BURMISTRZ BISZTYNKA
11-230 BISZTYNEK
ul. Kościuszki 2

ZARZĄDZENIE NR 134/2018
BURMISTRZA BISZTYNKA
z dnia 8 listopada 2018r.

w sprawie wprowadzenia „Polityki Bezpieczeństwa Przetwarzania Danych Osobowych" w Urzędzie Miejskim w Bisztynku.

Na podstawie art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z z2018 r. poz. 994 z późn. zm), art. 24 ust. 1 i 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/WE, § 20 ust.1 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 (Dz.U. z 2017 r. poz.2247) zarządza się, co następuje:

§ 1.

Celem określenia reguł i zasad obowiązujących przy przetwarzaniu danych osobowych w Urzędzie Miejskim w Bisztynku, wprowadza się w brzmieniu określonym w załączniku do niniejszego zarządzenia „Politykę Bezpieczeństwa Przetwarzania Danych Osobowych".

§ 2.

Zobowiązuje się wszystkich pracowników Urzędu Miejskiego w Bisztynku do przestrzegania postanowień zawartych w „Polityce Bezpieczeństwa Przetwarzania Danych Osobowych".

§ 3.

Nadzór nad przestrzeganiem postanowień zawartych w Polityce Bezpieczeństwa Przetwarzania Danych Osobowych powierza się Inspektorowi Ochrony Danych oraz Administratorowi Systemu Informatycznego Urzędu Miejskiego w Bisztynku.

§ 4.

Traci moc Zarządzenie Nr 146/2012 Burmistrza Bisztynka z dnia 31 grudnia 2012 r. w sprawie ustalenia dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych w Urzędzie Miejskim w Bisztynku oraz wyznaczenia Administratora Bezpieczeństwa Informacji

§ 5.

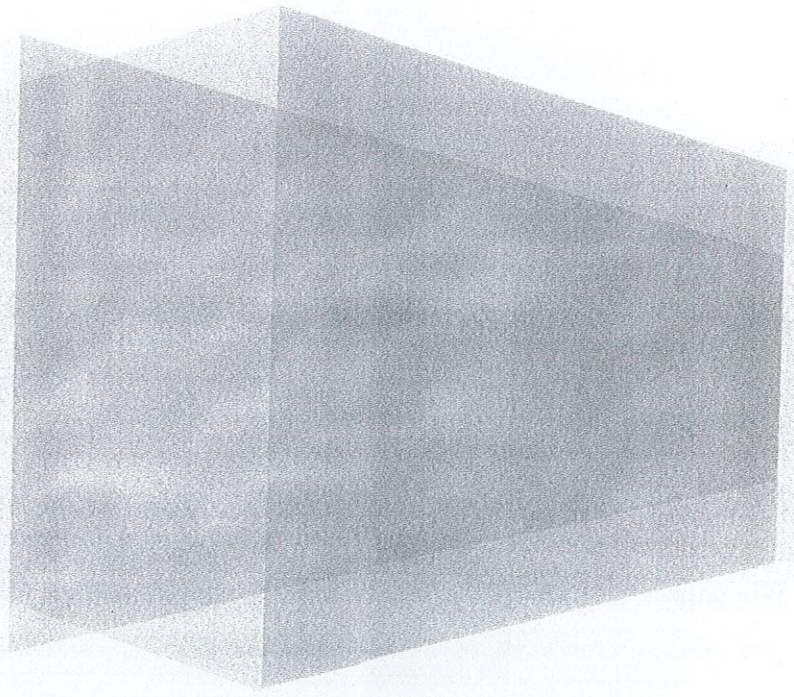
Zarządzenie wchodzi w życie z dniem podpisania z mocą obowiązującą od 25 maja 2018r.

BURMISTRZ
Marek Dominiak

POLITYKA BEZPIECZEŃSTWA
PRZETWARZANIA DANYCH OSOBOWYCH

W

URZĘDZIE MIEJSKIM W BISZTYNKU



2018

INSPEKTOR OCHRONY DANYCH

Monika Bark

Historia zmian

Data	Wersja	Opis zmiany	Autor
2012	1.0	Wdrożenie dokumentacji	Jarosław Wadowski
2018	1.1.	Wdrożenie zmian w dokumentacji	Grzegorz Szajerka

WERSJA 1.1		Pieczęć firmowa:	
Opracował zmiany :	**Data:**	**Zatwierdził:**	**Data:**
Grzegorz Szajerka	01.09.2018		

Spis treści

WPROWADZENIE

Realizując konstytucyjne prawo każdej osoby do ochrony życia prywatnego oraz postanowienia rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) w celu zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ww. rozporządzenia oraz zmianą, utratą, uszkodzeniem lub zniszczeniem, wprowadza się następujący zestaw procedur.

Niniejszy dokument jest zgodny z następującymi aktami prawnymi:

1. **„Ustawa o ochronie danych osobowych"** – rozumie się przez to ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych (tekst jedn. Dz. U. z 2018 r., poz. 1000),
2. **„Ogólnym rozporządzeniu o przetwarzaniu danych osobowych"** – rozumie się przez to Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.

Niniejszy dokument reguluje sprawy ochrony danych osobowych zawartych w systemie informatycznym eksploatowanym w lokalnej sieci komputerowej Microsoft Windows Network (MWN) oraz zbiorów danych zapisanych w postaci dokumentacji papierowej w .

Instrukcja dotyczy następujących niżej wymienionych baz danych:

1. PUMA - Ewidencja ludności, Podatki, Gospodarka nieruchomościami (Nieruchomości)
2. PB_USC - Urząd Stanu Cywilnego,
3. Źródło SRP – Dowody osobiste
4. Baza – Płatnik
5. Data – EWOPIS, EWMAPA

oraz zbiorów danych:

1. Przetwarzane w związku ze zmianą imion i nazwisk na podstawie ustawy o zmianie imion i nazwisk.
2. Przetwarzane w związku z wydawaniem decyzji o warunkach zabudowy i zagospodarowania terenu.
3. Przetwarzane w związku z działalnością gminnej komisji rozwiązywania problemów alkoholowych, na podstawie ustawy o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi.
4. Ewidencja ludności i dowodów osobistych.

5. Ewidencja podatników- rejestr podatników podatków i opłat lokalnych.
6. Zawarte w aktach stanu cywilnego.
7. Osób zobowiązanych do uiszczenia podatku od nieruchomości.
8. Ewidencja podatników- rejestr podatników podatku rolnego, leśnego.
9. Kandydatów na ławników przetwarzanych na podstawie ustawy Prawo o ustroju sądów powszechnych.
10. Przetwarzane w związku z nadawaniem numerów porządkowych nieruchomości –Prawo geodezyjne i kartograficzne.
11. Gromadzone ewidencji zbiorników bezodpływowych na odbieranie odpadów komunalnych
12. Gromadzone w ewidencji umów zawartych na odbieranie odpadów komunalnych od właścicieli nieruchomości na podstawie ustawy o utrzymaniu czystości i porządku w gminach
13. Najemców lokali mieszkalnych, przetwarzanych na podstawie o ochronie praw lokatorów i mieszkaniowym zasobie gminy.
14. Przetwarzane w związku z wydawaniem licencji na wykonywanie transportu drogowego.
15. Przetwarzane w związku z wydawaniem decyzji na zezwalających na usunięcie drzew i krzewów na podstawie ustawy o ochronie przyrody.
16. Wydawane w związku z wydawaniem decyzji na zajecie pasa drogowego na podstawie ustawy o drogach publicznych
17. Zawarte w rejestrze skarg i wniosków
18. Zgromadzone w ewidencji zabytków
19. Dotyczące nauczycieli, wychowawców i pracowników oświatowych przetwarzane na podstawie o systemie informacji oświatowej
20. Zawarte w arkuszach organizacyjnych szkół
21. Przetwarzane w związku z prowadzeniem nadzoru nad realizacja obowiązku szkolnego- ustawa o systemie oświaty
22. Dotyczące nauczycieli starających się o awans zawodowy- Karta Nauczyciela
23. Dotyczące zwrotu podatku akcyzowego
24. Zawarte w ewidencji wyrobów zawierających azbest
25. Ewidencji gruntów gminy
26. Ewidencja wojskowa i rejestracja przedpoborowych, świadczeń rzeczowych o osobistych, planowania obronnego i OC.

Do przetwarzania zbiorów danych zawierających dane osobowe stosuje się następujące programy:

- zbiór „Ewidencja ludności i dowodów osobistych" – przy użyciu systemu PUMA
- zbiór „Urząd Stanu Cywilnego" – przy użyciu programu PB_USC
- zbiór „Podatki" – przy użyciu systemu PUMA,

- zbiór „Kadry i wynagrodzenia" – przy użyciu programu PŁATNIK i PUMA
- zbiór „Świadczenia Rodzinne" – przy użyciu programu MS Office Word i Excel
- zbiór „Gospodarka nieruchomościami" – przy użyciu systemu PUMA

Osobami przetwarzającymi dane osobowe w zakresie:

- system „PUMA" – moduł „Ewidencja Ludności" oraz system „SWDO" są inspektor ds. Spraw Obywatelskich, Kierownik Urzędu Stanu Cywilnego
- programu „PB_USC" jest Kierownik Urzędu Stanu Cywilnego,
- system „PUMA" – moduły „Podatki", „Pojazdy", „Paliwa" i „Windykacja" jest inspektor: ds. podatków i opłat,
- system „PUMA" – moduł „Kadry" jest inspektor: ds. organizacyjnych i kadr,
- system „PUMA" – moduł „Płace" oraz program „PŁATNIK" jest inspektor: ds. płac,

Opis struktur zbiorów danych jest zawarty w Załączniku Nr 5 do niniejszego dokumentu.

Granice obszarów, w których przetwarzane są dane osobowe zostały opisane w Załączniku Nr 6.

Opisane reguły określają granice dopuszczalnego zachowania wszystkich użytkowników systemów informatycznych wspomagających pracę Urzędu. Dokument zwraca uwagę na konsekwencje, jakie mogą ponosić osoby przekraczające określone granice oraz procedury postępowania dla zapobiegania i minimalizowania skutków zagrożeń.

Odpowiednie zabezpieczenia, ochrona przetwarzanych danych oraz niezawodność funkcjonowania są podstawowymi wymogami stawianymi współczesnym systemom informatycznym. Dokument „Polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Bisztynku", zwany dalej „Polityką bezpieczeństwa", wskazujący sposób zabezpieczenia systemów informatycznych postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych w systemach informatycznych, przeznaczony jest dla osób zatrudnionych przy przetwarzaniu tych danych.

Potrzeba jego opracowania wynika z § 3 i 4 rozporządzenia 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. 2004r. Nr 100, póz. 1024), oraz zapisów Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.

1. „Polityka bezpieczeństwa" określa tryb postępowania w przypadku, gdy:

- stwierdzono naruszenie zabezpieczenia systemu informatycznego,

- stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci informatycznej mogą wskazywać na naruszenie zabezpieczeń tych danych.

2. „Polityka bezpieczeństwa" obowiązuje wszystkich pracowników Urzędu Miejskiego

3. Wykonywanie postanowień tego dokumentu ma zapewnić właściwą reakcję, ocenę i udokumentowanie przypadków naruszenia bezpieczeństwa systemów oraz zapewnić właściwy tryb działania w celu przywrócenia bezpieczeństwa danych przetwarzanych w systemie informatycznym Urzędu.

4. Administrator Danych, którym jest Burmistrz reprezentujący Urząd Miejski, powołuje Inspektora Ochrony Danych zwanego dalej „IOD" i Administratora Systemu Informatycznego (ASI).

5. „IOD" realizuje zadania w zakresie ochrony danych, a w szczególności:

- informowanie i doradzanie administratorowi lub podmiotowi przetwarzającemu, jak również ich pracownikom, w zakresie ich obowiązków wynikających z przepisów prawa o ochronie danych,
- monitorowanie zgodności organizacji z wszystkimi przepisami prawa dotyczącego ochrony danych, w tym audyty, działania podnoszące świadomość, a także szkolenia dla personelu zajmującego się przetwarzaniem danych,
- udzielanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania,
- pełnienie funkcji punktu kontaktowego dla osób fizycznych składających wnioski i żądania dotyczące przetwarzania ich danych osobowych i wykonywania ich praw,
- współpraca z organami ochrony danych i pełnienie funkcji punktu kontaktowego dla organów ochrony danych w kwestiach związanych z przetwarzaniem.

6. „Administrator Systemu Informatycznego" realizuje zadania w zakresie ochrony danych, a w szczególności:

- Operacyjne zarządzanie systemami informatycznymi w sposób zapewniający ochronę danych osobowych w nich przetwarzanych.
- Przestrzeganie opracowanych dla systemu procedur operacyjnych i bezpieczeństwa.
- Kontrola przepływu informacji pomiędzy systemem informatycznym a siecią publiczną oraz kontrola działań inicjowanych z sieci publicznej a systemem informatycznym.
- Zarządzanie stosowanymi w systemach informatycznym środkami uwierzytelnienia, w tym rejestrowanie i wyrejestrowywanie użytkowników oraz dokonywanie zmiany uprawnień na podstawie zaakceptowanych wniosków przez osobę do tego upoważnioną.
- Utrzymanie systemu w należytej sprawności technicznej.
- Regularne tworzenie kopii zapasowych zasobów danych osobowych oraz programów służących do ich przetwarzania oraz okresowe sprawdzanie poprawności wykonania kopii zapasowych.

- Wykonywanie lub nadzór nad wykonywaniem okresowych przeglądów i konserwacji, zgodnie z odrębnymi procedurami, sprzętu IT, systemów informatycznych, aplikacji oraz elektronicznych nośników informacji, na których zapisane są dane osobowe.

Rozdział 1

OPIS ZDARZEŃ NARUSZAJĄCYCH OCHRONĘ DANYCH OSOBOWYCH

1. Podział zagrożeń:

- zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu), ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu, ciągłość systemu zostaje zakłócona, nie dochodzi do naruszenia poufności danych,
- zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, administratora systemu, awarie sprzętowe, błędy oprogramowania), może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych,
- zagrożenia zamierzone, świadome i celowe - najpoważniejsze zagrożenia, naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy), zagrożenia te możemy podzielić na: nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu), nieuprawniony dostęp do systemu z jego wnętrza, nieuprawniony przekaz danych, pogorszenie jakości sprzętu i oprogramowania, bezpośrednie zagrożenie materialnych składników systemu.

2. Przypadki zakwalifikowane, jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe to głównie:

- sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.,
- niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych,
- awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, a w tym sam fakt pozostawienia serwisantów bez nadzoru,
- pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu,
- jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie,
- nastąpiło naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie,
- stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),

- nastąpiła niedopuszczalna manipulacja danymi osobowymi w systemie,
- ujawniono osobom nieupoważnionym dane osobowe lub objęte tajemnicą procedury ochrony przetwarzania albo inne strzeżone elementy systemu zabezpieczeń,
- praca w systemie lub jego sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony danych osobowych - np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.,
- ujawniono istnienie nieautoryzowanych kont dostępu do danych lub tzw. „bocznej furtki", itp.,
- podmieniono lub zniszczono nośniki z danymi osobowymi bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowano lub skopiowano dane osobowe,
- rażąco naruszono dyscyplinę pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, nie wykonanie w określonym terminie kopii
- bezpieczeństwa, prace na danych osobowych w celach prywatnych, itp.).

3. Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych osobowych (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. na papierze (wydrukach), kliszy, folii, zdjęciach, dyskietkach w formie niezabezpieczonej itp.

Rozdział 2

ZABEZPIECZENIE DANYCH OSOBOWYCH

§ 1.

Cele i zasady ogólne

1. Administratorem danych osobowych zawartych i przetwarzanych w systemach informatycznych Urzędu Miejskiego jest Burmistrz.

2. Administrator danych osobowych jest obowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych w systemach informatycznych Urzędu, a w szczególności:

   - zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym,
   - zapobiegać zabraniu danych przez osobę nieuprawnioną,
   - zapobiegać przetwarzaniu danych z naruszeniem ustawy oraz zmianie, utracie, uszkodzeniu lub zniszczeniu tych danych. Szczegółowe obowiązki Administratora Danych zawarte są w Załączniku Nr 1.

§ 2.

Cele ochrony i zasady ogólne

1. Celem wprowadzonych niniejszą Polityką zabezpieczeń i obostrzeń jest ochrona danych osobowych zawartych w eksploatowanym w sieci Microsoft Windows Network systemie.

   Określone niżej sposoby zabezpieczeń dotyczą:

   1.1 zabezpieczeń przed dostępem do danych osób nieupoważnionych na etapie eksploatacji systemu tj. wprowadzanie danych, aktualizacji lub usuwania danych, wyświetlania lub drukowania zestawień,

   1.2 ochrony danych zarchiwizowanych na nośnikach zewnętrznych, procedur niszczenia niepotrzebnych wydruków lub nośników danych.

   1.3 systemu zabezpieczeń przed dostępem osób niepowołanych do pomieszczeń, w których są eksploatowane urządzenia oraz sposobów dostępu do tych pomieszczeń pracowników, personelu pomocniczego Urzędu oraz serwisu zewnętrznego,

   1.4 monitorowania systemu zabezpieczeń,

1.5 zakresu obowiązków pracowników – w części dotyczącej bezpieczeństwa danych.

2. Strategia ochrony danych osobowych opiera się na następujących zasadach:

2.1 fizyczny dostęp do pomieszczeń, w których eksploatowane są systemy informatyczne blokują drzwi i systemy alarmowe.

2.2 podstawowym sposobem zabezpieczenia danych i dostępu do nich jest system definiowania użytkowników, grup użytkowników oraz haseł. Są to zabezpieczenia programowe wmontowane w eksploatowane systemy uniemożliwiające dostęp do systemu osobom nieupoważnionym.

2.3 dodatkowym systemem zabezpieczenia jest stosowanie kryptograficznej ochrony danych, jaką oferuje system operacyjny.

2.4 dodatkowe kopie danych zarchiwizowanych na nośnikach magnetycznych lub płytach CD są przechowywane w oddzielnym budynku – chronią w ten sposób dane na wypadek pożaru, klęski żywiołowej lub katastrofy. Prowadzona jest ścisła ewidencja tych nośników,

2.5 w pomieszczeniach, w których zainstalowany jest serwer i komputery zawierające bazy danych jest zainstalowany system alarmowy i przeciwpożarowy,

2.6 zagadnienia związane z ochroną danych i obowiązki stąd wynikające są ujęte w zakresach czynności pracowników stanowiące Załącznik Nr 3,

2.7 każdy pracownik Urzędu podpisze oświadczenie stanowiące Załącznik Nr 4,

2.8 za całość polityki bezpieczeństwa odpowiada Administrator Bezpieczeństwa Informacji.

§ 3.

Zabezpieczenia

Wprowadza się następujące zabezpieczenia danych w systemie informatycznym:

1. Na wszystkich stacja roboczych, na których przetwarzane są dane osobowe wprowadza się **wysoki** poziom zabezpieczeń.
2. Pomieszczenia, w których stoi serwer i komputery zawierające dane osobowe i kartoteki osobowe są zabezpieczone poprzez okratowane okna oraz system alarmowy i przeciwpożarowy. Wykaz tych pomieszczeń zawiera Załącznik Nr 6.

3. Ochronę przed awariami zasilania oraz zakłóceniami w sieci energetycznej serwera i stacji roboczych, na których przetwarzane są dane osobowe zapewniają zasilacze UPS.
4. Uruchomienie stacji roboczych, na których przetwarzane są dane osobowe wymaga podania hasła do systemu operacyjnego komputera,
5. Zalogowanie się do systemu wymaga podania nazwy użytkownika i hasła. Każdy użytkownik ma przypisane uprawnienia do wykonywania operacji. Nieudane próby logowania są rejestrowane, a po 3 nieudanych próbach logowania następuje czasowa blokada konta. Logowanie do systemu możliwe jest tylko w godzinach pracy Urzędu. Poza godzinami pracy Urzędu dopuszczalne jest logowanie do systemu jedynie za zgodą ADO wyrażoną na piśmie.
6. Oprogramowanie wykorzystywane do przetwarzania danych posiada własny system kont (zabezpieczonych hasłami) i uprawnień.
7. ADO oraz ASI w ramach uprawień nadanych przez Burmistrza ma uprawnienia do definiowania kont użytkowników i haseł.
8. Wykorzystany jest system szyfrowania danych (dostępny w systemie operacyjnym) uniemożliwiający odczyt danych osobom nieupoważnionym.
9. W celu ochrony przed dostępem do danych komputera z sieci publicznej wykorzystuje się system zapory ogniowej dostępnej w systemie operacyjnym.
10. Stosuje się aktywną ochronę antywirusową w czasie rzeczywistym na każdym komputerze, na którym przetwarzane są dane osobowe. Za aktualizację bazy wirusów odpowiada informatyk.
11. Wydruki zawierające dane osobowe powinny znajdować się w miejscu, które uniemożliwia dostęp osobom postronnym.
12. Kopie bezpieczeństwa na nośnikach magnetycznych wykonują okresowo pracownicy w ramach swoich obowiązków. Kopie bezpieczeństwa przechowywane są w kasie pancernej w pomieszczeniu Kasy Urzędu Miejskiego. Zapasowe kopie bezpieczeństwa są przechowywane w innym budynku również w szafie pancernej. Budynkiem tym jest budynek Urzędu Stanu Cywilnego w Bisztynku. Dostęp do nośników zawierających kopie danych mają tylko uprawnione osoby.
13. Kartoteki papierowe znajdują się w meblowych szafach, zamykanych na zamki meblowe w pokojach, w których przetwarzane dane osobowe.
14. Stosuje się następujące zabezpieczenia organizacyjne przed dostępem do danych osób niepowołanych:
    a) dostęp do danych mają wyłącznie pracownicy wyznaczeni przez Administratora Danych. Administrator Danych prowadzi ścisły rejestr tych pracowników obejmujący listę nazwisk użytkowników posiadających dostęp do danych, łącznie z ich identyfikatorami w systemie.
    b) w pokoju, do którego dostęp mają petenci monitory komputerowe ustawione są w ten sposób, by petenci nie widzieli zapisów na ekranie,
    c) w przypadku dłuższej bezczynności uruchamiane są tzw. wygaszacze ekranu, których dezaktywacja jest możliwa po podaniu prawidłowego hasła użytkownika.

d) częstotliwość tworzenia kopii bezpieczeństwa określa instrukcja archiwowania zasobów. Za wykonanie tych kopii odpowiedzialne są osoby przetwarzające dane osobowe..

e) tworzeniem kopii bezpieczeństwa na nośnikach optycznych (płyty CD-R/CD-RW) zajmuje się informatyk.

