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

Załącznik Nr 1
do Zarządzenia Nr ...2...../2015
Dyrektora IPAW
z dnia 02.03.2015 r.

POLITYKA BEZPIECZEŃSTWA
INSTYTUCJI POŚREDNICZĄCEJ AGLOMERACJI WAŁBRZYSKIEJ

Spis treści

I.Postanowienia ogólne....3
A.Definicje....3
B.Cel....4
C.Zakres stosowania....5
II.Administrator Danych....5
A.Zadania Administratora Danych....5
III.Obszar przetwarzania danych osobowych....6
IV.Wykaz zbiorów danych osobowych....7
V.Struktury zbiorów danych osobowych oraz sposób przepływu danych....7
VI.Środki Techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych....8
A.Środki ochrony fizycznej....8
B.Środki sprzętowe, informatyczne i telekomunikacyjne....9
C.Środki ochrony w ramach oprogramowania systemu....10
D.Środki ochrony w ramach narzędzi baz danych i innych narzędzi programowych....10
E.Środki ochrony w ramach systemu informatycznego....11
F.Środki organizacyjne....11
G.Odpowiedzialność osób upoważnionych do przetwarzania danych osobowych....13
VII.Postanowienia końcowe....13

I. Postanowienia ogólne

A. Definicje

Ilekroć w niniejszym dokumencie jest mowa o :

1. **IPAW** – należy przez to rozumieć Instytucje Pośredniczącą Aglomeracji Wałbrzyskiej
2. **Zbiorze danych** - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,
3. **Przetwarzaniu danych** - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,
4. **Administratorze Danych** – należy przez to rozumieć Dyrektora Instytucji Pośredniczącej Aglomeracji Wałbrzyskiej
5. **Koordynatora Działu IT** – należy przez to rozumieć pracownika IPAW odpowiedzialnego za funkcjonowanie systemu informatycznego IPAW oraz stosowanie technicznych i organizacyjnych środków ochrony,
6. **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.
7. **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, praktykę, staż w IPAW lub wolontariusz,
8. **sieci lokalnej** - należy przez to rozumieć połączenie systemów informatycznych IPAW wyłącznie dla własnych jej potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnej,
9. **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.

10. **ustawie** – rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r., poz. 1182 z późn. zm) lub inna ustawa, która zastąpi rzeczoną ustawę.
11. **rozporządzeniu** – rozumie się przez to rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U nr 100, poz. 1024),
12. **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 ...
13. **Infrastruktura UMW** - rozumie się przez to udostępniona na potrzeby Instytucji Pośredniczącej Aglomeracji Wałbrzyskiej Infrastrukturę Informatyczną Urzędu Miejskiego w Wałbrzychu, do której dostęp opisuje Porozumienie.

B. Cel

Wdrożenie polityki bezpieczeństwa w IPAW ma na celu zabezpieczenie przetwarzanych przez niego danych osobowych, w tym danych przetwarzanych w systemie informatycznym IPAW i poza nim, poprzez wykonanie obowiązków wynikających z ustawy i rozporządzenia.

W związku z tym, że w zbiorach danych IPAW przetwarzane są między innymi dane wrażliwe, a system informatyczny administratora danych posiada szerokopasmowe połączenie z internetem, niniejsza polityka bezpieczeństwa służy zapewnieniu wysokiego poziomu bezpieczeństwa danych w rozumieniu § 6 rozporządzenia. Niniejszy dokument opisuje niezbędny do uzyskania tego bezpieczeństwa zbiór procedur i zasad dotyczących przetwarzania danych osobowych oraz ich zabezpieczenia.

C. Zakres stosowania

1. Niniejsza polityka bezpieczeństwa dotyczy zarówno danych osobowych przetwarzanych w sposób tradycyjny w księgach, wykazach i innych zbiorach ewidencyjnych, jak i w systemach informatycznych.
2. Procedury i zasady określone w niniejszym dokumencie stosuje się do wszystkich osób upoważnionych do przetwarzania danych osobowych, zarówno zatrudnionych, jak i innych, np. wolontariuszy, praktykantów, stażystów.

