sieć obejmuje swym zasięgiem 5 budynków wykorzystując technologie przewodową, bezprzewodową oraz światłowodową pracującą w standardach IEEE802.3x-Full Duplex Ethernet, IEEE802.3z-1Gb Ethernet, IEEE 802.11g-Wi-Fi.
2. **Sieć światłowodowa** - Przez sieć światłowodową należy rozumieć fragmenty sieci komputerowej Urzędu Miejskiego w których wykorzystano zamiast przewodów miedzianych łącza światłowodowe oraz specjalne konwertery opisane poniżej. Sieć światłowodowa pracująca w standardach 10/100/1000BASE-TX.
3. **Konwerter światłowodowy** - Urządzenie którego zadaniem jest konwersja sygnału danych ze złącza RJ45 na złącze światłowodowe SC.
4. **Sieć Bezprzewodowa** - (skr. WLAN, od ang. Wireless Local Area Network) – sieć lokalna w której połączenia miedzy urządzeniami sieciowymi zrealizowano bez użycia przewodów (np. tzw. kabli miedzianych, czy światłowodów). Sieci tego typu wykonywane są najczęściej z wykorzystaniem mikrofal jako medium przenoszącego sygnały, ale również z użyciem podczerwieni. Są one projektowane w oparciu o standard IEEE 802.11.
5. **Szafa Krosownicza / Szafa Rackowa** - Jest to metalowa szafa, w której umieszczane są w specjalnych rackach serwery oraz aktywne i pasywne urządzenia będące elementami sieci komputerowej oraz urządzenia wspomagające, zabezpieczając przed dostępem osób niepowołanych.
6. **Racki** - To moduły do urządzeń umożliwiające ich montaż w szafie rackowej.
7. **Serwerownia** - wydzielone pomieszczenie będące środowiskiem pracy komputerów pełniących rolę serwerów, a także aktywnych i pasywnych elementów sieci komputerowych. Zabezpieczone przed dostępem osób niepowołanych, klimatyzowane oraz zabezpieczone na wypadek chwilowej utraty zasilania.
8. **Strefa zdemilitaryzowana / strefa ograniczonego zaufania** - (DMZ ang Demilitarized

Zone), jest to w skrócie wydzielony obszar sieci komputerowej nie należący ani do sieci wewnętrznej (tj. tej chronionej przez zaporę), ani do sieci zewnętrznej (tej przed zaporą; na ogół jest to Internet). W strefie zdemilitaryzowanej umieszczane są serwery "zwiększonego ryzyka włamania", przede wszystkim serwery świadczące usługi użytkownikom sieci zewnętrznej, którym ze względów bezpieczeństwa nie umożliwia się dostępu do sieci wewnętrznej. W strefie zdemilitaryzowanej umieszczane są serwery usług świadczonych użytkownikom sieci wewnętrznej, które muszą kontaktować się z obszarem sieci zewnętrznej serwery DNS, proxy, poczty, VPN i inne.

9. **Słowackiego 23A** - Przez „Słowackiego 23A" rozumie się wszystkie pomieszczenia należące do IPAW w budynku przy ul. Słowackiego 23A.
10. **Ratusz** - Przez „Ratusz" rozumie się wszystkie pomieszczenia należące do Urzędu Miejskiego w budynku przy pl. Magistrackim l.
11. **Porozumienie** – rozumie się przez to „Porozumienie w przedmiocie dostępu do systemu informatycznego i powierzenia przetwarzania danych osobowych" pomiędzy IPAW a Urzędem Miasta Wałbrzycha z dnia ...
12. **Infrastruktura UMW** - rozumie się przez to udostępniona na potrzeby Instytucji Pośredniczącej Aglomeracji Wałbrzyskiej Infrastrukturę Informatyczną Urzędu Miejskiego w Wałbrzychu, do której dostęp opisuje Porozumienie.
13. **Dokumentacja UMW** - rozumie się przez to dokumentacje przetwarzania danych osobowych w urzędzie miejskim wprowadzona zarządzeniem nr 947/2014 Prezydenta Miasta Wałbrzycha z w sprawie wprowadzenia dokumentacji przetwarzania danych osobowych w Urzędzie Miejskim w Wałbrzychu,

2. Ogólne Informacje o Sieci

Sieć Instytucji Pośredniczącej Aglomeracji Wałbrzyskiej to wydzielona fizycznie sieć LAN znajdująca się w budynku przy ulicy Słowackiego 23A. Fizycznie siec komputerowa IPAW połączona jest siecią światłowodową z Ratuszem Urzędu Miejskiego w Wałbrzychu. Logicznie natomiast sieć jest wydzieloną podsiecią ze względu na położenie budynku, oraz sprzętowe połączenia między IPAW a Urzędem Miejskim w Wałbrzychu. Budynek posiada własną infrastrukturę sieci w topologi gwiazdy/rozszerzonej gwiazdy wykonanej w technologi Fast Ethernet/Gigabit Ethernet (kategoria 5e, w standardzie TIA/EIA-568-B). Ruch między sieciami jest dozwolony tylko dla administratorów oraz usług administracyjnych.