15. Dla zapewnienia poufności, integralności i rozliczalności przetwarzania danych ADO stosuje środki techniczne i organizacyjne właściwe dla wysokiego poziomu bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym, stosownie do wymogów określonych w Rozporządzeniu i RODO określone w punktach powyżej. Ocenę skutków dla ochrony danych osobowych (DPIA) przeprowadza każdorazowy właściciel procesu wskazany przez administratora danych .DPIA jest przeprowadzana przy każdorazowej istotnej zmianie procesu przetwarzania danych osobowych, np. zmiana dostawcy usług, zmiana sposobu przetwarzania danych, wymiana zasobów biorących udział w procesie. Analizę ryzyka dla zasobów biorących udział w procesach przeprowadza każdorazowy właściciel procesu wskazany przez administratora danych lub administrator danych samodzielnie lub przy pomocy IOD.

§ 4.

Monitorowanie zabezpieczeń

1. Do monitorowania systemu zabezpieczeń, stosownie do swojego zakresu czynności zobligowani są:
   a) Administrator Danych
   b) IOD w ramach rekomendacji dobrych praktyk związanych z ochroną danych osobowych
   c) Administrator Systemu Informatycznego
2. W ramach monitoringu należy przeprowadzać następujące działania:
   a) okresowe sprawdzanie kopii bezpieczeństwa pod względem przydatności do odtworzenia danych,
   b) kontrola ewidencji nośników magnetycznych i optycznych,
   c) weryfikacja poprawności obowiązku informacyjnego związanego z monitoringiem.
3. IOD sporządza roczne plany kontroli zatwierdzone przez Administratora Danych i zgodnie z nimi przeprowadza kontrole oraz dokonuje półrocznych ocen stanu bezpieczeństwa danych osobowych.
4. Na podstawie zgromadzonych materiałów, o których mowa w pkt. 3. IOD sporządza roczne sprawozdanie i przedstawia Administratorowi Danych.

§ 5.

Szkolenia

1. Szkolenie podstawowe dotyczące bezpieczeństwa danych obejmuje wszystkich pracowników Urzędu Miejskiego.
2. System szkoleń szczegółowych obejmuje pracowników zatrudnionych bezpośrednio przy przetwarzaniu danych, w tym danych osobowych.
3. Tematyka szkoleń obejmuje:
    a) Przepisy i instrukcje wewnętrzne dotyczące ochrony danych archiwizacji zasobów i przechowywania nośników, niszczenie wydruków i zapisów na nośnikach magnetycznych i optycznych,
    b) Zakresy obowiązków pracowników związanych bezpośrednio z bezpieczeństwem danych i ochroną systemów na poszczególnych stanowiskach.
    c) Zmiany wykładni w zakresie RODO i przepisów związanych z ochroną danych osobowych.

§ 6.

Archiwizowanie danych

1. Dane systemów kopiowane są w trybie tygodniowym. Kopie awaryjne danych zapisywanych w programach wykonywane są codziennie Odpowiedzialnym za wykonanie kopii danych i kopii awaryjnych jest pracownik obsługujący dany program przetwarzający dane.
2. Dodatkowo na koniec każdego miesiąca wykonywane są kopie bezpieczeństwa z całego programu przetwarzającego dane. Nośniki z kopiami bezpieczeństwa przekazywane są do pomieszczenia serwerowni w budynku Urzędu.
3. Kopie awaryjne są przechowywane w szafie pancernej w Urzędzie Miejskim. Osobą odpowiedzialną za wymianę kopii awaryjnych na aktualne jest ASI.
4. Dyskietki, na których zapisywane są kopie bezpieczeństwa są każdorazowo wymazywane i formatowane, w taki sposób, aby nie można było odtworzyć ich zawartości. Płyty CD, na których przechowuje się kopie awaryjne niszczy się trwale w sposób mechaniczny.
5. Okresową weryfikację kopii bezpieczeństwa pod kątem ich przydatności do odtworzenia danych przeprowadza informatyk.

§ 7.

Niszczenie wydruków i zapisów na nośnikach magnetycznych

1. Nośniki magnetyczne przekazywane na zewnątrz powinny być pozbawione zapisów zawierających dane osobowe. Niszczenie poprzednich zapisów powinno odbywać się poprzez wymazywanie informacji oraz formatowanie nośnika.
2. Poprawność przygotowania nośnika magnetycznego powinna być sprawdzona przez ASI.
3. Uszkodzone nośniki magnetyczne przed ich wyrzuceniem należy fizycznie zniszczyć (przeciąć, przełamać itp.).
4. Po wykorzystaniu wydruki zawierające dane osobowe powinny być niszczone przez urządzenia niszczące (niszczarki dokumentów)

Rozdział 3

POSTĘPOWANIE W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. Każdy pracownik Urzędu Miejskiego, który poweźmie wiadomość w zakresie naruszenia bezpieczeństwa danych przez osobę przetwarzającą dane osobowe bądź posiada informację o mogącą mieć wpływ na bezpieczeństwo danych osobowych jest zobowiązany fakt ten niezwłocznie zgłosić ADO i IOD.

2. W razie niemożliwości zawiadomienia IOD lub osoby przez niego upoważnionej, należy powiadomić bezpośredniego przełożonego.

3. Do czasu przybycia na miejsce naruszenia ochrony danych osobowych IOD lub upoważnionej przez niego osoby, należy:

   - niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców,
   - rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
   - zaniechać - o ile to możliwe - dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę,
   - podjąć inne działania przewidziane i określone w instrukcjach technicznych i technologicznych stosownie do objawów i komunikatów towarzyszących naruszeniu,

- podjąć stosowne działania, jeśli zaistniały przypadek jest określony w dokumentacji systemu operacyjnego, dokumentacji bazy danych lub aplikacji użytkowej,
- zastosować się do innych instrukcji i regulaminów, jeżeli odnoszą się one do zaistniałego przypadku,
- udokumentować wstępnie zaistniałe naruszenie,
- nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia IOD lub osoby upoważnionej.

4. Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych, IOD lub osoba go zastępująca:

   - zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy Urzędu,
   - może żądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,
   - rozważa wagę naruszenia z administratorem danych osobowych czy nie nastąpiło **naruszenie danych osobowych lub wysokie ryzyko naruszenia praw lub wolności osób fizycznych**

5. ADO przy pomocy IOD dokumentuje zaistniały przypadek naruszenia oraz sporządza raport wg wzoru stanowiącego Załącznik Nr 7, który powinien zawierać w szczególności:

   - wskazanie osoby powiadamiającej o naruszeniu oraz innych osób zaangażowanych lub odpytanych w związku z naruszeniem,
   - określenie czasu i miejsca naruszenia i powiadomienia,
   - określenie okoliczności towarzyszących i rodzaju naruszenia,
   - wyszczególnienie wziętych faktycznie pod uwagę przesłanek do wyboru metody postępowania i opis podjętego działania,
   - wstępną ocenę przyczyn wystąpienia naruszenia,
   - ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego oraz ewentualną konieczność zgłoszenia incydentu do Urzędu Ochrony Danych Osobowych.

6. Raport, o którym mowa w pkt. 5, IOD niezwłocznie przekazuje Administratorowi Danych (Burmistrzowi), a w przypadku jego nieobecności osobie uprawnionej. Raporty odnotowane są w rejestrze naruszeń wzór Załącznik Nr 11.

7. Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu IOD zasięga niezbędnych opinii i proponuje postępowanie naprawcze , a w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych. W przypadku gdy naruszenie , może

spowodować znaczy uszczerbek dobra osobistego , której naruszenie dotyczy IOD wraz z ADO podejmują działania określone w Załączniku Nr.12 i Załączniku Nr 13 .

8. Zaistniałe naruszenie może stać się przedmiotem szczegółowej, zespołowej analizy prowadzonej przez Kierownictwo urzędu, IOD.

9. Analiza powinna zawierać wszechstronną ocenę zaistniałego naruszenia, wskazanie odpowiedzialnych, wnioski, co do ewentualnych przedsięwzięć proceduralnych, organizacyjnych, kadrowych i technicznych, które powinny zapobiec podobnym naruszeniom w przyszłości.

Rozdział 4

POSTANOWIENIA KOŃCOWE

1. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także, gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, wszczyna się postępowanie dyscyplinarne.

2. ADO zobowiązany jest prowadzić ewidencję osób, które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych wg wzoru stanowiącego Załącznik Nr 8 do niniejszego dokumentu.

3. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane, jako ciężkie naruszenie obowiązków pracowniczych, w szczególności przez osobę, która wobec naruszenia zabezpieczenia systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie powiadomiła o tym ADO i IOD.

4. Orzeczona kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia ADO i IOD nie wyklucza odpowiedzialności karnej tej osoby oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

5. W sprawach nieuregulowanych niniejszym dokumentem mają zastosowanie przepisy Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (tekst jedn. Dz. U. z 2018 r., poz. 1000), oraz Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, rozporządzenia 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) oraz rozporządzenie Ministra Sprawiedliwości z dnia 28 kwietnia 2004 r. w sprawie sposobu technicznego przygotowania systemów i sieci do przekazywania informacji - do gromadzenia wykazów połączeń telefonicznych i innych przekazów informacji oraz sposobów zabezpieczenia danych informatycznych (Dz. U. Nr 100, poz. 1023).

6. Niniejsza „Polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych" w Urzędzie Miejskim w wchodzi w życie z dniem jej podpisania przez Burmistrza

Załącznik Nr 1 do „Polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Bisztynku

Obowiązki Administratora Danych

1. Administrator danych zobowiązany jest do zapewnienia, aby dane osobowe były:

   a) przetwarzane zgodnie z prawem,
   b) zbierane dla oznaczonych, zgodnych z prawem celów,
   c) merytorycznie poprawne i adekwatne w stosunku do celów.

2. Wyznacza osobę, zwaną dalej Administratorem Bezpieczeństwa Informacji, odpowiedzialnym za bezpieczeństwo danych osobowych w systemie informatycznym, w tym w szczególności za przeciwdziałanie dostępowi osób niepowołanych do systemu, w którym przetwarzane są dane osobowe, oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń.

3. Opracowuje instrukcję postępowania w sytuacji naruszenia ochrony danych osobowych, przeznaczoną dla osób zatrudnionych przy przetwarzaniu tych danych.

4. Określa budynki, pomieszczenia lub części pomieszczeń, tworzące obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego.

5. Opracowuje instrukcję, określającą sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji.

6. Prowadzi ewidencję osób uprawnionych do przetwarzania danych osobowych w poszczególnych systemach.

7. Organizuje szkolenia mające na celu zaznajomienie każdej osoby przetwarzającej dane osobowe z przepisami dotyczącymi ich ochrony.

8. Odpowiada za to by zakres czynności osoby zatrudnionej przy przetwarzania danych osobowych określał odpowiedzialność tej osoby za:

   a) ochronę danych przed niepowołanym dostępem,
   b) nieuzasadnioną modyfikację lub zniszczenie danych,
   c) nielegalne ujawnienie danych.

   w stopniu odpowiednim do zadań realizowanych w procesie przetwarzania danych osobowych.

9. Prowadzenie rejestru czynności przetwarzania danych osobowych w Urzędzie Miasta Bisztynek zgodnie z Załącznik Nr 9.

Załącznik Nr 2 do „Polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Bisztynku

Obowiązki IOD

a) informowanie i doradzanie administratorowi lub podmiotowi przetwarzającemu, jak również ich pracownikom, w zakresie ich obowiązków wynikających z przepisów prawa o ochronie danych,
b) monitorowanie zgodności organizacji z wszystkimi przepisami prawa dotyczącego ochrony danych, w tym audyty, działania podnoszące świadomość, a także szkolenia dla personelu zajmującego się przetwarzaniem danych,
c) udzielanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania,
d) pełnienie funkcji punktu kontaktowego dla osób fizycznych składających wnioski i żądania dotyczące przetwarzania ich danych osobowych i wykonywania ich praw,
e) współpraca z organami ochrony danych i pełnienie funkcji punktu kontaktowego dla organów ochrony danych w kwestiach związanych z przetwarzaniem,
f) Badanie ewentualnych naruszeń w systemie zabezpieczeń danych osobowych,
g) Wdrożenie szkoleń z zakresu przepisów dotyczących ochrony danych osobowych oraz środków technicznych i organizacyjnych przy przetwarzaniu danych w systemach informatycznych,
h) Sporządzanie planów kontroli zatwierdzanych przez Administratora Danych oraz przeprowadzanie zgodnie z nimi kontroli.

Załącznik Nr 3 do „Polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Bisztynku

Dodatkowy zakres obowiązków

dla pracowników Urzędu Miejskiego w Bisztynku

1. Pracownik zobowiązany jest dbać o bezpieczeństwo powierzonych mu do przetwarzania, archiwizowania lub przechowywania danych zgodnie z obowiązującą w Urzędzie Polityką Bezpieczeństwa, regulaminami i instrukcjami wewnętrznymi, w tym m. in.:

    a) Chronić dane przed dostępem osób nieupoważnionych,
    b) Chronić dane przed przypadkowym lub nieumyślnym zniszczeniem, utratą lub modyfikacją,
    c) Chronić nośniki magnetyczne i optyczne oraz wydruki komputerowe przed dostępem osób nieupoważnionych oraz przed przypadkowym zniszczeniem,
    d) Utrzymywać w tajemnicy powierzone identyfikatory, hasła, częstotliwość ich zmiany oraz szczegóły technologiczne systemów także po ustaniu zatrudnienia w Urzędzie.
    e) Archiwizować dane zgodnie z instrukcją technologiczną,
    f) Prowadzić niezbędną, przewidzianą instrukcją technologiczną dokumentację pracy z systemem, archiwizowania danych itp.

2. Zabrania się pod rygorem odpowiedzialności służbowej i karnej:

    a) Ujawniać dane – w tym dane osobowe zawarte w obsługiwanych systemach,
    b) Kopiować bazy danych lub ich części poza przewidzianymi instrukcją technologiczną kopiami bezpieczeństwa,
    c) Zabrania się przetwarzania danych w sposób inny niż opisany instrukcją technologiczną.

Załącznik Nr 4 do „Polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Bisztynku

..... Bisztynek, dn. .....

(imię i nazwisko pracownika)

.....

(adres)

.....

OŚWIADCZENIE

(tekst oświadczenia podpisanego przez pracowników Urzędu Miejskiego oraz służb pomocniczych – sprzątaczka)

1. Stwierdzam własnoręcznym podpisem, że znana mi jest treść przepisów:

   a) o ochronie i postępowaniu z wiadomościami, stanowiącymi tajemnicę służbową,
   b) o zasadach ochrony oraz środkach i zabezpieczeniach danych osobowych (Dz. U. Nr 133 poz. 833) oraz rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 28 kwietnia 2004 roku (Dz. U. Nr 100 poz. 1024 z 2004 r.) oraz o odpowiedzialności karnej za naruszenie ochrony danych osobowych.

2 Jednocześnie zobowiązuję się nie ujawniać wiadomości, z którymi zapoznałem/zapoznałam się z racji wykonywanej pracy w Urzędzie Miejskim, a w szczególności nie będę:

   a) ujawniać danych zawartych w eksploatowanych w Urzędzie systemach informatycznych, zwłaszcza danych osobowych znajdujących się w tym systemach,
   b) ujawniać szczegółów technologicznych używanych w Urzędzie systemów oraz oprogramowania,
   c) udostępniać osobom nieupoważnionym nośniki magnetyczne i optyczne oraz wydruki komputerowe,
   d) kopiować lub przetwarzać danych w sposób inny niż dopuszczony obowiązującą instrukcją technologiczną.

....

(podpis pracownika) (podpis przełożonego)

Załącznik Nr 5 do „Polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Bisztynku

Opis struktur zbiorów danych

Zbiór danych „Ewidencja Ludności" (baza PUMA) zawiera następujące pola:

Dane osobowe
- nazwiska i imiona
- nazwisko rodowe i z poprzedniego małżeństwa
- imiona i nazwiska rodziców
- nazwiska rodowe rodziców
- płeć
- wykształcenie
- data urodzenia
- miejsce urodzenia
- nr aktu urodzenia, data, organ administracyjny i kod terytorialny
Numer ewidencyjny PESEL
Adres pobytu stałego oraz data zameldowania (państwo, województwo, powiat, gmina, kod terytorialny)
Archiwalne adresy pobytu stałego oraz data zameldowania i wymeldowania (państwo, województwo, powiat, gmina, kod terytorialny)
Adres czasowy oraz okres pobytu czasowego (państwo, województwo, powiat, gmina, kod terytorialny)
Archiwalne adresy czasowe oraz okresy pobytów czasowych (państwo, województwo, powiat, gmina, kod terytorialny)
Dokument tożsamości
- rodzaj dokumentu,
- seria i numer dokumentu
- wystawca dokumentu i kod terytorialny
- rysopis: wzrost, kolor oczu znaki szczególne
- data wydania dokumentu
- data ważności dokumentu
- data zmiany
Archiwalne dokumenty tożsamości (rodzaj, seria i nr, wystawca, kod terytorialny, rysopis, data wydania, data ważności dokumentu, data zmiany)
Stan cywilny:
- forma ustania
- data zmiany
- nr aktu małżeństwa
- PESEL współmałżonka
- imiona współmałżonka
- nazwisko rodowe współmałżonka
- organ administracyjny i kod terytorialny
Stan cywilny archiwalny (forma ustania, data zmiany, nr aktu małżeństwa, PESEL współmałżonka, imiona współmałżonka, nazwisko rodowe współmałżonka, organ administracyjny i kod terytorialny)
Obowiązek wojskowy
- czy podlega obowiązkowi
- rodzaj dokumentu i nr wojskowego dokumentu tożsamości

- klasyfikacja stopni
- stopień wojskowy
Data zgonu, nr aktu zgonu, kod terytorialny zgonu, wystawca
Obywatelstwo (data zmiany, podstawa prawna)

Zbiór danych „Dowody Osobiste" (baza SWDO) zawiera następujące pola:

• imiona i nazwisko (pierwszy człon, drugi człon), nazwisko rodowe
• imiona i nazwiska rodowe rodziców,
• data urodzenia
• miejsce urodzenia,
• numer PESEL
• kolor oczu
• wzrost w cm
• adres zameldowania (kod terytorialny, miejscowość, ulica, nr lokalu, nr domu
• rodzaj zameldowania
• kod pocztowy
• posiadany dotychczasowy dokument tożsamości(seria, nr, nazwa, siedziba wystawcy)
• przyczyny wystawienia dowodu
• data i przyczyna utraty
• podpis osoby
• fotografia
• podpis i pieczęć gminy
• nr formularza
• siedziba wystawy DO
• termin ważności dokumentu

Zbiór danych „Urząd Stanu Cywilnego" (baza USC) zawiera następujące pola:

• nazwisko i nazwisko rodowe
• imię (imiona)
• nazwisko z poprzedniego małżeństwa
• imiona rodziców, nazwisko i nazwisko rodowe rodziców
• imię i nazwisko, nazwisko rodowe współmałżonka
• data urodzenia
• miejsce urodzenia
• kraj urodzenia
• PESEL
• płeć
• obywatelstwo
• stan cywilny
• miejsce zamieszkania (siedziba zakładu)
• adres zameldowania na pobyt stały
• rodzaj dokumentu
• wystawca dokumentu, miejsce wydania
• seria i numer dowodu osobistego
• data wydania dowodu osobistego
• nr aktu urodzenia, data, nazwa USC
• nr aktu małżeństwa, data, nazwa USC