II. Administrator Danych

A. Zadania Administratora Danych

Administrator Danych realizuje zadania w zakresie nadzoru nad przestrzeganiem zasad ochrony danych osobowych, w tym zwłaszcza:

1. sprawdza zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych,
2. zapewnia zapoznanie się osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych,
3. sprawuje nadzór nad wdrożeniem stosownych środków fizycznych, a także organizacyjnych i technicznych – w celu zapewnienia bezpieczeństwa danych,
4. sprawuje nadzór nad funkcjonowaniem systemu zabezpieczeń, w tym także nad prowadzeniem ewidencji z zakresu ochrony danych osobowych,
5. nadzoruje udostępnianie danych osobowych odbiorcom danych i innym podmiotom,
6. przygotowuje wnioski zgłoszeń rejestracyjnych i aktualizacyjnych zbiorów danych oraz prowadzi inną korespondencję z Generalnym Inspektorem Danych Osobowych,
7. zatwierdza wzory dokumentów (odpowiednie klauzule w dokumentach) dotyczących ochrony danych osobowych, przygotowywane przez komórki organizacyjne IPAW.
8. nadzoruje prowadzenie ewidencji i innej dokumentacji z zakresu ochrony danych

osobowych,

9. prowadzi oraz aktualizuje dokumentację opisującą sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych,
10. podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia systemu informatycznego,
11. zatwierdza materiały szkoleniowe z zakresu ochrony danych osobowych i nadzoruje szkolenia osób upoważnianych do przetwarzania danych osobowych,
12. prowadzi rejestru zbiorów danych przetwarzanych z wyjątkiem zbiorów, o których mowa w art. 43 ust. 1 ustawy, zawierającego nazwę zbioru oraz informacje, o których mowa w art. 41 ust. 1 pkt 2-4a i 7 ustawy.

III. Obszar przetwarzania danych osobowych.

Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe;

1. Obszarem, w którym przetwarzane są dane osobowe jest Infrastruktura UMW oraz niżej wymienione pomieszczenia w budynku:
   a) budynek przy ul. Słowackiego 23A;
      - pomieszczenia Działu IT:
        - pokój 306,
        - wewnętrzny pokój w pokoju 306 oznaczony jako Serwerownia,
      - pomieszczenia Działu Finansów, Płatności i Windykacji
        - pokój 305,
      - pomieszczenia w pokoju 203:
        - pokój Dyrektora,
        - pokój Zastępcy Dyrektora,
        - pokój Działu Kontraktacji, Rozliczeń i Sprawozdawczości Operacji Sektora Gospodarczego,
        - pokój Działu Obsługi Naborów, Informacji i Promocji,

- pokoju 205 oznaczony jako 205a:
  - pokój wewnętrzny w pokoju 205 Działu Kontraktacji, Rozliczeń i Sprawozdawczości Operacji Sektora Publicznego oznaczony jako 205b.

2. Obszar, w którym przetwarzane są dane osobowe należy zamykać na czas nieobecności w nim osób zatrudnionych przy przetwarzaniu danych, w sposób uniemożliwiający dostęp do niego osób trzecich.
3. Szczególnym obszarem, w którym przetwarzane są dane o wysokim priorytecie i przebywać w nim mogą jedynie osoby zatrudnione ze specjalnym upoważnieniem są pomieszczenia:
   a) wewnętrzny pokój w pokoju 306 w budynku przy pl. Słowackiego 23A oznaczony jako Serwerownia,

IV. Wykaz zbiorów danych osobowych

1. W skład zbioru wchodzą :
   - dokumentacja papierowa (korespondencja, wnioski, deklaracje itd.),
   - urządzenia i oprogramowanie komputerowe służące do przetwarzania informacji oraz procedury przetwarzania danych w tym systemie, w tym procedury awaryjne,
   - wydruki komputerowe

Wykaz zbiorów danych osobowych przetwarzanych w systemie informatycznym prowadzi Administrator Danych według wzoru określonego w załączniku nr 1.1 do niniejszego opracowania.

V. Struktury zbiorów danych osobowych oraz sposób przepływu danych

Opisy struktur zbiorów danych osobowych oraz powiązań miedzy zbiorami jak również sposób przepływu danych pomiędzy poszczególnymi systemami prowadzi Administrator Danych według wzoru określonego w załączniku nr 1.1 do niniejszego opracowania.