2.1. *Topologia Fizyczna:*

Rozszerzona Gwiazda

2.2. *Standardy Sieci według IEEE:*

IEEE 802.3x - Full Duplex Ethernet,
IEEE 802.3z - 1 Gb Ethernet,

2.3. *Adresowanie Sieci:*

192.168.154.0/24 - Strefa Zdemilitaryzowana,
10.3.1.0/24 - Podsieć użytkowników IPAW
11.0.5.0/24 - VPN.

3. Budek Sieci IPAW.

3.1. Słowackiego:

Słowackiego jest głównym węzłem sieci IPAW, połączony z Głównym węzłem sieci Urzędu Miejskiego w Wałbrzychu.

Sieć fizyczna Słowackiego składa się z Głownego węzła znajdującego się w wewnętrznym pokoju 306 zwanym Serwerownią. W Szafie koksowniczej Serwerowni znajduje się kolejno:

- Przełącznica sieci LAN,
- Przełącznica Telefoniczna,
- Przełącznica Światłowodowa,

3.2. Uwagi:

Szczegółową dokumentację przebiegu sieci w budynku oraz jej pomiary, jak i dokumentację łącz światłowodowych można odnaleźć w planach instalacji sieci znajdujących się w Dziale IT.

4. Połączenie z internetem

Łącze internetowe dostarczone obecnie w ramach Infrastruktury UMW to asymetryczne łącze o przepustowości 100Mb/s połączenia przychodzące i 20MB/s połączenia wychodzące (technologia ADSL).

Pomiędzy urządzeniami dostawcy internetu, a serwerem zarządzającym dostępem do internetu w ramach infrastruktury UMW pełniącym funkcję routera wewnętrznego oraz zapory sieciowej istnieje specjalna wydzielona strefa zdemilitaryzowana (DMZ).

Dostęp do internetu zarządzany jest poprzez polityki na dwóch urządzeniach, routerze brzegowym oraz wewnętrznym serwerze.

5. Serwery i ich Role

W ramach infrastruktury UMW na potrzeby IPAW został stworzony serwer wirtualny IPAW pełniący rolę serwera bazodanowego. Pozostałe usługi oraz serwery wykorzystywane w ramach infrastruktury UMW opisuje Dokumentacja UMW.

TYTUŁ:	*Instrukcja Postępowania w Sytuacji Naruszenia Bezpieczeństwa Danych Osobowych*		
OPRACOWAŁ:	*Sebastian Węgrzynkiewicz* Imię i nazwisko	Podpis	Data
SPRAWDZIŁ:	Imię i nazwisko	Podpis	Data
ZATWIERDZIŁ:	Imię i nazwisko	Podpis	Data
OBOWIĄZUJE OD DNIA:			

Spis treści

I. Cel

Niniejsza instrukcja reguluje postępowanie pracowników IPAW zatrudnionych przy przetwarzaniu danych osobowych w przypadku stwierdzenia naruszenia bezpieczeństwa danych osobowych (Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie określenia podstawowych warunków technicznych i organizacyjnych jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych)

Celem niniejszej instrukcji jest określenie zadań pracowników w zakresie :

1. ochrony danych osobowych przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą oraz ochroną zasobów technicznych,
2. prawidłowego reagowania pracowników zatrudnionych przy przetwarzaniu danych osobowych w przypadku stwierdzenia naruszenia bezpieczeństwa danych osobowych lub zabezpieczeń systemu informatycznego.