• nr aktu zgonu, data, nazwa USC
• data zgonu
• godzina zgonu
• miejsce, data, godzina znalezienia zwłok
• imię i nazwisko (siedziba zakładu)
• data zawarcia małżeństwa
• nazwiska noszone po zawarciu małżeństwa
• przyczyna ustania małżeństwa
• świadkowie: nazwisko, imię(imiona)
• wyznanie
• wykształcenie
• telefon kontaktowy
• źródło utrzymania osoby, źródło utrzymania osoby utrzymującej
• separacja: data, sygnatura akt z dnia, siedziba sądu
• rozwód: data, sygnatura akt z dnia, siedziba sądu
• unieważnienie małżeństwa: data, sygnatura akt z dnia, siedziba sądu
• data uprawomocnienia: wyroku, orzeczenia, postanowienia
• rodzaj sądu
• liczba dzieci urodzonych przez matkę (żywo i martwo urodzone)
• żywotność dziecka (urodzone martwe, urodzone żywe)
• data poprzedniego porodu
• waga dziecka w gramach
• długość dziecka w centymetrach
• rodzaj porodu
• czas zgonu (w czasie porodu, przed porodem, nie ustalono)
• czas ciąży w tygodniach
• powód wpisania aktu
• rodzaj karty

Zbiór danych „Kadry i płace" (baza PUMA) zawiera następujące pola:

Dane osobowe
- imię i nazwisko
- data urodzenia
- płeć
- nr NIP
- numer PESEL
- stan cywilny,
- numer i seria dowodu osobistego,
- numer paszportu
- obywatelstwo,
- przynależność do oddziału NFZ
- uprawnienia emerytalno-rentowe
- orzeczenia o niepełnosprawności
- nazwa banku i numer konta,
Dane adresowe
- adres zamieszkania(miejscowość, ulica, nr domu, nr lokalu, kod)
Wysokość otrzymywanych wynagrodzeń
Historia zatrudnienia

Zbiór danych „Płatnik" (baza PLATNIK) zawiera następujące pola:

Dane osobowe
- imię i nazwisko
- data urodzenia
- płeć
- numer PESEL
- obywatelstwo
- przynależność do oddziału NFZ
- uprawnienia emerytalno-rentowe
- orzeczenia o niepełnosprawności
Dane adresowe
- adres zamieszkania(miejscowość, ulica, nr domu, nr lokalu, kod)
Wysokość podstaw oskładkowania

Zbiór danych „ Podatki" zawiera następujące pola:

Dane osobowe
▪ imiona i nazwiska,
▪ imiona i nazwiska rodowe rodziców,
▪ nazwisko rodowe,
▪ data urodzenia
▪ miejsce urodzenia,
▪ numer PESEL
▪ płeć
▪ stan cywilny
▪ posiadany dotychczasowy dokument tożsamości(seria, nr, nazwa, siedziba wystawcy)
Dane adresowe
- adres zamieszkania(miejscowość, ulica, nr domu, nr lokalu, kod pocztowy)
Numer NIP
Nr kartoteki
Numery działek
Nazwy obrębów
Adres nieruchomości (miejscowość, ulica, Nr domu, nr lokalu, kod pocztowy)
Powierzchnia gruntów rolnych w klasach
Powierzchnia lasów w klasach
Powierzchnia i rodzaje nieruchomości
Ulgi podatkowe
Wymiar podatku

Zbiór danych „ Pojazdy" (baza PUMA) zawiera następujące pola:

Dane osobowe
▪ imiona i nazwiska,
▪ imiona i nazwiska rodowe rodziców,
▪ nazwisko rodowe,
▪ data urodzenia
▪ miejsce urodzenia,
▪ numer PESEL
▪ płeć
▪ stan cywilny
▪ posiadany dotychczasowy dokument tożsamości(seria, nr, nazwa, siedziba wystawcy)
Dane adresowe

- adres zamieszkania(miejscowość, ulica, nr domu, nr lokalu, kod pocztowy)
Numer Regon
Numer rejestracyjny pojazdu
Rodzaj pojazdu
Data nabycia pojazdu
Data zarejestrowania pojazdu
Data zbycia pojazdu
Data wyrejestrowania pojazdu
Informacje o złożonych deklaracjach na podatek

Zbiór danych „ Paliwa" (baza PUMA) zawiera następujące pola:

Dane osobowe
▪ imiona i nazwiska,
▪ imiona i nazwiska rodowe rodziców,
▪ nazwisko rodowe,
▪ data urodzenia
▪ miejsce urodzenia,
▪ numer PESEL
▪ płeć
▪ stan cywilny
▪ posiadany dotychczasowy dokument tożsamości(seria, nr, nazwa, siedziba wystawcy)
Dane adresowe
- adres zamieszkania(miejscowość, ulica, nr domu, nr lokalu, kod pocztowy)
Numer Regon
Powierzchnia gruntów
Data złożenia wniosku
Data i nr decyzji
Ilość zakupionego oleju napędowego
Wartość przyznanego zwrotu podatku akcyzowego

Zbiór danych „ Windykacja" (baza PUMA) zawiera następujące pola:

Dane osobowe
▪ imiona i nazwiska,
▪ imiona i nazwiska rodowe rodziców,
▪ nazwisko rodowe,
▪ data urodzenia
▪ miejsce urodzenia,
▪ numer PESEL
▪ płeć
▪ stan cywilny
▪ posiadany dotychczasowy dokument tożsamości(seria, nr, nazwa, siedziba wystawcy)
Dane adresowe
- adres zamieszkania(miejscowość, ulica, nr domu, nr lokalu, kod pocztowy)
Numer Regon
Wielkość i rodzaj należności oraz terminy wpłat
Dokonane wpłaty
Informacje o wysłanych upomnieniach
Informacje o wystawionych tytułach wykonawczych
Nr kartoteki

Zbiór danych „Kadry" (baza PUMA) zawiera następujące pola:

Zakładka Kartoteki (nazwisko, imiona, PESEL, NIP)
Zakładka Umowa (typ umowy, data zawarcia od-do, typ pracownika, grupa pracownicza, stanowisko, miejsce pracy, wymiar czasu pracy, nominalny czas pracy, etatowy czas pracy, koszt uzyskania przychodu, jednostka organizacyjna, składniki płacowe, zakończenie umowy)
Zakładka ZUS (data rejestracji, podmiot podstawowy, prawo do emerytury, stopień niepełnoprawności, data rejestracji w NFZ, kod oddziału NFZ, kod zawodu, data wyrejestrowania)
Zakładka NIP (Państwo. Obywatelstwo, miejscowość, kod pocztowy, ulica, województwo, powiat, gmina, data urodzenia, nazwisko rodowe, dokument tożsamości, nr i seria DO, Urząd Skarbowy, poczta)
Zakładka Historia a) historia wykształcenia (data ukończenia, liczba lat) b) historia zatrudnienia(od-do, nazwa zakładu, typ umowy, staż)
Zakładka Kalendarz Pracownika (rok, miesiąc, kalendarz roczny, kalendarz miesięczny)
Zakładka Nieobecności (rodzaj urlopu, rodzaj zwolnienia data od-do, podsumowanie)
Zakładka Funkcje publiczne (rodzaj funkcji, data od-do, dieta)
Zakładka Potrącenia (rodzaj potrącenia, data od-do, kwota)
Zakładka Pożyczki (data, kwota, ilość rat, saldo)
Zakładka Badania (data od-do, rodzaj, orzeczenie, termin)
Zakładka Nagrody i Kary (nazwa, data, kwota)
Zakładka Szkolenia (nazwa, data)
Zakładka Języki obce (nazwa, poziom)
Zakładka Organizacje (data wstąpienia, stanowisko)
Zakładka Rodzina (imię, nazwisko, gospodarstwo, rodzinne, zdrowotne)
Zakładka Wojsko (nr książeczki, stopień wojskowy)
Zakładka Emerytury/renty (nr, kod, rodzaj, data odejścia)
Zakładka Limit samochodowy (data od-do, marka, nr rejestracyjny, poj. Silnika, przyznany limit)

Załącznik Nr 6 do „Polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Bisztynku

Granice obszarów (budynków i pomieszczeń), w których przetwarzane są dane osobowe

§1. Pomieszczeniami tworzącymi obszar, w którym znajdują się przetwarzane dane osobowe są pomieszczenia, w których znajdują się zbiory danych w formie kartotek, rejestrów i innych oraz stacjonarny sprzęt komputerowy, w którym znajdują się dane osobowe.

§2. W budynku Urzędu Miejskiego obszarem, w którym przetwarzane są dane osobowe w formie kartotek, rejestrów i stacjonarnego sprzętu komputerowego jest pomieszczenie:

Legenda (1): (D) drzwi zamykane na klucz, (S): zamknięte niemetalowe / metalowe szafy (klucze), (N) niszczarki dokumentów, (O) zabezpieczenie okien (kraty/folia antywłamaniowa/rolety), (A) system alarmowy przeciwwłamaniowy, (M) monitoring kamer, (SO) służba ochrony, (SF) sejf lub kasa pancerna, (P) system przeciwpożarowy /gaśnice

Lp.	Nazwa zbioru danych	Program służący do przetwarzania baz danych	Lokalizacja	Zabezpieczenia fizyczne (1)
1.	Dane osobowe (wszystkie)	System PUMA	Bisztynek, ul. Kościuszki 2 pokój nr 18 (poddasze)	S, D, A, P, SF
2.	Dane osobowe Pracowników	System PUMA – moduł Kadry	Bisztynek, ul. Kościuszki 2 pokój nr 9 (I piętro)	S, A, SF
3.	Dane osobowe Podatników	System PUMA – moduł Podatki, Windykacja, Pojazdy, Paliwa	Bisztynek, ul. Kościuszki 2 pokój nr 5 (parter)	D, S, N, O, A
4.	Dane osobowe Pracowników	System PUMA – moduł Kadry, Płace Program PŁATNIK	Bisztynek, ul. Kościuszki 2 pokój nr 6 (parter)	D, S, O, A, SF
5.	Dane osobowe – Wnioski o wydanie decyzji środowiskowych	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 2 (parter)	D, S, O, A
6.	Dane osobowe - Zaświadczenia	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 2 (parter)	D, S, O, A
7.	Nawiązywanie kontaktów – udzielanie i wymiana informacji	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 2 (parter)	D, S, O, A
8.	Naruszenie stanu wody na gruncie – melioracje	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 2 (parter)	D, S, O, A

9.	Zezwolenia na prowadzenie, odzyskiwania, unieszkodliwiania i transportu odpadów	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 2 (parter)	D, S, O, A
10.	Rejestr działalności regulowanej w zakresie odbioru i transportu odpadów	Wydruk papierowy Wersja elektroniczna	Bisztynek, ul. Kościuszki 2 pokój nr 2 (parter)	D, S, O, A
11.	Decyzje – wycinka drzew	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 2 (parter)	D, S, O, A
12.	Decyzje – zatwierdzenie podziału nieruchomości	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 2 (parter)	D, S, O, A
13.	Zlecenia, umowy – Fundusz Sołecki	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 2 (parter)	D, S, O, A
14.	Organy uchwałodawcze – sołtysi	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 2 (parter)	D, S, O, A
15.	Gospodarka Łowiecka	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 2 (parter)	D, S, O, A
16.	Sprzedaż nieruchomości	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 2 (parter)	D, S, O, A
17.	Dzierżawa - grunty	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 2 (parter)	D, S, O, A
18.	Wynajem lokali – mieszkania socjalne i lokale użytkowe	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 2 (parter)	D, S, O, A
19.	Nadanie numeru nieruchomości	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 2 (parter)	D, S, O, A
20.	Akta osiedleńcze	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 2 (parter)	D, S, O, A
21.	Decyzje o nadaniu działki na własność	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 2 (parter)	D, S, O, A
22.	Aktualizacja opłat rocznych z tyt. Użyt. Wiecz.	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 2 (parter)	D, S, O, A
23.	Listy osób do kwalifikacji wojskowej	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 4 (parter)	D, S, O, A, P
24.	Listy osób pełniących świadczenia osobowe, rzeczowe	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 4 (parter)	D, S, O, A, P
25.	Wykaz członków Formacji OC	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 4 (parter)	D, S, O, A, P
26.	Skład osobowy Zarządu M-G ZOSP	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 4 (parter)	D, S, O, A, P

27.	Kartoteka podatkowa	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 5 (parter)	D, S, N, O, A,
28.	Wnioski podatników	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 5 (parter)	D, S, N, O, A,
29.	Zaświadczenia	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 5 (parter)	D, S, N, O, A,
30.	Deklaracje podatkowe	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 5 (parter)	D, S, N, O, A,
31.	Dowody wpłat podatkowych	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 5 (parter)	D, S, N, O, A,
32.	Dane osobowe byłych pracowników oświaty	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 6 (parter)	D, S, O, A, SF
33.	Dane osobowe – karty wynagrodzeń pracowników	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 6 (parter)	D, S, O, A, SF
34.	Dane osobowe – PITy pracowników	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 6 (parter)	D, S, O, A, SF
35.	Dane osobowe – zgłoszenie do ubezpieczeń	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 6 (parter)	D, S, O, A, SF
36.	Dane osobowe – raporty imienne RCA, RSA	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 6 (parter)	D, S, O, A, SF
37.	Dane osobowe – oświadczenia majątkowe Radnych Rady Miejskiej	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 7 (parter)	D, S, O, A
38.	Wnioski o wpis do CEIDG	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 8 (I piętro)	D, S, A
39.	Porozumienia na dowóz dzieci do szkół	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 8 (I piętro)	D, S, A
40.	Zaświadczenia z planu zagospodarowania przestrzennego	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 8 (I piętro)	D, S, A
41.	Decyzje o warunkach zabudowy	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 8 (I piętro)	D, S, A
42.	Decyzje dot. dróg publicznych	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 8 (I piętro)	D, S, A
43.	Dane osobowe – skazani wyrokiem Sądu na prace na cel społeczny	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 8 (I piętro)	D, S, A
44.	Dane osobowe – pracowników prac społeczno-użytecznych	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 8 (I piętro)	D, S, A

45.	Dane osobowe – podania, wnioski	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 8 (I piętro)	D, S, A
46.	Dane osobowe – decyzje zatwierdzające podział nieruchomości	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 8 (I piętro)	D, S, A
47.	Dane osobowe – sprzedaż nieruchomości	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 8 (I piętro)	D, S, A
48.	Zaświadczenia	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 8 (I piętro)	D, S, A
49.	Dane osobowe – dzierżawy gruntu	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 8 (I piętro)	D, S, A
50.	Wynajem lokali socjalnych i użytkowych	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 8 (I piętro)	D, S, A
51.	Nadanie nr porządkowego nieruchomości	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 8 (I piętro)	D, S, A
52.	Aktualizacja opłaty z tyt. Użyt. Wiecz.	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 8 (I piętro)	D, S, A
53.	Prace zlecone ze składką na ZUS	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 9 (I piętro)	D, S, A
54.	Umowy zbiorowe	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 9 (I piętro)	D, S, A
55.	Praktyki – dane osobowe	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 9 (I piętro)	D, S, A
56.	Badania lekarskie w zakresie medycyny pracy	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 9 (I piętro)	D, S, A
57.	Zaświadczenia o zatrudnieniu	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 9 (I piętro)	D, SF, A
58.	Staże zawodowe	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 9 (I piętro)	D, S, A
59.	Zapotrzebowanie i nabór kandydatów do pracy	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 9 (I piętro)	D, S, A
60.	Konkursy na stanowiska	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 9 (I piętro)	D, SF, A
61.	Obsługa zatrudnienia	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 9 (I piętro)	D, SF, A
62.	Czas pracy	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 9 (I piętro)	D, S, A

63.	Urlopy osób zatrudnionych	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 9 (I piętro)	D, S, A
64.	Szkolenia i doskonalenie osób zatrudnionych	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 9 (I piętro)	D, S, A
65.	Akta osobowe pracowników, kierowników jednostek organizacyjnych	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 9 (I piętro)	D, SF, A
66.	Upoważnienia	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 10 (I piętro)	D, S, A
67.	Rejestr skarg i wniosków	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 10 (I piętro)	D, S, A
68.	Dane osobowe – umowy	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 10 (I piętro)	D, S, A
69.	Dane osobowe – poświadczenia	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 10 (I piętro)	D, S, A
70.	Oświadczenia ostatniej woli spadkowej	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 12 (I piętro)	D, SF, A
71.	Dane osobowe – stypendia	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 15 (I piętro)	D, S
72.	Dane osobowe – pracodawcy młodocianych	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 15 (I piętro)	D, S
73.	Listy płac pracowników, kierowników jednostek, nauczycieli	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 17 (poddasze)	D, S, A, P
74.	Umowy (np. o dzieło, o pożyczki z ZFŚS)	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 17 (poddasze)	D, S, A, P
75.	Wyciągi bankowe	Wydruk papierowy	Bisztynek, ul. Kościuszki 2 pokój nr 17 (poddasze)	D, S, A, P

§3. W budynku będącym własnością Gminy przy ul. Kościelnej 39 w Bisztynku, w którym przetwarzane są dane osobowe w formie kartotek, rejestrów i stacjonarnego sprzętu komputerowego są następujące pomieszczenia:

Lp.	Nazwa zbioru danych	Program służący do przetwarzania baz danych	Lokalizacja	Zabezpieczenia fizyczne (1)
1.	Dane osobowe	System PUMA – moduły Ewidencja Ludności, Wyborcy	Bisztynek, ul. Kościelna 39 pokój nr 1 (I piętro)	S, D, A, O, P, SF
2.	Dane osobowe	System PB_USC	Bisztynek, ul. Kościelna 39 pokój nr 1 (I piętro)	S, D, A, O, P, SF

3.	Dane osobowe	System SWDO	Bisztynek, ul. Kościelna 39 pokój nr 1 (I piętro)	S, D, A, O, P, SF
4.	Akta zbiorowe urodzeń, małżeństw, zgonów	wydruk papierowy	Bisztynek, ul. Kościelna 39 archiwum (I piętro)	D, S, O, A, P
5.	Księgi urodzeń, małżeństw, zgonów	księgi (wersja papierowa)	Bisztynek, ul. Kościelna 39 archiwum (I piętro)	D, S, O, A, P
6.	Skorowidze do ksiąg s.c.	wersja papierowa	Bisztynek, ul. Kościelna 39 archiwum (I piętro)	D, S, O, A, P
7.	Karty Osobowe Mieszkańców, odsyłacze	wersja papierowa	Bisztynek, ul. Kościelna 39 archiwum (I piętro)	D, S, O, A, P
8.	Koperty dowodowe	wersja papierowa	Bisztynek, ul. Kościelna 39 archiwum (I piętro)	D, S, O, A, P
9.	Koperty dowodowe	wersja papierowa	Bisztynek, ul. Kościelna 39 pokój nr 1 (I piętro)	D, S, A, P, N
10.	Decyzje, wnioski, postanowienia, zaświadczenia, zawiadomienia,	wersja papierowa	Bisztynek, ul. Kościelna 39 pokój nr 1 (I piętro)	D, S, A, P, N
11.	Księgi meldunkowe	księgi (wersja papierowa)	Bisztynek, ul. Kościelna 39 pokój nr 1 (I piętro)	D, S, A, P, N

Załącznik Nr 6A do „Polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Bisztynku

Sposób przepływu danych pomiędzy poszczególnymi systemami.

System (moduły)/ Program A	System(moduły)/ Program B	Kierunek przepływu danych osobowych (pomiędzy programami lub modułami)	Sposób przesyłania danych osobowych
System PUMA Moduły Kadry i Płace	Program Płatnik	Jednokierunkowo z systemu PUMA do programu Płatnik	Półautomatycznie – eksport pliku z systemu PUMA (Kadry, Płace) na serwer, z którego następnie pobierany jest przez program Płatnik
PUMA - moduł Kadry	PUMA - moduł Płace PUMA - moduł Kontrahent	Dwukierunkowo	Automatycznie
PUMA - moduł Dopłaty rolnicze - paliwa	PUMA - moduł Grunty PUMA - moduł Kontrahent		
PUMA - moduł Ewidencja ludności	PUMA - moduł Wyborcy PUMA - moduł Statystyki PUMA - moduł Eksport danych		
PUMA - moduł Grunty	PUMA - moduł Dopłaty rolnicze – paliwa PUMA - moduł Kontrahent PUMA - moduł Windykacja podatkowa PUMA - moduł Podatki PUMA - moduł Zaświadczenia PUMA - moduł Eksport danych		
PUMA - moduł Kasa	PUMA - moduł Kontrahent PUMA - moduł Windykacja podatkowa PUMA - moduł Opłaty inkasenckie		
PUMA - moduł Kontrahent	PUMA - moduł Ewidencja ludności		
PUMA - moduł OPJ	PUMA - moduł Kontrahent PUMA - moduł Podatki PUMA - moduł Windykacja podatkowa		
PUMA - moduł Płace	PUMA - moduł Kadry PUMA - moduł Kontrahent PUMA - moduł FK		
PUMA - moduł Windykacja podatkowa	PUMA - moduł Kontrahent PUMA - moduł Podatki od osób fizycznych i prawnych PUMA - moduł Kasa PUMA - moduł OPJ PUMA - moduł Opłaty różne		

	PUMA - moduł Podatki od środków transportu		
PUMA - moduł Wyborcy	PUMA - moduł Ewidencja ludności		
PUMA - moduł Zaświadczenia	PUMA - moduł Podatki PUMA - moduł Windykacja PUMA - moduł OPJ PUMA - moduł Kontrahent		

Załącznik Nr 7 do „Polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Bisztynku

Wzór

Raport

z naruszenia bezpieczeństwa systemu informatycznego w Urzędzie Miejskim w Bisztynku

1. Data: .... Godzina: .....

(dd.mm.rr) (gg:mm)

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

.....