VI. Środki Techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

A. Środki ochrony fizycznej

1. Pomieszczenia w budynku przy pl. Słowackiego 23A, w których zlokalizowany jest obszar przetwarzania danych osobowych są zamykane po zakończeniu pracy. Budynek jest dozorowany w godzinach pracy, oraz wyposażony w system alarmowy.
2. Urządzania służące do przetwarzania danych osobowych znajdują się w pomieszczeniach zabezpieczonych.
3. Serwerownia stanowi dodatkowo zamykane pomieszczenie do której dostęp jest monitorowany i rejestrowany.
4. Serwery oraz komputery służące do przechowywania danych są udostępnione w ramach Infrastruktury UMW, środki ochrony fizycznej wydzielonej infrastruktury opisuje dokumentacja UMW.
5. Przebywanie osób nieuprawnionych w pomieszczeniach tworzących obszar przetwarzania danych osobowych dopuszczalne jest tylko w obecności osoby zatrudnionej przy przetwarzaniu danych lub w obecności Administratora Danych lub innej osoby upoważnionej.
6. Pomieszczenia, o których mowa powyżej powinny być zamykane na czas nieobecności w nich osób zatrudnionych przy przetwarzaniu danych, w sposób uniemożliwiający dostęp do nich osób trzecich.
7. W przypadku przebywania osób postronnych w pomieszczeniach, o których mowa wyżej, monitory stanowisk dostępu do danych osobowych powinny być ustawione w taki sposób aby uniemożliwiać im wgląd w dane.
8. Do przebywania w pomieszczeniach serwerowni i Serwerowni uprawnieni są Administrator Danych oraz pracownicy Działu IT.

9. Przebywanie w pomieszczeniach serwerowni osób nieuprawnionych (konserwator, osoba sprzątająca) dopuszczalne jest tylko w obecności jednej z osób upoważnionych, o których mowa w pkt. 8, a w przypadku ich nieobecności – w obecności osoby pisemnie upoważnionej przez Administratora Danych. Rejestr wejść jest prowadzony w Dziale IT.

B. Środki sprzętowe, informatyczne i telekomunikacyjne

1. System informatyczny oraz systemy przetwarzające dane zabezpieczone są przed nieupoważnionym dostępem osób trzecich systemem autentykacji i autoryzacji użytkowników.
2. Urządzenia wchodzące w skład systemu informatycznego podłączone są do odrębnego obwodu elektrycznego, systemy składowania danych zabezpieczone na wypadek zaniku napięcia albo awarii w sieci zasilającej urządzeniami podtrzymującymi napięcie (UPS).
3. Siec lokalna podłączona do Internetu za pomocą zestawu „Zapór Ogniowych" (Firewall) tworzących strefę zdemilitaryzowaną (*ang. demilitarized zone – DMZ*).
4. Na wszystkich serwerach oraz wszystkich stacjach roboczych zainstalowano oprogramowanie antywirusowe. Poczta elektroniczna wpływająca do IPAW skanowana jest programem antywirusowym zarówno przed wysłaniem jak i podczas odbierania wiadomości.
5. W ramach Infrastruktury UMW wdrożono system kopii zapasowych z wykorzystaniem nośników zewnętrznych.
6. W ramach Infrastruktury UMW nośniki zawierające kopie zapasowe przechowywane są w szafie pancernej, w innym pomieszczeniu niż serwerownia – miejsce składowania danych.
7. W ramach Infrastruktury UMW i IPAW kluczowe składniki systemu informatycznego tj. serwery, brzegowe urządzenia sieciowe, stacje robocze, nośniki danych oraz strategiczne urządzenie wspomagające (urządzenia UPS, streamery, NAS itp.) posiadają określony cykl życia (*ang. live time*). Po upłynięciu tego okresu winny być wymienione na nowe. Zestawienie sprzętu wraz z określonym cyklem życia stanowi załącznik nr 1.2 do Polityki Bezpieczeństwa.

C. Środki ochrony w ramach oprogramowania systemu

1. Dostęp fizyczny do baz danych osobowych zastrzeżony jest wyłącznie Administratora Systemu.
2. Konfiguracja systemu umożliwia użytkownikom końcowym dostęp do danych osobowych jedynie za pośrednictwem aplikacji.
3. System informatyczny pozwala zdefiniować odpowiednie prawa dostępu do zasobów informatycznych systemu.
4. W sieciowym systemie operacyjnym zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do systemu.