II. Diagnozowanie.

1. Naruszenie systemu ochrony danych osobowych może zostać stwierdzone na podstawie oceny :
    a) stanu urządzeń technicznych,
    b) zawartości zbiorów danych osobowych,
    c) sposobu działania programu lub jakości komunikacji w sieci teleinformatycznej,
    d) metod pracy (w tym obiegu dokumentów).
2. Oznaka, naruszenia zabezpieczenia systemu, świadczą o próbie nielegalnego wejścia w posiadanie danych osobowych, może być w szczególności :
    a) naruszenie haseł dostępu (system nie reaguje na hasło lub je ignoruje – usunięty mechanizm identyfikowania użytkownika poprzez hasło),
    b) częściowy lub całkowity brak bazy danych,
    c) brak możliwości uruchomienia właściwej aplikacji,
    d) naruszenie plomb lub zabezpieczeń mechanicznych sprzętu komputerowego, zmiana położenia lub inne oznaki wskazujące na możliwość dokonania demontażu komputerów,
    e) ślady kradzieży w pomieszczeniu, w którym znajduje się sprzęt komputerowy,
    f) komunikat systemu o otwarciu sesji (dostępu do bazy danych) w czasie nieobecności użytkownika,
    g) ślady naruszenia koperty zawierającej kopie archiwalną.

III. Działania.

W przypadku stwierdzenia naruszenia bezpieczeństwa danych osobowych należy bezzwłocznie :

1. powiadomić Administratora Danych lub kierownika własnej komórki organizacyjnej,
2. zablokować dostęp do systemu dla użytkowników oraz osób nieupoważnionych,
3. podjąć działania mające na celu zminimalizowanie lub całkowite wyeliminowanie powstałego zagrożenia – o ile czynności te nie spowodują przekroczenia uprawnień pracownika,
4. zabezpieczyć dowody umożliwiające ustalenie przyczyn oraz skutków naruszenia bezpieczeństwa systemu,
5. oczekiwać na miejscu zdarzenia na Administratora Danych Informacji lub innej upoważnionej przez niego osoby,
6. kierownik komórki organizacyjnej pracownika po otrzymaniu powiadomienia o naruszeniu bezpieczeństwa danych osobowych jest zobowiązany niezwłocznie powiadomić Administratora Danych.
7. na stanowisku, na którym stwierdzono naruszenie zabezpieczenia danych Administrator Danych i kierownik komórki organizacyjnej pracownika przejmują nadzór nad pracą w systemie odsuwając jednocześnie od stanowiska pracownika, który dotychczas na nim pracował, aż do czasu wydania odmiennej decyzji.

IV. Wnioski.

Administratora Danych lub osoba przez niego upoważniona podejmuje czynności wyjaśniające mające na celu ustalenie :

1. przyczyn i okoliczności naruszenia bezpieczeństwa danych osobowych,
2. osób winnych naruszenia bezpieczeństwa danych osobowych,
3. skutków naruszenia.

V. Obowiązki.

1. Administratora Danych zobowiązany jest do powiadomienia o zaistniałej sytuacji Administratora Danych, który podejmuje decyzje o wykonaniu czynności zmierzających do przywrócenia poprawnej pracy systemu oraz o ponownym przystąpieniu do pracy w systemie.
2. Administratora Danych zobowiązany jest do sporządzenia pisemnego raportu na temat zaistniałej sytuacji na formularzu raportu niezgodności będącego z załącznikiem 1 do

Procedury nadzoru nad produktem niezgodnym.

3. W przypadku, gdy naruszenie bezpieczeństwa danych osobowych zakończyło się kradzieżą danych o fakcie tym Administrator Danych zawiadamia niezwłocznie organy policji lub inne organy ścigania.

VI. Kary.

1. Za naruszenie bezpieczeństwa danych osobowych Administrator Danych może stosować kary porządkowe, niezależnie od zastosowania kar, o których mowa wyżej.
2. Wg Rozdziału 8 Ustawy o Ochronie Danych Osobowych, za naruszanie bezpieczeństwa danych osobowych obowiązują następujące kary:
    a) Kto przetwarza w zbiorze dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do których przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
    b) Kto będąc obowiązany do ochrony danych osobowych udostępnia je lub umożliwia dostęp do nich osobom nieupoważnionym podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
    c) Jeżeli sprawca działa nieumyślnie, podlega grzywnie, karze ograniczenia wolności lub pozbawienia wolności do roku.
    d) Kto narusza choćby nieumyślnie obowiązek zabezpieczenia ich przed zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

TYTUŁ:	***Wzór formularza karty uprawnień jednostkowych***		
OPRACOWAŁ:	*Sebastian Węgrzynkiewicz* Imię i nazwisko	Podpis	Data
SPRAWDZIŁ:	Imię i nazwisko	Podpis	Data
ZATWIERDZIŁ:	Imię i nazwisko	Podpis	Data
OBOWIĄZUJE OD DNIA:			