(imię, nazwisko, stanowisko służbowe, nazwa użytkownika, (jeśli występuje)

3. Lokalizacja zdarzenia:

.....

(np. nr pokoju, nazwa pomieszczenia)

4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:

.....

.....

.....

5. Przyczyny wystąpienia zdarzenia:

.....

.....

.....

6. Podjęte działania:

.....

.....

.....

7. Postępowanie wyjaśniające:

.....

.....

.....

.....

(data, podpis ADO lub IOD)

Załącznik Nr 8 do „Polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Bisztynku

Wzór

Wykaz osób,

które zostały zapoznane z „Polityką bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Bisztynku

przeznaczonej dla osób zatrudnionych przy przetwarzaniu tych danych.

Lp.	Nazwisko i imię	Stanowisko	Data	Podpis
1.	**Marek Kazimierz Dominiak**	Burmistrz Bisztynka		
2.	**Włodzimierz Mońka**	Zastępca Burmistrza		
3.	**Banach Iwona**	Sekretarz Gminy i Miasta		
4.	**Banaszkiewicz Elżbieta**	Skarbnik Gminy i Miasta		
5.	**Gach Tomasz**	ds. Zarządzania Kryzysowego, spraw Obronnych, Obrony Cywilnej, Informacji Niejawnych, Ochrony p.poż. i BHP		
6.	**Goszcz Elżbieta**	ds. gospodarki gruntami		
7.	**Katarzyna Pawelec**	ds. windykacji należności i obsługi kasy		
8.	**Anna Cieślukowska**	ds. księgowości budżetowej i spraw finansowych		
9.	**Szuksztul Elżbieta**	ds. gospodarki nieruchomościami i lokalami		
10.	**Wójcik Jolanta**	ds. Oświaty, Kultury i Zdrowia Pełnomocnik ds. Informacji Niejawnych		
11.	**Milena Walendziak**	ds. podatków i opłat		

12.	Giczewska Irena	ds. księgowości budżetowej		
13.	Marcin Ignatowski	Radca Prawny		
14.	Anna Sommerfeld	ds. rolnictwa i ochrony środowiska		
15.	Borek Danuta	ds. płac		
16.	Papszun Anna	ds. księgowości budżetowej szkół podstawowych		
17.	Brodowska – Kozerska Beata	Kierownik USC		
18.	Łukasz Hołowieszko	ds. inwestycji, zamówień publicznych, zagospodarowania przestrzennego		
19.	Drozdowski Mariusz	Kierownik Referatu Dróg i Robót Publicznych		
20.	Wadowski Jarosław	ds. informatyki		
21.	Grabowska Marlena	ds. ewidencji działalności gospodarczej, rozwiązywania problemów alkoholowych, zamówień publicznych		
22.	Justyna Łuczyc	ds. księgowości budżetowej Gimnazjum Publicznego i Przedszkola Samorządowego		
23.	Mazur Joanna	ds. obsługi Rady Miejskiej		
24.	Ewa Prościńska	ds. organizacyjnych i kadr		
25.	Martyna Metejunas	ds. kancelaryjno – organizacyjnych		
26.	Kobryń Justyna	ds. promocji gminy i strategii ekorozwoju Gminy		
27.	Paulina Kurpińska	ds. Spraw Obywatelskich		
28.	Piotr Kulczycki	ds. ochrony środowiska		
29.	Katarzyna Rakieć	ds. księgowości budżetowej		
30.	Duplicka Anna			

Załącznik Nr 9 do „Polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Bisztynku

REJESTR CZYNNOŚCI PRZETWARZANIA w Urzędzie Miejskim w Bisztynku		
Lp.	**Opis pola informacyjnego**	**Dane**
1.	**Nazwa administratora danych:**	Urząd Miejski w Bisztynku
2.	**Dane kontaktowe administratora:**	ul. Tadeusza Kościuszki 2, 11-230 Bisztynek
Proces 1		
1.	**Cel przetwarzania danych:**	Obsługa kadrowa
2.	**Zbiór danych:**	Dane osobowe pracowników
3.	**Kategorie danych przetwarzane w procesie:**	Imiona i nazwiska, Imiona rodziców, Data urodzenia, Miejsce urodzenia, Adres zamieszkania lub pobytu, Nr PESEL, Nr NIP, Miejsce pracy, Zawód, Wykształcenie, Seria i nr dowodu osobistego , Nr tel., Nr rachunku bankowego, Stan zdrowia, Inne orzeczenia wydane w postępowaniu sądowym, administracyjnym, egzekucyjnym
4.	**Kategorie odbiorców danych:**	W szczególności Urząd Miejski, ZU, US
5.	**Państwo trzecie, do którego przekazuje się dane:**	Dane nie będą przekazywane do państw trzecich
6.	**Planowany termin usunięcia danych:**	Zgodnie z przepisami prawa
7.	**Opis zabezpieczeń technicznych:**	Wynika z Polityki Bezpieczeństwa
8.	**Opis zabezpieczeń organizacyjnych:**	Wynika z Polityki Bezpieczeństwa

Proces 2		
1.	Cel przetwarzania danych:	Obsługa podmiotów zewnętrznych
2.	Zbiór danych:	Podmioty zewnętrzne
3.	Kategorie danych przetwarzane w procesie:	W szczególności dane teleadresowe , nip
4.	Kategorie odbiorców danych:	W szczególności Urząd Miejski, US
5.	Państwo trzecie, do którego przekazuje się dane:	Dane nie są przekazywane do państwa trzeciego
6.	Planowany termin usunięcia danych:	Zgodnie z przepisami prawa
7.	Opis zabezpieczeń technicznych:	Wynika z Polityki Bezpieczeństwa
8.	Opis zabezpieczeń organizacyjnych:	Wynika z Polityki Bezpieczeństwa

Proces 3		
1.	Cel przetwarzania danych:	Obsługa podatkowa gminy
2.	Zbiór danych:	Podatnicy
3.	Kategorie danych przetwarzane w procesie:	Imiona i nazwiska, Imiona rodziców , Data urodzenia, Miejsce urodzenia, Adres zamieszkania lub pobytu, Nr PESEL, Seria i nr dowodu osobistego,
4.	Kategorie odbiorców danych:	Komornicy
5.	Państwo trzecie, do którego przekazuje się dane:	Dane nie są przekazywane do państwa trzeciego
6.	Planowany termin usunięcia danych:	Zgodnie z przepisami prawa
7.	Opis zabezpieczeń technicznych:	Wynika z Polityki Bezpieczeństwa
8.	Opis zabezpieczeń organizacyjnych:	Wynika z Polityki Bezpieczeństwa

Proces 4

1.	Cel przetwarzania danych:	Rozpatrywanie wniosków
2.	Zbiór danych:	Wnioski o wydanie decyzji środowiskowych
3.	Kategorie danych przetwarzane w procesie:	Imiona i nazwiska, Imiona rodziców , Data urodzenia, Miejsce urodzenia, Adres zamieszkania lub pobytu, Nr PESEL, Nr NIP, Wykształcenie, Nr tel.
4.	Kategorie odbiorców danych:	W szczególności urząd miejski
5.	Państwo trzecie, do którego przekazuje się dane:	Dane nie będą przekazywane do państw trzecich
6.	Planowany termin usunięcia danych:	Zgodnie z przepisami prawa
7.	Opis zabezpieczeń technicznych:	Wynika z Polityki Bezpieczeństwa
8.	Opis zabezpieczeń organizacyjnych:	Wynika z Polityki Bezpieczeństwa

Proces 5

1.	Cel przetwarzania danych:	Wydawanie zaświadczeń
2.	Zbiór danych:	Zaświadczenia
3.	Kategorie danych przetwarzane w procesie:	Imiona i nazwiska, Data urodzenia, Adres zamieszkania lub pobytu, Nr tel.
4.	Kategorie odbiorców danych:	W szczególności urząd miejski i instytucje na potrzeby , których wydane są zaświadczenia
5.	Państwo trzecie, do którego przekazuje się dane:	Dane nie są przekazywane do państwa trzeciego
6.	Planowany termin usunięcia danych:	Zgodnie z przepisami prawa
7.	Opis zabezpieczeń technicznych:	Wynika z Polityki Bezpieczeństwa
8.	Opis zabezpieczeń organizacyjnych:	Wynika z Polityki Bezpieczeństwa

Proces 6

1.	Cel przetwarzania danych:	Gospodarka wodna

2.	Zbiór danych:	Melioracja
3.	Kategorie danych przetwarzane w procesie:	Imiona i nazwiska, Adres zamieszkania lub pobytu, Nr tel.
4.	Kategorie odbiorców danych:	W szczególności urząd miejski
5.	Państwo trzecie, do którego przekazuje się dane:	Dane nie są przekazywane do państwa trzeciego
6.	Planowany termin usunięcia danych:	Zgodnie z przepisami prawa
7.	Opis zabezpieczeń technicznych:	Wynika z Polityki Bezpieczeństwa
8.	Opis zabezpieczeń organizacyjnych:	Wynika z Polityki Bezpieczeństwa
Proces 7		
1.	Cel przetwarzania danych:	Zezwolenia związane z gospodarką odpadami
2.	Zbiór danych:	Odpady
3.	Kategorie danych przetwarzane w procesie:	Imiona i nazwiska, Adres zamieszkania lub pobytu, Nr NIP, Nr tel.
4.	Kategorie odbiorców danych:	W szczególności urząd miejski
5.	Państwo trzecie, do którego przekazuje się dane:	Dane nie będą przekazywane do państw trzecich
6.	Planowany termin usunięcia danych:	Zgodnie z przepisami prawa
7.	Opis zabezpieczeń technicznych:	Wynika z Polityki Bezpieczeństwa
8.	Opis zabezpieczeń organizacyjnych:	Wynika z Polityki Bezpieczeństwa
Proces 8		
1.	Cel przetwarzania danych:	Rejestr działalności regulowanej
2.	Zbiór danych:	Rejestr działalności dot. odpadów
3.	Kategorie danych przetwarzane w procesie:	Imiona i nazwiska, Adres zamieszkania lub pobytu, Nr NIP, Wykształcenie, Nr tel.
4.	Kategorie odbiorców danych:	W szczególności urząd miejski

5.	Państwo trzecie, do którego przekazuje się dane:	Dane nie są przekazywane do państwa trzeciego
6.	Planowany termin usunięcia danych:	Zgodnie z przepisami prawa
7.	Opis zabezpieczeń technicznych:	Wynika z Polityki Bezpieczeństwa
8.	Opis zabezpieczeń organizacyjnych:	Wynika z Polityki Bezpieczeństwa

Proces 9

1.	Cel przetwarzania danych:	Rozpatrywanie wniosków dot. usunięcia drzew i krzewów
2.	Zbiór danych:	Usunięcia drzew i krzewów
3.	Kategorie danych przetwarzane w procesie:	Imiona i nazwiska, Adres zamieszkania lub pobytu, Nr tel., Nr działki
4.	Kategorie odbiorców danych:	W szczególności urząd miejski i inne instytucje uprawnione
5.	Państwo trzecie, do którego przekazuje się dane:	Dane nie są przekazywane do państwa trzeciego
6.	Planowany termin usunięcia danych:	Zgodnie z przepisami prawa
7.	Opis zabezpieczeń technicznych:	Wynika z Polityki Bezpieczeństwa
8.	Opis zabezpieczeń organizacyjnych:	Wynika z Polityki Bezpieczeństwa

Proces 10

1.	Cel przetwarzania danych:	Rozpatrywanie podziału nieruchomości
2.	Zbiór danych:	Podział nieruchomości
3.	Kategorie danych przetwarzane w procesie:	Imiona i nazwiska, Adres zamieszkania lub pobytu, Nr działki
4.	Kategorie odbiorców danych:	W szczególności urząd miejski i inne instytucje uprawnione
5.	Państwo trzecie, do którego przekazuje się dane:	Dane nie są przekazywane do państwa trzeciego

6.	Planowany termin usunięcia danych:	Zgodnie z przepisami prawa
7.	Opis zabezpieczeń technicznych:	Wynika z Polityki Bezpieczeństwa
8.	Opis zabezpieczeń organizacyjnych:	Wynika z Polityki Bezpieczeństwa

Proces 11

1.	**Cel przetwarzania danych:**	Wykonywanie umów
2.	**Zbiór danych:**	Umowy, zlecenia
3.	**Kategorie danych przetwarzane w procesie:**	Imiona i nazwiska, Adres zamieszkania lub pobytu, Nr PESEL, Nr NIP, Miejsce pracy , Nr tel., Nr rachunku bankowego
4.	**Kategorie odbiorców danych:**	W szczególności urząd miejski i inne instytucje uprawnione
5.	**Państwo trzecie, do którego przekazuje się dane:**	Dane nie są przekazywane do państwa trzeciego
6.	**Planowany termin usunięcia danych:**	Zgodnie z przepisami prawa
7.	**Opis zabezpieczeń technicznych:**	Wynika z Polityki Bezpieczeństwa
8.	**Opis zabezpieczeń organizacyjnych:**	Wynika z Polityki Bezpieczeństwa

Proces 12

1.	**Cel przetwarzania danych:**	Rejestracja organów jednostek samorządu terytorialnie
2.	**Zbiór danych:**	Sołtysi
3.	**Kategorie danych przetwarzane w procesie:**	Imiona i nazwiska, Adres zamieszkania lub pobytu, Nr tel.
4.	**Kategorie odbiorców danych:**	W szczególności urząd miejski i inne instytucje uprawnione
5.	**Państwo trzecie, do którego przekazuje się dane:**	Dane nie są przekazywane do państwa trzeciego
6.	**Planowany termin usunięcia danych:**	Zgodnie z przepisami prawa

7.	Opis zabezpieczeń technicznych:	Wynika z Polityki Bezpieczeństwa
8.	Opis zabezpieczeń organizacyjnych:	Wynika z Polityki Bezpieczeństwa

Proces 13

1.	**Cel przetwarzania danych:**	Rejestracja szkód łowieckich
2.	**Zbiór danych:**	Szkody Łowieckie
3.	**Kategorie danych przetwarzane w procesie:**	Imiona i nazwiska, Adres zamieszkania lub pobytu, Wykształcenie, Nr tel.,
4.	**Kategorie odbiorców danych:**	W szczególności urząd miejski i inne instytucje uprawnione
5.	**Państwo trzecie, do którego przekazuje się dane:**	Dane nie są przekazywane do państwa trzeciego
6.	**Planowany termin usunięcia danych:**	Zgodnie z przepisami prawa
7.	**Opis zabezpieczeń technicznych:**	Wynika z Polityki Bezpieczeństwa
8.	**Opis zabezpieczeń organizacyjnych:**	Wynika z Polityki Bezpieczeństwa

Proces 14

1.	**Cel przetwarzania danych:**	Gospodarka nieruchomościami
2.	**Zbiór danych:**	Sprzedaż nieruchomości
3.	**Kategorie danych przetwarzane w procesie:**	
4.	**Kategorie odbiorców danych:**	W szczególności urząd miejski i inne instytucje uprawnione
5.	**Państwo trzecie, do którego przekazuje się dane:**	Dane nie są przekazywane do państwa trzeciego
6.	**Planowany termin usunięcia danych:**	Zgodnie z przepisami prawa
7.	**Opis zabezpieczeń technicznych:**	Wynika z Polityki Bezpieczeństwa

8.	Opis zabezpieczeń organizacyjnych:	Wynika z Polityki Bezpieczeństwa

Proces 15

1.	Cel przetwarzania danych:	Gospodarka nieruchomościami
2.	Zbiór danych:	Dzierżawy gruntów
3.	Kategorie danych przetwarzane w procesie:	
4.	Kategorie odbiorców danych:	
5.	Państwo trzecie, do którego przekazuje się dane:	Dane nie są przekazywane do państwa trzeciego
6.	Planowany termin usunięcia danych:	
7.	Opis zabezpieczeń technicznych:	Wynika z Polityki Bezpieczeństwa
8.	Opis zabezpieczeń organizacyjnych:	Wynika z Polityki Bezpieczeństwa

Proces 16

1.	Cel przetwarzania danych:	Gospodarka nieruchomościami
2.	Zbiór danych:	Nadanie numeru nieruchomości
3.	Kategorie danych przetwarzane w procesie:	
4.	Kategorie odbiorców danych:	
5.	Państwo trzecie, do którego przekazuje się dane:	Dane nie są przekazywane do państwa trzeciego
6.	Planowany termin usunięcia danych:	
7.	Opis zabezpieczeń technicznych:	Wynika z Polityki Bezpieczeństwa
8.	Opis zabezpieczeń organizacyjnych:	Wynika z Polityki Bezpieczeństwa

Proces 17		
1.	Cel przetwarzania danych:	Gospodarka nieruchomościami
2.	Zbiór danych:	Akta osiedleńcze
3.	Kategorie danych przetwarzane w procesie:	
4.	Kategorie odbiorców danych:	
5.	Państwo trzecie, do którego przekazuje się dane:	Dane nie są przekazywane do państwa trzeciego
6.	Planowany termin usunięcia danych:	
7.	Opis zabezpieczeń technicznych:	Wynika z Polityki Bezpieczeństwa
8.	Opis zabezpieczeń organizacyjnych:	Wynika z Polityki Bezpieczeństwa

Proces 18		
1.	Cel przetwarzania danych:	Gospodarka nieruchomościami
2.	Zbiór danych:	Decyzje o nadaniu działki na własność
3.	Kategorie danych przetwarzane w procesie:	
4.	Kategorie odbiorców danych:	
5.	Państwo trzecie, do którego przekazuje się dane:	Dane nie są przekazywane do państwa trzeciego
6.	Planowany termin usunięcia danych:	
7.	Opis zabezpieczeń technicznych:	Wynika z Polityki Bezpieczeństwa
8.	Opis zabezpieczeń organizacyjnych:	Wynika z Polityki Bezpieczeństwa

Proces 19

1.	Cel przetwarzania danych:	Gospodarka nieruchomościami
2.	Zbiór danych:	Aktualizacja opłat rocznych z tytułu użytkowania wiecz.
3.	Kategorie danych przetwarzane w procesie:	
4.	Kategorie odbiorców danych:	
5.	Państwo trzecie, do którego przekazuje się dane:	Dane nie są przekazywane do państwa trzeciego
6.	Planowany termin usunięcia danych:	
7.	Opis zabezpieczeń technicznych:	Wynika z Polityki Bezpieczeństwa
8.	Opis zabezpieczeń organizacyjnych:	Wynika z Polityki Bezpieczeństwa

Proces 20

1.	Cel przetwarzania danych:	Zadania gminy w zakresie służby wojskowej
2.	Zbiór danych:	Listy do kwalifikacji wojskowej
3.	Kategorie danych przetwarzane w procesie:	
4.	Kategorie odbiorców danych:	
5.	Państwo trzecie, do którego przekazuje się dane:	Dane nie są przekazywane do państwa trzeciego
6.	Planowany termin usunięcia danych:	
7.	Opis zabezpieczeń technicznych:	Wynika z Polityki Bezpieczeństwa
8.	Opis zabezpieczeń organizacyjnych:	Wynika z Polityki Bezpieczeństwa

Proces 21

1.	Cel przetwarzania danych:	Administracja

2.	Zbiór danych:	Listy osób pełniących świadczenia osobowe, rzeczowe
3.	Kategorie danych przetwarzane w procesie:	
4.	Kategorie odbiorców danych:	
5.	Państwo trzecie, do którego przekazuje się dane:	Dane nie są przekazywane do państwa trzeciego
6.	Planowany termin usunięcia danych:	
7.	Opis zabezpieczeń technicznych:	Wynika z Polityki Bezpieczeństwa
8.	Opis zabezpieczeń organizacyjnych:	Wynika z Polityki Bezpieczeństwa

Proces 22

1.	Cel przetwarzania danych:	Rejestr
2.	Zbiór danych:	Wykaz członków Formacji OC
3.	Kategorie danych przetwarzane w procesie:	
4.	Kategorie odbiorców danych:	
5.	Państwo trzecie, do którego przekazuje się dane:	Dane nie są przekazywane do państwa trzeciego
6.	Planowany termin usunięcia danych:	
7.	Opis zabezpieczeń technicznych:	Wynika z Polityki Bezpieczeństwa
8.	Opis zabezpieczeń organizacyjnych:	Wynika z Polityki Bezpieczeństwa

Proces 23

1.	Cel przetwarzania danych:	Administracja podatkami lokalnymi
2.	Zbiór danych:	Kartoteka podatkowa
3.	Kategorie danych przetwarzane w procesie:	

4.	Kategorie odbiorców danych:	
5.	Państwo trzecie, do którego przekazuje się dane:	Dane nie są przekazywane do państwa trzeciego
6.	Planowany termin usunięcia danych:	
7.	Opis zabezpieczeń technicznych:	Wynika z Polityki Bezpieczeństwa
8.	Opis zabezpieczeń organizacyjnych:	Wynika z Polityki Bezpieczeństwa

	Proces 24	
1.	Cel przetwarzania danych:	Rozpatrywanie wniosków podatników
2.	Zbiór danych:	Wnioski podatników
3.	Kategorie danych przetwarzane w procesie:	
4.	Kategorie odbiorców danych:	
5.	Państwo trzecie, do którego przekazuje się dane:	Dane nie są przekazywane do państwa trzeciego
6.	Planowany termin usunięcia danych:	
7.	Opis zabezpieczeń technicznych:	Wynika z Polityki Bezpieczeństwa
8.	Opis zabezpieczeń organizacyjnych:	Wynika z Polityki Bezpieczeństwa

	Proces 25	
1.	Cel przetwarzania danych:	Rozpatrywanie wniosków o zaświadczenia
2.	Zbiór danych:	Zaświadczenia
3.	Kategorie danych przetwarzane w procesie:	
4.	Kategorie odbiorców danych:	

5.	Państwo trzecie, do którego przekazuje się dane:	Dane nie są przekazywane do państwa trzeciego
6.	Planowany termin usunięcia danych:	
7.	Opis zabezpieczeń technicznych:	Wynika z Polityki Bezpieczeństwa
8.	Opis zabezpieczeń organizacyjnych:	Wynika z Polityki Bezpieczeństwa

Załącznik Nr 10 do „Polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Bisztynku

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Niniejszym, jako Administrator Danych występujący pod nazwą **Urząd Miejski w Bisztynku** zwanym (dalej Administrator Danych), na mocy delegacji uprawnienia do nadawania upoważnień wynikających z uprawnień Administratora Danych, na podstawie art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1) – dalej **RODO (GDPR) oraz przepisów** Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (tekst jedn. Dz. U. z 2018 r., poz. 1000), niniejszym upoważniam do przetwarzania danych osobowych w formie papierowej oraz systemach informatycznych :

Imię i nazwisko osoby upoważnianej	Zbiory danych objęte zakresem upoważnienia	Data nadania upoważnienia

Osoba upoważniona obowiązana jest przetwarzać dane osobowe zawarte w ww. zbiorach danych osobowych w zakresie i w sposób wymagany do wypełnienia obowiązków służbowych względem Administratora Danych.