D. Środki ochrony w ramach narzędzi baz danych i innych narzędzi programowych

1. Aplikacje służące do przetwarzania danych osobowych muszą posiadać mechanizmy jednoznacznej autentykacji użytkownika i autoryzacji poziomu uprawnień za pomocą 1 z 2 metod:
    1. Autentykacja i autoryzacja za pomocą domeny MS Active Directory protokołem Kerberos, ADSI, LDAP ;
    2. Dodatkowego loginu i hasła dostępu na poziomie aplikacji przetwarzającej dane.
2. Dla każdego użytkownika systemu informatycznego jest ustalony odrębny identyfikator.
3. Zdefiniowano użytkowników i ich prawa dostępu do danych osobowych na poziomie systemu informatycznego (unikalny identyfikator i hasło w domenie MS Active Driectory).
4. Systemy informatyczne, które udostępniają dane osobowe muszą spełniać warunki opisane z art. 32 i 33 ustawy i § 7 rozporządzenia. Wymagane w przywołanych przepisach obowiązki sprowadzają się m.in. do zapewnienia i udostępniania – na żądanie osoby, której dane są przetwarzane – informacji o:
    1. dacie, od kiedy przetwarza się w zbiorze jej dane osobowe, oraz treści tych danych,
    2. źródle, z którego pochodzą dane jej dotyczące, chyba że administrator jest obowiązany do zachowania w tym zakresie tajemnicy państwowej, służbowej lub zawodowej,

3. sposobie i zakresie udostępniania jej danych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym dane te są udostępniane,
4. sposobie, w jaki zebrano dane.

E. Środki ochrony w ramach systemu informatycznego

1. Wszystkie komputery IPAW są skonfigurowane w sposób uniemożliwiający logowanie lokalne. Jedynym możliwym uruchomieniem systemu jest logowanie do domeny Active Directrory o nazwie um.local za pomocą ważnego identyfikatora i hasła dostępu.
2. Zastosowano automatyczny i zabezpieczony hasłem wygaszacz ekranu w przypadku dłuższej nieaktywności użytkownika.
3. Każdy użytkownik systemu może i powinien na czas przerwy w pracy w systemie informatycznym zablokować komputer za pomocą klawiatury, kombinacją klawiszy [windows] + L

F. Środki organizacyjne

1. Administratora Danych przyznaje uprawnienia w zakresie dostępu do danych osobowych.
2. Osoby upoważnione do przetwarzania danych osobowych są przed dopuszczeniem ich do pracy z tymi danymi szkolone w zakresie obowiązujących przepisów o ochronie danych osobowych, procedur przetwarzania danych oraz informowane o podstawowych zagrożeniach związanych z przetwarzaniem danych w systemie informatycznym.
3. Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych.
4. Osobę, która utraciła uprawnienia dostępu do danych osobowych, należy niezwłocznie wyrejestrować i unieważnić jej hasło oraz podjąć inne niezbędne czynności uniemożliwiające jej dalszy dostęp do danych.
5. Czynności wymienione w pkt. 4. wykonuje Administrator Systemu na polecenie Administratora Danych lub osoby upoważnionej.
6. Nie wolno wykorzystywać identyfikatora osoby, która utraciła uprawnienia do dostępu do danych. Identyfikator osoby winien być unikalny.
7. Wprowadzono Instrukcje Zarządzania Systemem Informatycznym.

8. Wprowadzono zasadę czystego biurka i czystego ekranu.
9. Zdefiniowano procedury postępowania w sytuacji naruszenia ochrony danych osobowych.
10. Wprowadzono obowiązek rejestracji wszystkich przypadków awarii systemu, działań konserwacyjnych w systemie oraz naprawy systemu.
11. Określono sposób postępowania z nośnikami informacji.
12. Podczas wymiany informacji z osobą której tożsamości nie można zweryfikować (np. rozmowa telefoniczna, nie podpisany podpisem elektronicznym e-mail) urzędnik może przekazać informacje dot. pracy IPAW nie zakazane prawem, a będące w jego posiadaniu lub objęte zakresem jego kompetencji lub uprawnień.

    Szczególnie powinny to być informacje zależne od potrzeb i oczekiwań klientów a dotyczące:

    - organizacji pracy IPAW,
    - obowiązującego prawa zewnętrznego i miejscowego w tym treści tego prawa oraz o zmianach tego prawa,
    - naborze kandydatów do służby urzędniczej,
    - obowiązujących procedur,
    - prowadzonych rejestrach, ewidencjach i archiwach oraz o sposobach i zasadach udostępniania danych w nich zawartych,
    - rodzajów usług publicznych,
    - treści aktów administracyjnych i ich rozstrzygnięć nie rozstrzygnięć dotyczących spraw indywidualnych bo nie wiemy z kim rozmawiamy ,
    - stanowiska w prawach publicznych zajęte przez organy władzy stanowiącej i wykonawczej,
    - kompetencji kierownictwa IPAW i urzędników,
    - inne informacje, będące powszechnie znanymi, które mogą przyczynić się do nawiązania kontaktu z klientem i są potrzebne lub oczekiwane przez klienta.
13. Podczas wymiany informacji z osobą której tożsamości nie można zweryfikować (np. rozmowa telefoniczna, nie podpisany podpisem elektronicznym e-mail) urzędnik nie może przekazać informacji dotyczących:

- danych osobowych stron postępowania administracyjnego,
- przebiegu indywidualnego postępowania administracyjnego,
- tajemnicy handlowej i skarbowej,
- informacji niejawnych,

14. Każdy dokument papierowy przeznaczony do wyrzucenia powinien być uprzednio zniszczony w sposób uniemożliwiający jego odczytanie (np. przy pomocy niszczarki do dokumentów).
15. W umowach zawieranych z kontrahentami zewnętrznymi należy umieszczać klauzulę o zachowaniu poufności. W uzasadnionych przypadkach w powyższych umowach należy określić sankcję za złamanie takiej klauzuli.

G. Odpowiedzialność osób upoważnionych do przetwarzania danych osobowych

Niezastosowanie się do prowadzonej przez administratora danych polityki bezpieczeństwa przetwarzania danych osobowych, której założenia określa niniejszy dokument, i naruszenie procedur ochrony danych przez pracowników upoważnionych do przetwarzania danych osobowych będzie potraktowane jako ciężkie naruszenie obowiązków pracowniczych.

Niezależnie od powyższego, osoby popełniające przestępstwo mogą być pociągnięte do odpowiedzialności karnej zwłaszcza na podstawie art. 51-52 ustawy oraz art. 266 Kodeksu karnego.

VII. Postanowienia końcowe.

Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest przed dopuszczeniem do przetwarzania danych zapoznać się:

1. z niniejszym dokumentem,
2. ustawą,
3. rozporządzeniem,
4. zarządzeniem nr ... Dyrektora Instytucji Pośredniczącej Aglomeracji Wałbrzyskiej w sprawie wprowadzenia dokumentacji danych osobowych w Instytucji Pośredniczącej

Aglomeracji Wałbrzyskiej, oraz złożyć stosowne oświadczenie, potwierdzające znajomość treści ww. dokumentów.

Załącznik nr 1.1 do Polityki Bezpieczeństwa. Wzór wykazu zbiorów danych osobowych.	*Strona* 1

TYTUŁ:	***Wzór wykazu zbiorów 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:			

Str 1 Dodano datę zgłoszenia dokumentu do GIODO

Wykaz zbiorów danych zgłoszonych do GIODO
stan na dzień _____

Nr zgłoszenia	Nr księgi	Nazwa zbioru	Data zgłoszenia	Data zatwierdzenia / aktualizacji

Wykaz pozostałych zbiorów danych osobowych przetwarzanych w systemie informatycznym.

Zbiór danych	Lokalizacja zbioru danych	System Merytoryczny

Załącznik nr 1.3 do Polityki Bezpieczeństwa. Tabela żywotności sprzętu informatycznego	*Strona* 1

TYTUŁ:	***Tabela żywotności sprzętu informatycznego***		
OPRACOWAŁ:	*Sebastian Węgrzynkiewicz* Imię i nazwisko	Podpis	Data
SPRAWDZIŁ:	Imię i nazwisko	Podpis	Data
ZATWIERDZIŁ:	Imię i nazwisko	Podpis	Data
OBOWIĄZUJE OD DNIA:			

Nazwa Sprzętu	**Optymalny okresy wymiany technologicznej**	**Maksymalny okres użytkowania**	**Uwagi**
Serwery	6 lat	9 lat	W zależności od obciążenia. Zaleca się by z wiekiem przesuwać na mniej krytyczne usługi
Dysk serwerowy (gwarancja producenta 5 lat)	5 lat	9 lat	MTBF wynosi średnio 100 000h
Dysk seryjny (gwarancja producenta 3 lata)	3 lata	6 lat	
Dysk SSD	40% zużycia	60 % zużycia	
NAS	5 lat	8 lat	
Przełącznik sieciowy	6 lat	10 lat	
Router	6 lat	10 lat	
UPS Serwera	5 lat	8 lat	Wymiana akumulatora co 2 lata
UPS	5 lat	8 lat	Wymiana akumulatora co 3 lata
Urządzenia taśmowe	4 lata	6 lat	
Taśmy (daily)	12 m-c	2 lata	
Taśmy (weekly)	24 m-c	3 lata	
Taśmy (monthly i pozostałe)	24 m-c	4 lata	
Stacje robocze	5 lata	7 lat	
Komputer przenośny	3 lata	5 lat	
Drukarka	4 lata	7 lat	Maksymalnie 3 wymiany bębna w przypadku urządzeń Kyoce