Osoba upoważniona zobowiązuje się do przetwarzania danych osobowych zgodnie z udzielonym upoważnieniem oraz z przepisami RODO, ustawy o ochronie danych osobowych, wydanymi na jej podstawie aktami wykonawczymi i obowiązującymi u Administratora danych wewnętrznymi regulacjami w sprawie ochrony danych osobowych.

Naruszenie ww. obowiązków może skutkować poniesieniem odpowiedzialności karnej na podstawie przepisów określonych w Ustawie o ochronie danych osobowych oraz stanowi ciężkie naruszenie obowiązków pracowniczych wynikających z art.100 § 2 pkt 4 i 5 Kodeksu Pracy, które może być podstawą rozwiązania umowy o pracę w trybie art. 52 Kodeksu Pracy lub odpowiedzialności cywilnej.

.....
Data i podpis upoważniającego

.....
Data i podpis osoby upoważnionej

Oświadczenie

Oświadczam, że zapoznałam/em się – w zakresie wynikającym z przydzielonych zadań – z obowiązującymi w odniesieniu do ochrony danych osobowych przepisami prawa i regulacjami wewnętrznymi obowiązującymi u Administratora Danych (w szczególności z Dokumentacją ochrony danych osobowych). Przyjmuję do wiadomości zawarte w nich obowiązki dotyczące ochrony danych osobowych i zobowiązuję się do ich stosowania.

Świadoma/y jestem obowiązku ochrony danych osobowych na zajmowanym stanowisku i w zakresie udzielonego mi upoważnienia do przetwarzania danych osobowych, a w szczególności obowiązku zachowania w tajemnicy danych osobowych i sposobów ich zabezpieczenia, również po ustaniu zatrudnienia lub współpracy.

.....
Data i podpis osoby upoważnionej

Załącznik Nr 11 do „Polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Bisztynku

REJESTR NARUSZEŃ BEZPIECZEŃSTWA

Naruszenie bezpieczeństwa – opis naruszenia	Źródło zgłoszenia – osoba/podmiot zgłaszający incydent	Data rozpoczęcia	Data zakończenia	Odpowiedzialny za błąd/naruszenie lub informacja o braku takiej osoby	Przyczyna	Działanie zapobiegawcze / korygujące wraz ze wskazaniem osoby odpowiedzialnej za wykonanie	Ocena skuteczności podjętych działań

Dla .....

(dane administratora)

Załącznik Nr 12 do „Polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Bisztynku

Urząd Ochrony Danych Osobowych

ul. Stawki 2

00-193 Warszawa

ZGŁOSZENIE

W SPRAWIE NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Niniejszym w trybie art. 33 ogólnego rozporządzenia o ochronie danych, zgłaszam naruszenie ochrony danych osobowych, które miało miejsce w dniu … w … .

1.	**Charakter naruszenia ochrony danych:**	Np. *Przesłanie przez pracownika wiadomości e-mail do błędnego adresata (nieznana osoba) zamiast do współpracownika wraz z załącznikiem w formacie pliku Excel (takie jak: imię i nazwisko, adres zamieszkania, PESEL, nr. dowodu tożsamości,, numer telefonu, adresy e-mail)*
2.	**Kategoria i przybliżona liczba osób, których dane dotyczą:**	Np.. *Liczba osób, których dane dotyczą .....*
3.	**Liczba wpisów, których dotyczy naruszenie:**	Np. *821*
4.	**Możliwe konsekwencje naruszenia ochrony danych:**	Np. *Powstanie szkód majątkowych u osób fizycznych, takich jak utrata kontroli nad własnymi danymi osobowymi lub kradzież lub sfałszowanie tożsamości, strata finansowa*
5.	**Środki zastosowane lub proponowane w celu zaradzenia naruszenia ochrony danych osobowych, w tym zastosowane środki w celu zminimalizowania ewentualnych negatywnych skutków naruszenia ochrony danych:**	Np. *Wdrożenie stosownych środków kryptograficznych, w tym w tym pseudonimizacja, zakaz przesyłania załączników zawierających dane osobowe w sposób niezabezpieczony.*
6.	**Dane inspektora ochrony danych**	Np. ....., *nr. telefonu: XXX XXX XXX, adres e-mail: iod@domena.pl*

.....

(podpis)

*W przypadku zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin, administrator danych zobowiązany jest do złożenia wyjaśnień w przedmiocie przyczyn opóźnienia.

....., dnia ..... r.

.....
(pieczęć Administratora)

Załącznik Nr 13 do „Polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Bisztynku

Komunikat o naruszeniu ochrony danych

Komunikat o naruszeniu ochrony danych z dnia .....

1.	Charakter naruszenia ochrony danych:	
2.	Kategoria i przybliżona liczba osób, których dane dotyczą:	
3.	Liczba wpisów, których dotyczy naruszenie:	
4.	Możliwe konsekwencje naruszenia ochrony danych:	
5.	Środki zastosowane lub proponowane w celu zaradzenia naruszenia ochrony danych osobowych, w tym środki zastosowane w celu zminimalizowania ewentualnych negatywnych skutków naruszenia ochrony danych:	

.....

DODATKOWE PROCEDURY

1. PROCEDURY ZWIĄZANE Z PRAWAMI JEDNOSTKI
2. PROCEDURA WYCOFANIA NOŚNIKÓW
3. INSTRUKCJA BEZPIECZENGO PRZESYŁANIA INFORMACJI CYFROWYCH

PROCEDURY ZWIĄZANE Z PRAWAMI JEDNOSTKI

PROCEDURA 1

Prawo do ograniczenia przetwarzania danych

Procedura bezpieczeństwa przetwarzania danych osobowych		Data wprowadzenia: 00.00.2018 r.
Numer Procedury : 1	Realizacja prawa do ograniczenia przetwarzania danych osoby, której dane dotyczą	Nr wersji procedury : 1.0
		Ilość stron : 2

1. Uczestnicy procedury:

- wnioskodawca;
- osoba upoważniona do przetwarzania danych osobowych;
- Administrator Systemu Informatycznego;
- Administrator danych.

2. Wymagane dokumenty:

- wniosek osoby, której dane dotyczą, o ograniczenie przetwarzania jego danych osobowych;
- ewidencja udzielanych informacji w sprawach dotyczących praw osób, których dane dotyczą;
- odpowiedź na wniosek.

3. Przesłanki warunkujące skuteczność żądania:

Osoba, której dane dotyczą, ma prawo żądania ograniczenia przetwarzania w następujących przypadkach:

- osoba ta kwestionuje prawidłowość danych osobowych – na okres pozwalający sprawdzić prawidłowość tych danych;
- przetwarzanie jest niezgodne z prawem, a osoba ta sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;
- Administrator Danych nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne tej osobie do ustalenia, dochodzenia lub obrony roszczeń;
- osoba ta wniosła sprzeciw wobec przetwarzania jej danych – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie Administratora Danych są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.

4. Procedura:

- rejestracja wniosku
- ustalenie zasadności żądania;
- przedstawienie propozycji działania Administratorowi danych;
- w przypadku żądania uzasadnionego (pkt 3):
  - powiadomić Administratora danych o konieczności ograniczenia przetwarzania danych,

- na podstawie decyzji Administratora danych ograniczyć przetwarzanie tylko do przechowywania danych,
- przygotować odpowiedź na żądanie i przedstawić ją do podpisu Administratorowi danych,
- wysłać odpowiedź wnioskodawcy i poinformować o odbiorcach danych, jeżeli żądano tego we wniosku,
- poinformować pisemnie odbiorców danych o decyzji ograniczenia przetwarzania,

W przypadku podjęcia decyzji o ograniczeniu przetwarzania danych – dane te można przetwarzać wyłącznie za zgodą osoby, której dane dotyczą, lub w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego;

5. W przypadku żądania nieuzasadnionego:

- sporządzić decyzję odmowną ograniczenia przetwarzania z uzasadnieniem,
- przedstawić decyzję do podpisu Administratorowi danych;
- przesłać decyzję wnioskodawcy listem poleconym.

PROCEDURA 2

Prawo dostępu do danych

Procedura bezpieczeństwa przetwarzania danych osobowych		Data wprowadzenia: 00.00.2018 r.
Numer Procedury : 2	Realizacja prawa dostępu do danych osobowych osoby, której dane dotyczą	Nr wersji procedury : 1.0
		Ilość stron : 1

1. Uczestnicy procedury:

- wnioskodawca
- osoby wyznaczone do realizacji prawa przez Administratora;
- Administrator danych.

2. Wymagane dokumenty:

- wniosek o udostępnienie danych osobowych;
- wzór odpowiedzi na żądanie prawa dostępu do danych;
- ewidencja udzielanych informacji w sprawach dotyczących praw osób, których dane dotyczą.

3. Procedura:

- ujęcie wniosku na ewidencję;
- przygotowanie odpowiedzi na wniosek;
- przedstawienie Administratorowi danych wniosku do podpisu;
- wysłanie odpowiedzi do wnioskodawcy;
- dokonanie wpisu w ewidencji o wysłaniu odpowiedzi na wniosek.

4. Uwagi:

- udzielane informacje:
  - cele przetwarzania danych osobowych,
  - kategorie danych osobowych,
  - odbiorcy lub kategorie odbiorców danych,
  - planowany okres przechowywania danych osobowych lub kryteria ustalania tego okresu,
  - informacje o prawie do sprostowania danych, usunięcia lub ograniczenia przetwarzania danych osobowych oraz do wniesienia sprzeciwu wobec takiego przetwarzania,
  - informacja o prawie wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych w Warszawie,
  - informacja źródle pozyskania danych osobowych,

- informacja o zautomatyzowanym podejmowaniu decyzji, w tym profilowaniu oraz istotne informacje o zasada ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą;

- wnioskodawcy dostarcza się kopie danych osobowych podlegających przetwarzaniu. Za kolejne kopie pobiera się opłatę, wynikającą z kosztów administracyjnych.

PROCEDURA 3

Prawo do sprostowania danych

Procedura bezpieczeństwa przetwarzania danych osobowych		Data wprowadzenia: 00.00.2018 r.
Numer Procedury : 3	Realizacja prawa do sprostowania danych osoby, której dane dotyczą	**Nr wersji procedury : 1.0**
		Ilość stron : 1

1. **Uczestnicy procedury:**

- wnioskodawca;
- osoba upoważniona do przetwarzania danych osobowych;
- Administrator Systemu Informatycznego;
- Administrator danych.

2. **Wymagane dokumenty:**

- wniosek osoby, której dane dotyczą, o sprostowanie danych osobowych;
- ewidencja udzielanych informacji w sprawach dotyczących praw osób, których dane dotyczą;
- odpowiedź na wniosek;
- opcjonalnie – dodatkowe oświadczenie o przetwarzaniu danych osobowych.

3. **Procedura:**

- rejestracja wniosku ;
- sprostowanie nieprawidłowych danych osobowych w zbiorze przetwarzanym w systemie informatycznym lub przetwarzanym tradycyjnie;
- przygotowanie odpowiedzi na wniosek o sprostowaniu danych;
- przedstawienie odpowiedzi na wniosek do podpisu Administratorowi danych;
- przesłanie wnioskodawcy odpowiedzi na wniosek;
- opcjonalnie – przesłanie wnioskodawcy dodatkowego oświadczenia o przetwarzaniu danych osobowych;
- przesłać odbiorcom danych informację o decyzji sprostowania danych

PROCEDURA 4

Prawo do usunięcia danych - bycia zapomnianym

Procedura bezpieczeństwa przetwarzania danych osobowych	Data wprowadzenia: 00.00.2018 r.

Numer Procedury : 4	Realizacja prawa do usunięcia danych - do bycia zapomnianym - osoby, której dane dotyczą	Nr wersji procedury : 1.0 Ilość stron : 2

1. Uczestnicy procedury:

- wnioskodawca;
- osoba upoważniona do przetwarzania danych osobowych;
- Administrator Systemu Informatycznego;
- Administrator danych.

2. Wymagane dokumenty:

- wniosek osoby, której dane dotyczą, o usunięcie danych osobowych („bycia zapomnianym");
- ewidencja udzielanych informacji w sprawach dotyczących praw osób, których dane dotyczą;
- odpowiedź na wniosek.

3. Przesłanki warunkujące żądanie usunięcia danych („do bycia zapomnianym"):

- dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
- osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie danych „zwykłych" lub „szczególnych kategorii" i nie ma innej podstawy prawnej przetwarzania;
- osoba, której dane dotyczą, wnosi sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania jej danych osobowych:
  - w celu wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi Danych,
  - do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora Danych, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem,
  - opartych na profilowaniu;

    i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania,

  - na potrzeby marketingu bezpośredniego, w tym profilowania;
- dane osobowe są przetwarzane niezgodnie z prawem;
- dane osobowe muszą być usunięte w celu wywiązania się z obowiązku prawnego;
- dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego oferowanych dziecku, które ukończyło 16 lat.

W przypadku upublicznienia danych osobowych Administratora Danych ma obowiązek usunąć te dane osobowe, podejmując w tym celu rozsądne działania, w tym środki techniczne, by poinformować administratorów przetwarzających te dane osobowe, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich repliki.

4. Nieskuteczność żądania:

Żądanie usunięcia danych („bycia zapomnianym") jest nieskuteczne w zakresie w jakim przetwarzanie jest niezbędne:

- do korzystania z prawa do wolności wypowiedzi i informacji;
- do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi Danych;
- z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego:
  - profilaktyki zdrowotnej, medycyny pracy, oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa lub zgodnie z umową z pracownikami służby zdrowia,
  - interes publiczny w dziedzinie zdrowia publicznego, taki jak ochrona przed zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub

wyrobów medycznych, na podstawie prawa, które przewiduje odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową,

z zastrzeżeniem warunków i zabezpieczeń, że dane osobowe będą przetwarzane przez lub na odpowiedzialność pracownika podlegającego obowiązkowi zachowania tajemnicy zawodowej na mocy prawa lub przepisów ustanowionych przez właściwe organy krajowe lub przez inną osobę również podlegającą obowiązkowi zachowania tajemnicy zawodowej na mocy prawa lub przepisów ustanowionych przez właściwe organy krajowe;

- do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub dla celów statystycznych, o ile prawdopodobne jest, że realizacja prawa do usunięcia danych uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania;
- do ustalenia, dochodzenia lub obrony roszczeń.

5. Procedura:

- rejestracja wniosku;
- ustalenie zasadności żądania;
- w przypadku żądania uzasadnionego (pkt 3):
  - powiadomić Administratora danych o konieczności usunięcia danych,
  - na podstawie decyzji Administratora danych usunąć dane i powiadomić innych administratorów w przypadku upublicznienia danych,
  - przygotować odpowiedź na żądanie i przedstawić ją do podpisu Administratorowi danych,
  - wysłać odpowiedź wnioskodawcy i poinformować go o odbiorcach danych,
  - poinformować odbiorców danych o decyzji usunięcia danych;

- w przypadku żądania nieuzasadnionego (pkt 4):
  - powiadomić Kierownika Administratora danych o nieskuteczności żądania, z określeniem przyczyny,
  - przygotować odpowiedź na żądanie wnioskodawcy i przedstawić ją do podpisu Administratorowi danych,
  - wysłać odpowiedź wnioskodawcy.

PROCEDURA 5

Prawo do przenoszenia danych

Procedura bezpieczeństwa przetwarzania danych osobowych		Data wprowadzenia: 00.00.2018 r.
Numer Procedury : 5	Realizacja prawa do przenoszenia danych osoby, której dane dotyczą	Nr wersji procedury : 1.0
		Ilość stron : 2

1. Uczestnicy procedury:

- wnioskodawca
- osoba upoważniona do przetwarzania danych osobowych;
- Administrator Systemu Informatycznego;
- Administrator danych.

2. Wymagane dokumenty:

- wniosek osoby, której dane dotyczą, o przeniesienie danych osobowych;
- ewidencja udzielanych informacji w sprawach dotyczących praw osób, których dane dotyczą;
- odpowiedź na wniosek.

3. Przesłanki warunkujące zasadność żądania:

Osoba, której dane dotyczą ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do druku dane osobowe jej dotyczące, które dostarczyła Administratorowi Danych, oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane, jeżeli:

- przetwarzanie odbywa się na podstawie zgody lub umowy;
- przetwarzanie odbywa się w sposób zautomatyzowany.

Wykonując prawo do przenoszenia danych osoba, której dane dotyczą, ma prawo żądania, by dane osobowe zostały przesłane przez Administratora Danych bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe.

4. Nieskuteczność żądania:

- prawo do przenoszenia danych nie ma zastosowania do przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi Danych;
- prawo do przenoszenia danych nie ma zastosowania w przypadku przetwarzania danych dla celów interesu publicznego w dziedzinie zdrowia publicznego takich, jak:
  - profilaktyka zdrowotna, medycyna pracy, ocena zdolności pracownika do pracy, diagnoza medyczna, zapewnienie opieki zdrowotnej lub zabezpieczenia społecznego, leczenie lub zarządzanie systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa lub zgodnie z umową z pracownikami służby zdrowia,
  - ochrona przed zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa, które przewiduje odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową,

z zastrzeżeniem warunków i zabezpieczeń, że dane osobowe będą przetwarzane przez lub na odpowiedzialność pracownika podlegającego obowiązkowi zachowania tajemnicy zawodowej na mocy prawa lub przepisów ustanowionych przez właściwe organy krajowe lub przez inną osobę również podlegającą obowiązkowi zachowania tajemnicy zawodowej na mocy prawa lub przepisów ustanowionych przez właściwe organy krajowe;

- prawo do przenoszenia danych nie ma zastosowania w przypadku przetwarzania danych dla celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub dla celów statystycznych, o ile prawdopodobne jest, że realizacja prawa do usunięcia danych uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania;
- prawo do przenoszenia danych nie ma zastosowania w przypadku przetwarzania danych dla celów ustalenia, dochodzenia lub obrony roszczeń.

5. Procedura:

- rejestracja wniosku ;
- ustalenie zasadności żądania;
- przedstawienie propozycji działania Administratorowi danych;
- w przypadku żądania uzasadnionego (pkt 3):
  - powiadomić Administratora danych o konieczności przeniesienia danych,
  - na podstawie decyzji Administratora danych przygotować w ustrukturyzowanym, powszechnie używanym formacie nadającym się do druku dane osobowe dotyczące wnioskodawcy,
  - przesłać wnioskodawcy przygotowane dane lub bezpośrednio wskazanemu przez wnioskodawcę administratorowi,
  - poinformować pisemnie wnioskodawcę o sposobie realizacji wniosku;

- w przypadku żądania nieuzasadnionego (pkt 4):
  - sporządzić decyzję odmowną z uzasadnieniem,
  - przedstawić decyzję do podpisu Administratorowi danych;
  - przesłać decyzję wnioskodawcy listem poleconym za potwierdzeniem odbioru.

PROCEDURA 6

PRAWO DO SPRZECIWU NA ZAUTOMATYZOWANE PODEJMOWANIE DECYZJI, W TYM PROFILOWANIE

Procedura bezpieczeństwa przetwarzania danych osobowych		Data wprowadzenia: 00.00.2018 r.
Numer Procedury : 6	Realizacja prawa do sprzeciwu na zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach, w tym profilowanie	Nr wersji procedury : 1.0
		Ilość stron : 2

1. Uczestnicy procedury:

- wnioskodawca;
- osoba upoważniona do przetwarzania danych osobowych;
- Administrator Systemu Informatycznego;
- Administrator danych.

2. Wymagane dokumenty:

- sprzeciw osoby, której dane dotyczą, na zautomatyzowane podejmowanie decyzji, w tym profilowanie;
- ewidencja udzielanych informacji w sprawach dotyczących praw osób, których dane dotyczą;
- odpowiedź na sprzeciw.

3. Przesłanki warunkujące skuteczność sprzeciwu:

- osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania jej danych celem:
  - wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi,
  - wynikającym z prawnie uzasadnionych interesów realizowanych przez administratora, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem, w tym profilowania. W takich przypadkach nie wolno już przetwarzać tych danych osobowych, chyba że wykaże się istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń;

- jeżeli dane osobowe są przetwarzane na potrzeby marketingu bezpośredniego, osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania dotyczących jej danych osobowych na potrzeby takiego marketingu, w tym profilowania, w zakresie, w jakim przetwarzanie jest związane z takim marketingiem bezpośrednim. W taki przypadku nie wolno już przetwarzać tych danych osobowych do takich celów;

- jeżeli dane osobowe są przetwarzane do celów badań naukowych lub historycznych lub do celów statystycznych, osoba, której dane dotyczą, ma prawo wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym;
- osoba, której dane dotyczą, ma prawo by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa.

Uwagi:

- najpóźniej przy okazji pierwszej komunikacji z osobą, której dane dotyczą, wyraźnie informuje się ją o prawie do sprzeciwu w przypadku celów przetwarzania określonych w ust. 3 pkt 1 i 2
- osoba, której dane dotyczą, może wykonać prawo do sprzeciwu za pośrednictwem zautomatyzowanych środków wykorzystujących specyfikacje techniczne.

4. Nieskuteczność sprzeciwu:

W przypadku zautomatyzowanego przetwarzania danych osobowych, w tym profilowania sprzeciw jest nieskuteczny w przypadku:

- gdy decyzja jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a administratorem;
- gdy takie przetwarzanie danych jest dozwolone prawem i które przewiduje właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą;
- jeżeli decyzja opiera się na wyraźnej zgodzie osoby, której dane dotyczą.

Decyzje nie mogą opierać się na szczególnych kategoriach danych osobowych, chyba że osoba, której dane dotyczą wyraziła na to zgodę lub dane przetwarzane są ze względu na ważny interes publiczny.

5. Procedura:

- rejestracja sprzeciwu ;
- ustalenie zasadności sprzeciwu;
- przedstawienie propozycji decyzji Administratorowi danych;
- w przypadku sprzeciwu uzasadnionego (pkt 3):
  - powiadomić Administratora danych o konieczności zaprzestania przetwarzania danych,
  - zaprzestać przetwarzanie danych osobowych,
  - na podstawie decyzji Administratora danych przygotować odpowiedź na sprzeciw,
  - poinformować pisemnie osobę wnoszącą sprzeciw o sposobie realizacji żądania;

- w przypadku nieskuteczności sprzeciwu (pkt 4):
  - sporządzić decyzję odmowną z uzasadnieniem,
  - przedstawić decyzję do podpisu Administratorowi danych,
  - przesłać decyzję wnioskodawcy listem poleconym za potwierdzeniem odbio

PROCEDURA 7

Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych

Procedura bezpieczeństwa przetwarzania danych osobowych		Data wprowadzenia: 00.00.2018 r.
Numer Procedury : 7	Zawiadamianie osoby, której dane dotyczą o naruszeniu ochrony danych osobowych	**Nr wersji procedury : 1.0**
		Ilość stron : 1

1. Uczestnicy procedury:

- Inspektor Ochrony Danych Osobowych;
- Administrator danych.

2. Wymagane dokumenty:

- zawiadomienie o naruszeniu ochrony danych osobowych;
- ewidencja naruszeń ochrony danych osobowych.

3. Wymagalność zawiadomienia osoby, której dane dotyczą:

Zawiadomienie jest wymagane jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.

Zawiadomienie powinno jasnym i prostym językiem opisać charakter naruszenia ochrony danych osobowych oraz zawierać:

- imię i nazwisko Inspektora Ochrony Danych Osobowych oraz jego dane kontaktowe
- możliwe konsekwencje naruszenia ochrony danych osobowych
- środki zastosowane lub proponowane w celu zaradzenia naruszeniu ochrony danych osobowych w tym środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

4. Przypadki, w których nie jest wymagane zawiadomienie:

- administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i zostały one zastosowane do danych osobowych, których dotyczy naruszenie – w szczególności takie jak szyfrowanie;
- administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą;
- zawiadomienie osoby, której dane dotyczą, wymagałoby niewspółmiernie dużego wysiłku – w tym przypadku administrator wydaje publiczny komunikat lub stosuje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

5. Procedura:

- na podstawie raportu ASI opracować zawiadomienie osoby, której dane dotyczy, o naruszeniu ochrony jej danych;
- zarejestrować zawiadomienie w *Ewidencji naruszeń ochrony danych osobowych*;
- przedstawić zawiadomienie Administratorowi danych do podpisu;
- przesłać zawiadomienie listem poleconym za potwierdzeniem odbioru;
- drugi egzemplarz zarchiwizować w teczce akt.

PROCEDURA 8

UDOSTĘPNIENIE DANYCH OSOBOWYCH

Procedura bezpieczeństwa przetwarzania danych osobowych		Data wprowadzenia: 00.00.2018 r.
Numer Procedury : 8	Wniosek o udostępnienie danych osobowych na podstawie przepisów prawa	**Nr wersji procedury : 1.0**
		Ilość stron : 5

.....,dnia .....

Sz.P.....
.....

WNIOSEK O UDOSTĘPNIENIE DANYCH ZE ZBIORU DANYCH OSOBOWYCH

1.Wnioskodawca :

2. Podstawa prawna upoważniająca do pozyskania informacji :

3.Oznaczenie lub nazwa zbioru, z którego mają być udostępnione informacje:

4.Zakres żądanych informacji ze zbioru:

5.Forma przekazania lub udostępnienia informacji:

6.Imię, nazwisko osoby upoważnionej do pobrania informacji lub zapoznania się z ich treścią:

.....
(Imię i nazwisko, podpis)

Opinia Inspektora Ochrony Danych Osobowych :

.....
(Podpis IODO)

Decyzja Administratora danych :

.....
(Podpis Administratora danych)

PROCEDURA WYCOFANIA NOŚNIKÓW

Procedura wycofywania nośników

Niniejsza procedura opisuje zasady wycofywania z użycia nośników informatycznych w Urzędzie Miejskim w Bisztynku

1.1 SŁOWNIK POJĘĆ

SI – System Informatyczny

Pod pojęciem Systemu Informatycznego należy rozumieć:

- Zbiór powiązanych ze sobą elementów, którego funkcją jest przetwarzanie informacji. W skład systemu informatycznego mogą wchodzić takie elementy jak: serwery, sieci, urządzenia sieciowe, urządzenia do przechowywania danych, komputery, systemy operacyjne, bazy danych, strony WWW, aplikacje itp.
- Logicznie bądź funkcjonalnie wydzielony podsystem Systemu Informatycznego, np. system kadrowo-płacowy, system finansowy, system do zarządzania kursami itp.

Rejestr Wycofanych Nośników – rejestr prowadzony przez ASI., w którym odnotowuje się wycofane z eksploatacji nośniki objęte niniejszą procedurą, tj. zawierające informacje poufne (w tym dane osobowe) lub oprogramowanie podlegające licencjonowaniu.

ASI – Administrator Systemu Informatycznego – wyznaczona osoba, odpowiedzialna za zarządzanie danym SI.

1. Pod pojęciem nośnik informatyczny rozumiemy:
   a) Dyski twarde komputerowe i serwerowe wszelkich typów.
   b) Płyty CD, DVD lub podobne.
   c) Taśmy magnetyczne.
   d) Pamięci flash (pendrive).
   e) Dyski przenośne HDD, SSD itp.
2. Procedura wycofywania dotyczy nośników zawierających informacje poufne (w tym dane osobowe) lub oprogramowanie podlegające licencjonowaniu.
3. Wycofaniu podlegają te nośniki, dla których minął okres ich ważności, nie przewiduje się ich dalszego użytkowania lub istnieje prawdopodobieństwo, że dalsze ich użytkowanie może nie spełniać wymogów bezpieczeństwa przechowywania informacji.
4. Poprzez niszczenie danych, zapisanych na nośniku, rozumieć należy takie ich zniszczenie, które uniemożliwia ponowne ich odtworzenie. Zniszczenie danych może wykorzystywać metody zarówno programowe (użycie programów do kasowania danych) jak i sprzętowe (fizyczne zniszczenie nośnika).
5. Dopuszcza się składowanie nośników przeznaczonych do wycofania, stosując następujące zasady:
   a) nośniki muszą być przechowywane w metalowym sejfie, w zamykanym pomieszczeniu, do którego nie mają dostępu osoby trzecie;
   b) nośniki przeznaczone do wycofania muszą być odpowiednio oznaczone, w sposób uniemożliwiający ich przypadkowe, ponowne użycie;
6. Niszczenia nośników dokonuje się w następujący sposób:
   a) Dyski twarde, dyski SSD, pamięci przenośne typu flash (w tym pendrive, dyski przenośnie), taśmy magnetyczne należy przekazać ASI ..... Po ocenie przez ASI stanu technicznego nośnika podejmuje on decyzję o sposobie usunięcia z niego danych:
      i. jeżeli nośnik nie jest uszkodzony, usunięcie danych następuje przy wykorzystaniu specjalnie do tego celu przeznaczonych programów;
      ii. w przypadku gdy nie można usunąć danych z nośnika w sposób programowy, należy go przekazać do fizycznego zniszczenia wyspecjalizowanej firmie, zajmującej się profesjonalnym niszczeniem danych;
   b) Płyty CD, DVD itp. przełamuje się na kilka części, lub niszczy w niszczarce przeznaczonej do utylizacji płyt CD.
7. Po zakończeniu niszczenia, należy sporządzić odpowiedni protokół likwidacyjny nośników. Protokół musi zawierać wyszczególnienie zniszczonych nośników wraz z ich opisem, datą likwidacji, nazwiska osób, które tego dokonały, lub raport z firmy, której nośniki zostały przekazane do zniszczenia.
8. W **Rejestrze Wycofanych Nośników** należy odnotować fakt wycofania nośników, dołączając protokół likwidacyjny.
9. Wzór protokołu likwidacyjnego nośników stanowi Załącznik nr 1.

Miejscowość, data

.....
/pieczęć/

2 PROTOKÓŁ LIKWIDACYJNY NOŚNIKÓW INFORMATYCZNYCH

Komisja w składzie:

1. Przewodniczący komisji: .....
1. Członek komisji: .....
2. Członek komisji: .....

potwierdza zniszczenie następujących nośników informatycznych:

L.p.	Opis nośnika	Data likwidacji	Osoba odpowiedzialna za zniszczenie nośnika
1.	Dysk twardy WD500AAKX, S/N: WCC2EA459291	03.03.2017	Jan Kowalski
2.	Pamięć flash (pendrvie) PQI, 16GB	03.03.2017	Jan Kowalski
3.	Dysk SSD 240 GB GOODRAM, SN:9VMFALN4	09.04.2017	Andrzej Nowak
...			

Podpisy członków komisji:

1. .....

1. .....

2. .....

Instrukcja bezpiecznego przesyłania informacji cyfrowych

Wersja. 1.1

Spis treści

1. Wstęp

Wszystkie poufne informacje (w tym dane osobowe) należy przesyłać w sposób bezpieczny i gwarantujący, że poza odbiorcą wiadomości nikt inny nie będzie w stanie ich odczytać. Dlatego np. przesyłanie takich informacji za pomocą wiadomości e-mail, bez zastosowania dodatkowych mechanizmów bezpieczeństwa, nie jest bezpieczne i należy się tego wystrzegać.

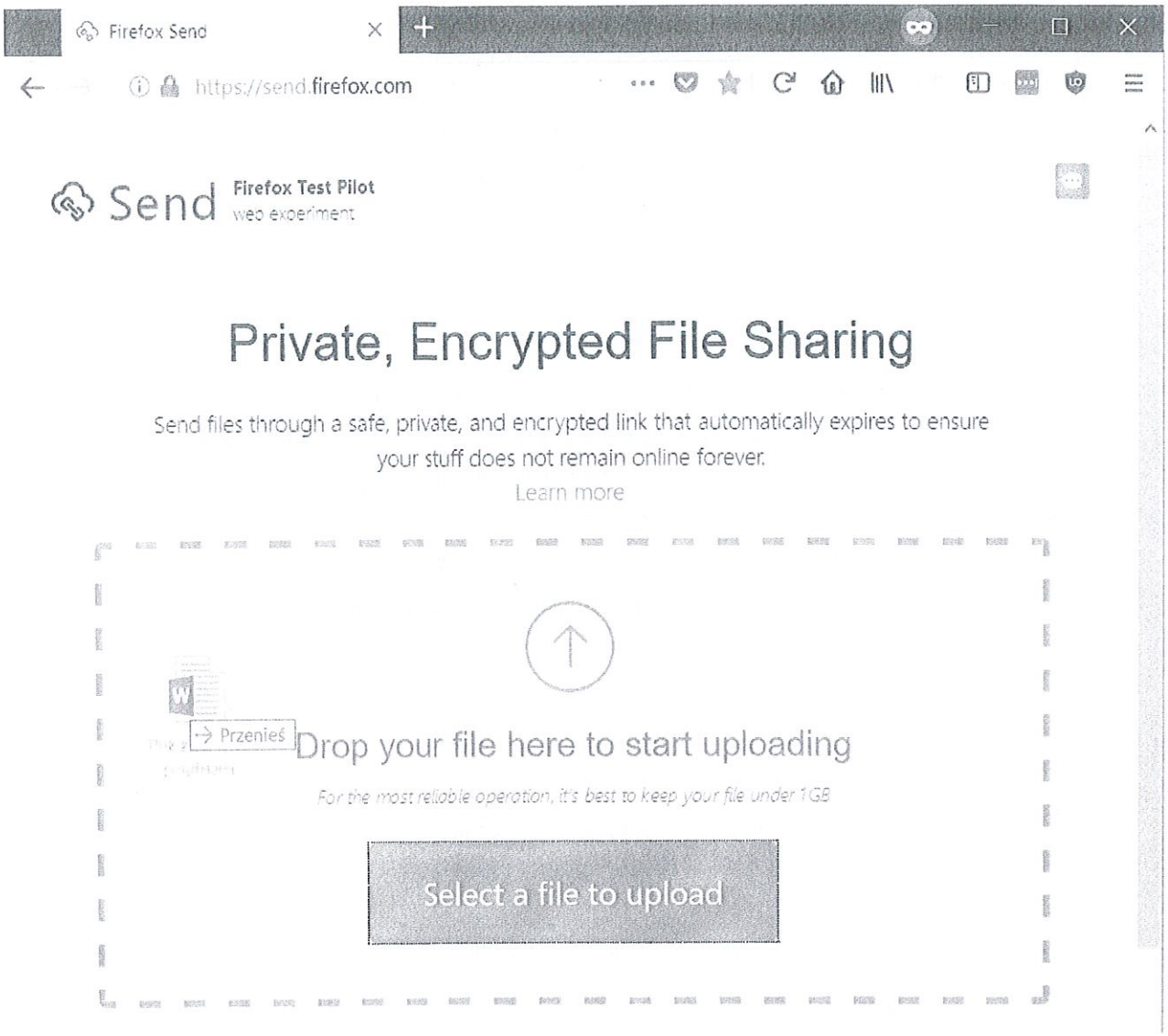
Jednym ze sposobów zabezpieczania informacji przed ich odczytaniem przez osoby nieuprawnione, jest ich szyfrowanie. Jest to proces, w wyniku którego informacja jawna przekształcona zostaje w tzw. kryptogram, czyli tekst zaszyfrowany. Nawet, jeśli ktoś nieuprawniony przechwyci przesyłane dane, nie będzie w stanie ich odczytać. Operacją odwrotną do szyfrowania jest deszyfrowanie. Poniżej przedstawiono dwa, zalecane przez IOD i ASI, sposoby szyfrowania i bezpiecznego przesyłania informacji (plików), do których należy się stosować.

2. Przesyłanie informacji przy pomocy usługi send.firefox.com

Najprostszą i najszybszą metodą przesyłania informacji chronionych (plików) jest skorzystanie z usługi „Send", udostępnionej przez The Mozilla Foundation, do bezpiecznego dzielenia się plikami. Plik, przed przesłaniem na serwer, szyfrowany jest automatycznie na komputerze użytkownika, a następnie generowany jest odnośnik, dzięki któremu można go odszyfrować i pobrać. Co ważne, pliki w usłudze „Send" są automatycznie kasowane z serwera po ich jednorazowym (domyślnie) pobraniu lub po upływie 24h. **Po tym czasie nie będzie można już ich pobrać i trzeba je na nowo tam wysłać.** Zabezpiecza to pliki przed ryzykiem wycieku (nie są przechowywane na serwerze w nieskończoność).

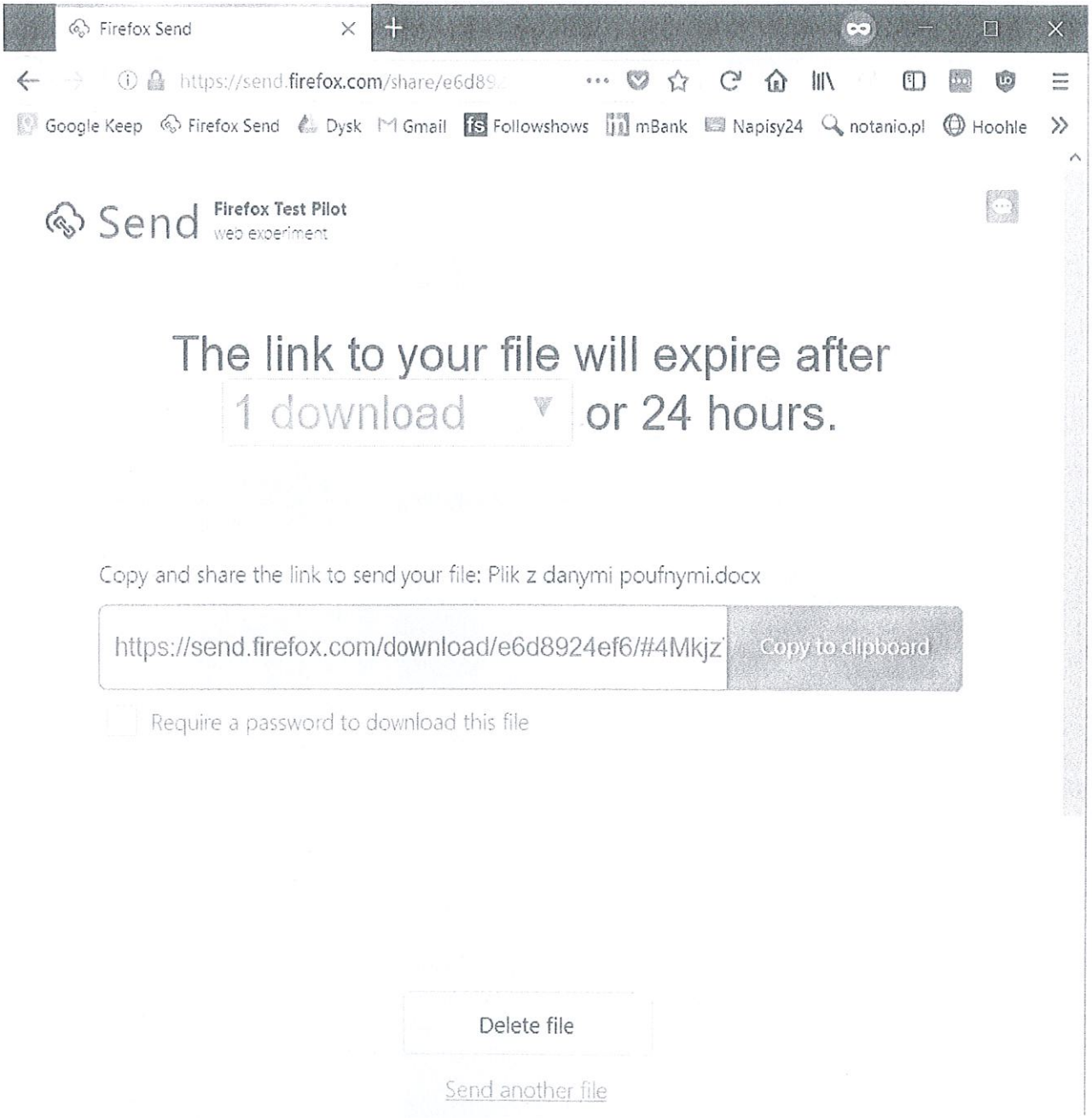
Wejdź na stronę https://send.firefox.com/

Przeciągnij plik, który chcesz przesłać, na zaznaczony niebieską ramką obszar, lub kliknij w przycisk „Select file to upload" po czym wybierz plik do przesłania.

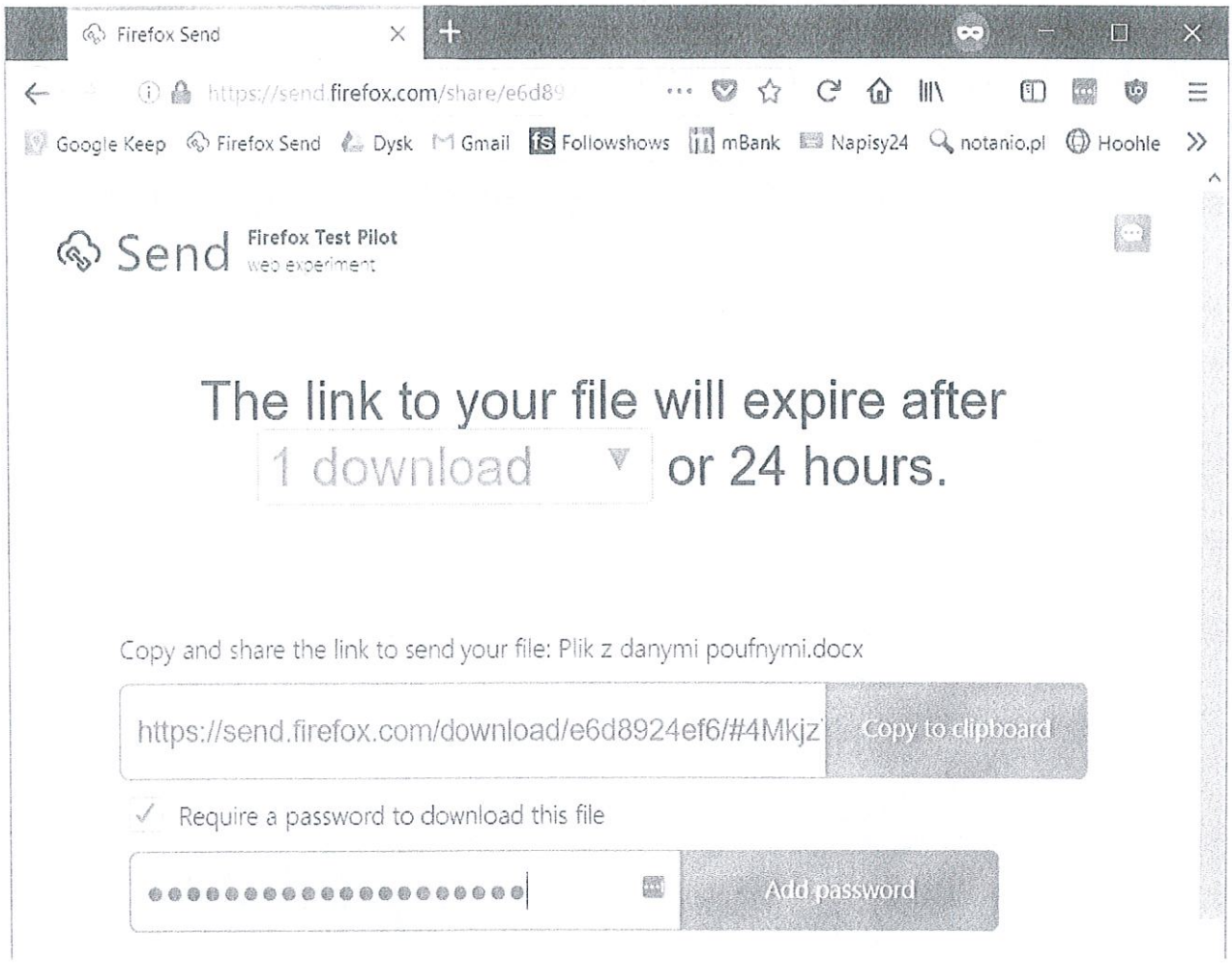


Po przesłaniu pliku możesz ustalić, ile razy będzie można go pobrać, wybierając z rozwijanej listy odpowiednią wartość: 1, 2, 3, 4, 5 lub 20. Po osiągnięciu ustalonego przez Ciebie limitu pobrań, lub po upływie 24h, plik zostanie automatycznie skasowany z serwera, w zależności co nastąpi szybciej.

Skopiuj udostępniony link klikając w przycisk „Copy to clipboard". Teraz możesz już go wysłać np. w wiadomości e-mail (upewniając się ze szczególną starannością, że wpisałeś poprawny adres odbiorcy – skoro przesyłasz dane szczególnie chronione, dochowaj adekwatnej ostrożności) lub przez nasz wewnętrzny komunikator (zalecane), a osoba której go udostępniłeś będzie mogła pobrać wysłany przez Ciebie plik.



W celu dodatkowej ochrony możesz zaznaczyć też opcję „Require a password to download this file" i wpisać hasło, które będzie trzeba podać, aby pobrać plik. Kliknij „Add password" żeby je zatwierdzić. Informację jak wygenerować hasło znajdziesz w punkcie 3.1.

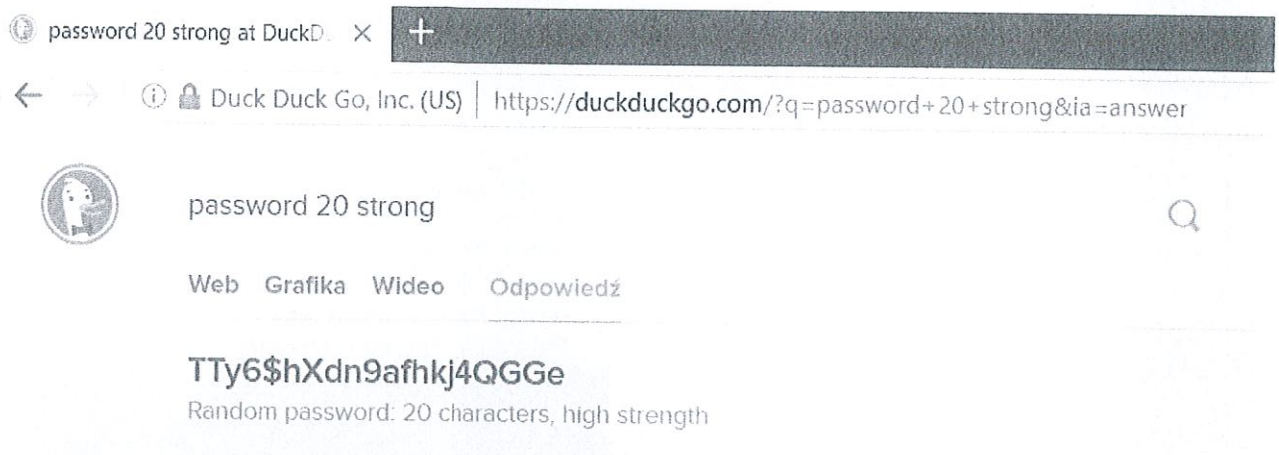


3.1 GENEROWANIE HASEŁ JEDNORAZOWYCH

Do zaszyfrowania i zabezpieczenia pliku będziesz potrzebować minimum 20 znakowego hasła. Jest to wymóg konieczny, gdyż tylko tak długie hasła zapewniają odpowiedni poziom bezpieczeństwa szyfrowanym danym. Hasło możesz wygenerować wchodząc np. na stronę:

https://duckduckgo.com/?q=password+20+strong&ia=answer

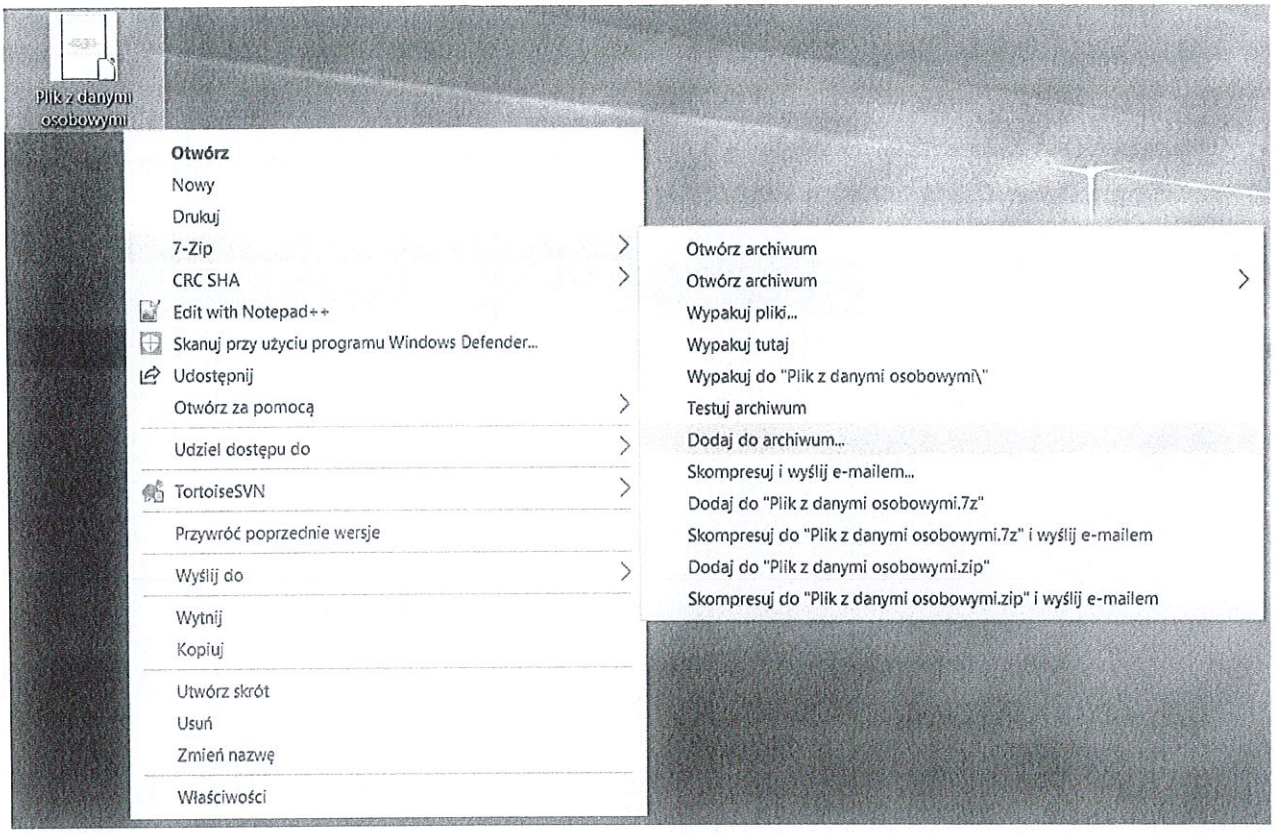
Dla wygody możesz dodać ten adres do zakładek przeglądarki internetowej, której używasz. Jak widać na poniższym zrzucie ekranu, wygenerowane hasło to: TTy6$hXdn9afhkj4QGGe



Pamiętaj, aby nie używać tego samego hasła do szyfrowania różnych danych. Za każdym razem generuj nowe hasło.

3.2 Szyfrowanie danych

Kliknij prawym przyciskiem myszy na pliku (lub katalogu), który chcesz zaszyfrować i wybierz z menu podręcznego: 7-Zip → Dodaj do archiwum...



W nowo otwartym oknie programu zaznacz i uzupełnij poniższe opcje:

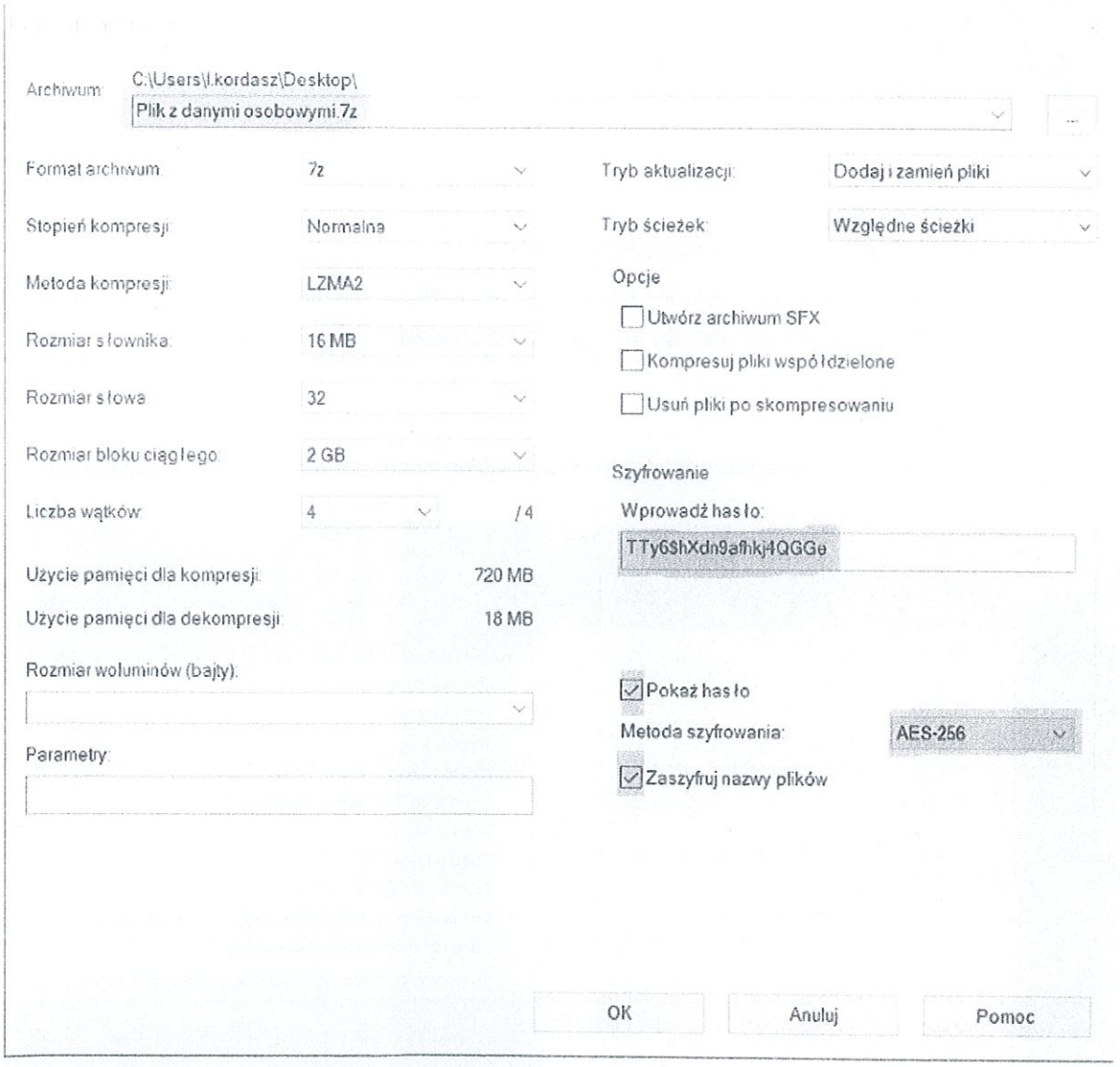
a) Archiwum: – jest to nazwa pliku po zaszyfrowaniu; Domyślnie będzie to nazwa pliku, który chcesz zaszyfrować, z dodanym rozszerzeniem .7z W przypadku, gdy nie chcesz ujawniać nazwy pliku niezaszyfrowanego, możesz tu wpisać cokolwiek innego, np.: tajne.7z

b) Zaznacz opcje: Zaszyfruj nazwy plików oraz Pokaż hasło.

c) Z rozwijanej listy wybierz mechanizm szyfrowania, AES-256.

d) W polu Wprowadź hasło: wklej wcześniej wygenerowane i skopiowane hasło.

e) Kliknij OK żeby zaszyfrować plik.



Po zaszyfrowaniu otrzymasz plik z rozszerzeniem .7z, który możesz już np. wysłać jako załącznik w wiadomości e-mail,

zapisać na płycie CD czy pamięci typu pendrive.

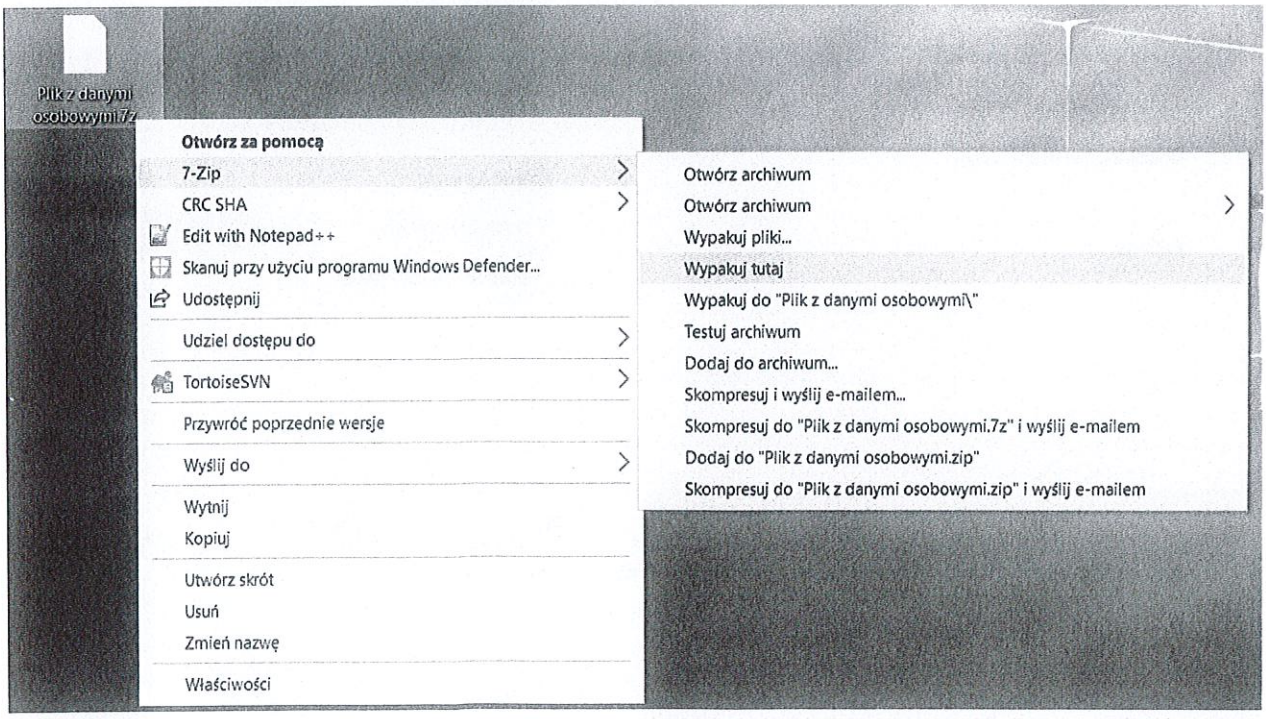
Pamiętaj jednocześnie, aby:

a) nie przesyłać nigdy hasła razem z zaszyfrowanym plikiem;

b) nie przesyłać hasła tym samym kanałem komunikacji – np. jeżeli przesłałeś plik wiadomością e-mail, to hasło do niego przekaż przy pomocy np. naszego wewnętrznego komunikatora lub telefonicznie.

3.3 Deszyfrowanie danych

Żeby odszyfrować plik kliknij na nim Prawym przyciskiem myszy i wybierz z menu podręcznego 7-Zip → Wypakuj tutaj



W nowo otwartym oknie wprowadź hasło do odszyfrowania pliku i kliknij OK.

Upłynęło czasu:	00:00:35	Całkowity rozmiar:	41242
Pozostało czasu:		Szybkość:	
Pliki:	0	Przetworzono:	0
Współczynnik kompresji:			

Wprowadź hasło

Wprowadź hasło:

TTy6$hXdn9afhkj4QGGe

Pokaż hasło

OK Anuluj

Tło Wstrzymaj Anuluj

2018

Instrukcja zarządzania systemem informatycznym przetwarzającym dane osobowe.

Niniejsza instrukcja stanowi podstawę do określenia sposobu zarządzania systemem informatycznym przetwarzającym dane osobowe.

Jarosław Wadowski
Urząd Miejski w Bisztynku
2018-09-01

Historia Zmian

Data	Wersja	Opis zmiany	Autor
01.09.2018	1.1	Aktualizacja	Grzegorz Szajerka

WERSJA 1.1		Pieczęć firmowa:	
Opracował:	**Data:**	**Zatwierdził:**	**Data:**

Niniejsza instrukcja dotyczy każdego zbioru danych osobowych przetwarzanego w Urzędzie Miejskim w Bisztynku zarówno w formie elektronicznej jak i papierowej.

Aktualny wykaz przetwarzanych zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, ich lokalizacją i sposobem dostępu znajduje się w pok. Nr 18.

Burmistrz Bisztynka wprowadza instrukcje i upoważnia administratora systemów informatycznych do nadzorowania wdrożenia sposobu administrowania i zarządzania środkami informatycznymi wspomagającymi procesy przetwarzania informacji stanowiących dane osobowe w rozumieniu RODO oraz ustawy o ochronie danych osobowych wraz z późniejszymi zmianami.

Administrator Systemów Informatycznych we współpracy z Inspektorem Ochrony Danych odpowiada za korygowanie niniejszej instrukcji w przypadku uzasadnionych zmian w przepisach prawnych dotyczących przetwarzania danych osobowych w systemach informatycznych, jak również zmian organizacyjno-funkcjonalnych zachodzących w Urzędzie.

Administrator Systemów Informatycznych we współpracy z Inspektorem Ochrony Danych publikuje zatwierdzony dokument. Wszyscy pracownicy urzędu są zobowiązani zapoznać się z niniejszą instrukcją. Aktualna wersja niniejszej instrukcji jest podstawą szkoleń poświęconych zagadnieniu ochrony danych osobowych w urzędzie, związanych z nadawaniem pracownikom uprawnień do korzystania z systemu informatycznego przetwarzającego dane osobowe.

§ 1. Ta instrukcja to określenie sposobu zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych.

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

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM, SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH W OKREŚLA:

1. Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym.
2. Sposób przydziału haseł dla użytkowników i częstotliwość ich zmiany oraz osoby odpowiedzialne za te czynności.
3. Sposób rejestrowania i wyrejestrowywania użytkowników oraz wskazanie osoby odpowiedzialnej za te czynności.

4. Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym

ury rozpoczęcia i zakończenia pracy.
5. Metoda i częstotliwość tworzenia kopii awaryjnych.
6. Sposób realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4 rozporządzenia.
7. Metoda i częstotliwość sprawdzania obecności wirusów komputerowych oraz metoda ich usuwania.
8. Sposób i czas przechowywania nośników informacji, w tym kopii informatycznych i wydruków.
9. Sposób dokonywania przeglądów i konserwacji systemu i zbioru danych osobowych.
10. Sposób postępowania w zakresie komunikacji w sieci komputerowej.

Przetwarzać dane osobowe w systemach informatycznych może wyłącznie osoba posiadająca pisemne upoważnienie do przetwarzania danych osobowych (wzór upoważnienia stanowi załącznik do niniejszej instrukcji). Wydanie upoważnienia oraz rejestracja użytkownika systemu informatycznego przetwarzającego dane osobowe następuje na wniosek przełożonego lub koordynatora zadania, na rzecz którego będą wykonywane czynności związane z przetwarzaniem danych osobowych. W formie pisemnej składa on wniosek do Administratora bezpieczeństwa informacji odpowiedniego dla zakresu danych o wydanie upoważnienia do przetwarzania danych osobowych. Wniosek ten powinien zawierać:

- Imię i nazwisko pracownika, któremu upoważnienie zostanie nadane,
- Nazwę zbioru danych osobowych oraz nazwę systemu informatycznego, do którego użytkownik będzie miał dostęp,
- Zakres upoważnienia do przetwarzania danych osobowych,
- Datę, z jaką upoważnienie ma być nadane,
- Okres ważności upoważnienia.

Oryginał upoważnienia zostaje przekazywany pracownikowi za potwierdzeniem odbioru, kopia zostaje dołączona do akt osobowych pracownika oraz przekazana do wiadomości przełożonego.

OPIS SZCZEGÓŁOWY:

1. System informatyczny przetwarzający dane osobowe wykorzystuje mechanizm haseł, jako narzędzie umożliwiające bezpieczne uwierzytelnienie. Administrator bezpieczeństwa informacji przydziela hasła tymczasowemu użytkownikowi, który pierwszy raz korzysta z systemu informatycznego.

2. Hasła generuje administrator systemu informatycznego. **Hasło i login użytkownika wraz z dodatkowymi informacjami jest przekazywane w formie papierowej drukowanej w zamkniętej kopercie, którego po przeczytaniu zostaje zniszczone w odpowiednim** urządzeniu niszczącym.

3. System informatyczny przetwarzający dane osobowe jest skonfigurowany w sposób wymuszający bezpieczne zarządzanie identyfikatorami i hasłami użytkowników.

   Ze względu na to:

3.1 Identyfikator składa się z sześciu znaków, z których trzy pierwsze odpowiadają trzem pierwszym literom imienia użytkownika a trzy kolejne odpowiadają trzem pierwszym literom jego nazwiska.

3.2 W identyfikatorze pomija się polskie znaki diakrytyczne.

3.3 W przypadku zbieżności nadawanego identyfikatora z identyfikatorem wcześniej zarejestrowanego użytkownika administrator systemu, za zgodą administratora bezpieczeństwa informacji, nadaje inny identyfikator odstępując od zasady określonej w ust. l.

   a. Hasło tymczasowe przydzielone użytkownikowi musi być zmienione po pierwszym udanym załogowaniu się do systemu informatycznego przetwarzającego dane osobowe.
   b. Hasła są zmieniane przez użytkowników.
   c. System informatyczny wyposażony jest w mechanizmy wymuszające zmianę hasła po upływie 180 dni od dnia ostatniej zmiany hasła.
   d. System informatyczny wyposażony jest w mechanizm pozwalający na wymuszenie, jakości hasła. Hasło składa się, z co najmniej ośmiu znaków, zawiera co najmniej jedną literę wielką, jedną cyfrę i jeden znak specjalny.
   e. Wprowadzone hasło różni się od co najmniej trzech ostatnio stosowanych, przy czym system informatyczny jest wyposażony w mechanizmy pozwalające na wymuszenie wymaganych różnic.
   f. System informatyczny posiada mechanizmy automatycznego generowania przez administratora systemu informatycznego haseł dla użytkownika, który może być włączony w uzasadnionych przypadkach, na wniosek administratora bezpieczeństwa informacji.

3.4 Hasło administratora bezpieczeństwa danych przechowywane jest w zamkniętej kopercie w sejfie ognioodpornym, do którego ma dostęp tylko i wyłącznie Burmistrz Bisztynka i Zastępca Burmistrza Bisztynka.

Dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła.

Identyfikator jest w sposób jednoznaczny przypisany użytkownikowi. Użytkownik odpowiedzialny jest za wszystkie czynności wykonane przy użyciu identyfikatora, którym się posługuje lub posługiwał.

Identyfikator i hasło do systemu informatycznego przetwarzającego dane osobowe są przydzielane użytkownikowi tylko w przypadku, gdy posiada on pisemne upoważnienie do przetwarzania danych osobowych wydane przez administratora danych osobowych lub osobę przez niego uprawnioną. Za przydzielenie i wygenerowanie identyfikatora i hasła użytkownikowi, który pierwszy raz będzie korzystał z systemu informatycznego (czynności te wykonuje na pisemny lub przesłany drogą elektroniczną wniosek administratora bezpieczeństwa informacji).

OPIS SZCZEGÓŁOWY:

1. Rejestracja użytkownika systemu informatycznego przetwarzającego dane osobowe następuje na wniosek przełożonego pracownika po zatwierdzeniu przez administratora bezpieczeństwa informacji i jest wykonywana przez administratora systemu.

Określenie sposobu rejestrowania i wyrejestrowywania użytkowników oraz wskazanie osoby odpowiedzialnej za te czynności

2. Wyrejestrowanie użytkownika z systemu informatycznego może nastąpić na wniosek administratora danych osobowych, przełożonego użytkownika lub koordynatora zadania, na rzecz którego były wykonywane czynności związane z przetwarzaniem danych osobowych. Pisemny wniosek o wyrejestrowanie użytkownika systemu należy złożyć do Administratora bezpieczeństwa informacji. Wyrejestrowanie użytkowania z systemu realizuje administrator odpowiedniego systemu informatycznego na pisemny lub przesłany drogą elektroniczną wniosek administratora bezpieczeństwa informacji. Wyrejestrowanie może mieć charakter czasowy lub trwały.

3. Wyrejestrowanie następuje poprzez:

a) zablokowanie konta użytkownika do czasu ustania przyczyny uzasadniającej blokadę (wyrejestrowanie czasowe),

b) usunięcie danych użytkownika z bazy użytkowników systemu (wyrejestrowanie trwałe).

4. Przyczyną czasowego wyrejestrowania użytkownika z systemu informatycznego jest :

   a) nieobecność w pracy trwająca dłużej niż 21 dni kalendarzowych,

   b) zawieszenie w pełnieniu obowiązków służbowych,

   c) zwolnienie z pełnienia obowiązków służbowych.

5. Przyczyną trwałego wyrejestrowania użytkownika z systemu informatycznego jest rozwiązanie lub wygaśnięcie stosunku pracy użytkownika.

Administrator bezpieczeństwa informacji jest zobowiązany do prowadzenia ewidencji pracowników upoważnionych do przetwarzania danych osobowych w Urzędzie. Zgodnie z art. 39 ust. 1 ustawy taka ewidencja zawiera:

- Imię i nazwisko osoby upoważnionej,
- Datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych,
- Nazwa sytemu informatycznego, którego dotyczy upoważnienie,
- Identyfikator nadany w systemie.

Osoby uprawnione do wykonywania prac administracyjnych w systemie informatycznym posiadają własne konta administracyjne, do których mają przydzielone hasło. Zasady zarządzania hasłami są analogiczne, jak w przypadku haseł użytkowników.

Nazwy i hasła użytkowników posiadających uprawnienia administratorów systemów informatycznych powinny być przechowywane w zamkniętej szafie, do której dostęp jest w pełni kontrolowany, przy czym dostęp do szafy mają wyłącznie uprawnione osoby. Nazwy użytkowników oraz hasła powinny być przechowywane w opieczętowanej i opatrzonej podpisem administratorów systemu kopercie. W przypadku konieczności awaryjnego użycia nazw i haseł tych użytkowników konieczny jest wpis ilustrujący zaistniałą sytuację w ***„Dzienniku haseł"*** znajdującym się w szafie wraz z kopertą, w której znajdują się hasła. Wpis powinien zawierać następujące informacje:

- Imię i nazwisko oraz stanowisko osoby upoważnionej udostępniającej dostęp do szafy, w której znajdują się hasła,
- Imię i nazwisko oraz stanowisko osoby, która pobiera nazwy użytkowników i hasła, - krótki opis sytuacji, która zmusiła do awaryjnego wykorzystania haseł.

O konieczności i okolicznościach awaryjnego użycia nazw i haseł musi niezwłocznie zostać powiadomiony administrator bezpieczeństwa informacji.

Przed rozpoczęciem pracy, w trakcie rozpoczynania pracy z systemem informatycznym oraz w trakcie pracy każdy pracownik obowiązany jest do zwrócenia bacznej uwagi, czy nie wystąpiły symptomy mogące świadczyć o naruszeniu ochrony danych osobowych. Szczegółowy opis takich symptomów oraz sposób postępowania w przypadku ich wykrycia został opisany w dokumencie „Polityka bezpieczeństwa" zaktualizowana w dniu 25.05.2018r.

1. Rozpoczęcie pracy użytkownika w systemie informatycznym obejmuje wprowadzenie identyfikatora i hasła w sposób minimalizujący ryzyko podejrzenia przez osoby nieupoważnione.

2. W przypadku odejścia pracownika od stanowiska komputerowego obowiązany jest on włączyć tzw. wygaszacz ekranu odblokowywany hasłem.

3. Użytkownik powinien powiadomić administratora bezpieczeństwa informacji lub inne osoby przez niego upoważnione zgodnie z „Instrukcją postępowania w sytuacji naruszenia ochrony danych osobowych", jeżeli:

Procedury rozpoczęcia i zakończenia pracy w systemie informatycznym

   a) *Wygląd, zakres danych lub sposób działania aplikacji odbiega od stanu normalnego.*

   b) *Pewne opcje, dostępne użytkownikowi w normalnej sytuacji, przestały być dostępne lub też pewne opcje, niedostępne użytkownikowi w normalnej sytuacji, stały się dostępne.*

4. Zakończenie pracy użytkownika w systemie informatycznym obejmuje wylogowanie się użytkownika z aplikacji oraz wyłączenie komputera.

Metoda i częstotliwość tworzenia kopii awaryjnych w systemie teleinformatycznym

1. Dane osobowe przetwarzane w systemie informatycznym podlegają zabezpieczeniu poprzez tworzenie kopii awaryjnych. Za proces tworzenia kopii awaryjnych odpowiada administrator bezpieczeństwa informacji.

2. W przypadku lokalnego przetwarzania danych osobowych na stacjach roboczych użytkownicy systemu informatycznego zobowiązani są do centralnego przechowywania kopii danych, tak aby możliwe było zabezpieczenie ich dostępności poprzez wykonanie kopii awaryjnych. Niestosowanie się do tego wymagania stanowi wykroczenie przeciwko zasadom ochrony informacji i może skutkować konsekwencjami służbowymi.

3. Kopie awaryjne informacji przechowywanych w systemie informatycznym przetwarzającym dane osobowe tworzone są w następujący sposób:

   a) *Kopia awaryjna aplikacji przetwarzającej dane osobowe wykonywana jest po wprowadzeniu zmian do aplikacji, kopie umieszczane są na nośnikach optycznych i magnetycznych. Kopia wykonywana jest w dwóch egzemplarzach jednym optycznym i jednym magnetycznym. Kopie są przechowywane w dwóch miejscach zabezpieczonych przed niepowołanym dostępem.*

   b) *Kopia awaryjna danych osobowych przetwarzanych przez aplikację wykonywana jest raz w miesiącu. Codziennie wykonywana jest kopia przyrostowa lub różnicowa (w zależności od specyfiki zmian informacji w systemie informatycznym). Rodzaj wykonywanej, codziennie kopii określa administrator bezpieczeństwa informacji.*

   c) *Kopia awaryjna danych konfiguracyjnych systemu informatycznego przetwarzającego dane osobowe, w tym uprawnień użytkowników systemu*

wykonywana jest raz na miesiąc. Codziennie może być wykonywana kopia różnicowa o ile dane konfiguracyjne uległy zmianom.

d) *Do tworzenia kopii awaryjnych wykorzystywane są przeznaczone do tego celu urządzenia wchodzące w skład systemu informatycznego.*

e) *Wszelkie kopie awaryjne mogą być sporządzane automatycznie lub wywoływane w sposób ręczny. Za ustalanie grafiku sporządzania kopii zapasowych jest odpowiedzialny administrator danych osobowych.*

f) *Administrator danych osobowych dokonuje zakupów nośników kopii awaryjnych.*

4. Administrator bezpieczeństwa informacji wykonuje testy odtworzeniowe kopii awaryjnych. W tym celu zabezpiecza on platformę sprzętowo-programową pozwalającą na ich przeprowadzenie. Testy przeprowadzane są raz na pół roku i obejmują sprawdzenie możliwości odtworzenia przechowywanych danych osobowych oraz danych konfiguracyjnych. Administrator bezpieczeństwa informacji sporządza protokół potwierdzający wykonanie testów, uwzględniający:

   a) *Imię i nazwisko osoby przeprowadzającej test.*
   b) *Powodzenie lub niepowodzenie odtworzenia danych z kopii awaryjnej.*
   c) *Czas potrzebny na odtworzenie danych.*
   d) *Problemy, które pojawiły się w czasie wykonywania testu.*

5. Negatywne wyniki testu lub zaistnienie problemów w trakcie odtwarzania danych może stać się podstawą do zmiany sposobu tworzenia kopii awaryjnych w urzędzie lub zmiany technologii wykorzystywanej do tworzenia kopii [urządzenia, nośniki]. W przypadku wystąpienia negatywnych wyników lub problemów administrator bezpieczeństwa informacji przeprowadza analizy przyczyn i podejmuje działania w celu zmniejszenia ryzyka utraty danych poprzez brak możliwości odtworzenia kopii.

6. Nośniki kopii awaryjnych, które zostały wycofane z użycia, **podlegają zniszczeniu po usunięciu danych osobowych, w odpowiednim urządzeniu niszczącym** przez administratora bezpieczeństwa informacji.

7. Z
a
s
a
c
y

Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, o którym mowa w pkt III załącznika do rozporządzenia.

przechowywania i inwentaryzacji kopii awaryjnych, jak również podstawowe warunki odtwarzania systemu informatycznego po awarii zostały opisane w wytycznych „Tworzenie kopii awaryjnych".

W związku z tym, że system informatyczny narażony jest na działanie oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do tego systemu konieczne jest podjęcie odpowiednich środków ochronnych.

Można wyróżnić następujące rodzaje występujących tu zagrożeń:

- nieuprawniony dostęp bezpośrednio do bazy danych,
- uszkodzenie kodu aplikacji umożliwiającej dostęp do bazy danych w taki sposób, że przetwarzane dane osobowe ulegną zafałszowaniu lub zniszczeniu,
- przechwycenie danych podczas transmisji w przypadku rozproszonego przetwarzania danych z wykorzystaniem ogólnodostępnej sieci Internet,
- przechwycenie danych z aplikacji umożliwiającej dostęp do bazy danych na stacji roboczej wykorzystywanej do przetwarzania danych osobowych przez wyspecjalizowany program szpiegowski i nielegalne przesłanie tych danych poza miejsce przetwarzania danych,
- uszkodzenie lub zafałszowanie danych osobowych przez wirus komputerowy zakłócający pracę aplikacji umożliwiającej dostęp do bazy danych na stacji roboczej wykorzystywanej do przetwarzania danych osobowych.

W celu przeciwdziałania wymienionym zagrożeniom system informatyczny musi posiadać

następujące zabezpieczenia:

- fizyczne odseparowanie serwera bazy danych od sieci zewnętrznej,
- autoryzacja użytkowników przy zachowaniu odpowiedniego poziomu komplikacji haseł dostępu,
- stosowanie rygorystycznego systemu autoryzacji dostępu do wszystkich serwerów, na których znajdują się elementy aplikacji umożliwiających przetwarzanie danych osobowych,
- stosowaniu aplikacji w postaci skompilowanej i nie umieszczenie kodu źródłowego aplikacji na powszechnie dostępnych serwerach,
- stosowanie szyfrowanej transmisji danych przy zastosowaniu odpowiedniej długości klucza szyfrującego,
- stosowanie odpowiedniej ochrony antywirusowej na stacjach roboczych wykorzystywanych do przetwarzania danych osobowych.

Potencjalnymi źródłami przedostawania się programów szpiegowskich oraz wirusów komputerowych na stacje robocze są:

- załączniki do poczty elektronicznej,
- przeglądane strony internetowe,
- pliki i aplikacje pochodzące z nośników wymiennych uruchamiane i odczytywane na stacji roboczej..

W celu zapewnienia ochrony antywirusowej administrator systemu informatycznego przetwarzającego dane osobowe, lub osoba specjalnie do tego celu wyznaczona, jest odpowiedzialny za zarządzanie systemem wykrywającym i usuwającym wirusy. System antywirusowy powinien być skonfigurowany w następujący sposób:

- rezydentny monitor antywirusowy (uruchomiony w pamięci operacyjnej stacji roboczej) powinien być stale włączony,
- antywirusowy skaner ruchu internetowego powinien być stale włączony,
- monitor zapewniający ochronę przed wirusami makr w dokumentach MS Office powinien być stale włączony,
- skaner poczty elektronicznej powinien być stale włączony.

Systemy antywirusowe zainstalowane na stacjach roboczych powinny być skonfigurowane w sposób następujący:

- zablokowanie możliwości ingerencji użytkownika w ustawienia oprogramowania antywirusowego,
- możliwość centralnego uaktualnienia wzorców wirusów.

System antywirusowy powinien być aktualizowany na podstawie materiałów publikowanych przez producenta oprogramowania.

Użytkownicy systemu informatycznego zobowiązani są do następujących działań:

- skanowania zawartości dysków stacji roboczej pracującej w systemie informatycznym pod względem potencjalnie niebezpiecznych kodów - przynajmniej 2 razy w tygodniu,
- skanowania zawartości nośników wymiennych odczytywanych na stacji roboczej pracującej w systemie informatycznym pod względem potencjalnie niebezpiecznych kodów - przy każdym odczycie,
- skanowanie informacji przesyłanych do systemu informatycznego pod kątem pojawienia się niebezpiecznych kodów - na bieżąco.

W przypadku wystąpienia infekcji i braku możliwości automatycznego usunięcia wirusów przez system antywirusowy administrator systemu informatycznego lub inny wyznaczony pracownik powinien podjąć działania zmierzające do usunięcia zagrożenia. W szczególności działania te mogą obejmować:

- usunięcie zainfekowanych plików, o ile jest to akceptowalne ze względu na prawidłowe funkcjonowanie systemu informatycznego,
- odtworzenie plików z kopii zapasowych po uprzednim sprawdzeniu, czy dane zapisane na kopiach nie są zainfekowane,

- samodzielną ingerencję w zawartość pliku - w zależności od posiadanych kwalifikacji lub skonsultowanie się z zewnętrznymi ekspertami.

System informatyczny przetwarzający dane osobowe powinien posiadać mechanizmy pozwalające na zabezpieczenie ich przed utratą lub wystąpieniem zafałszowania w wyniku awarii zasilania lub zakłóceń w sieci zasilającej. W związku z tym system informatyczny powinien być wyposażony, w co najmniej:

- filtry zabezpieczające stacje robocze przed skutkami przepięcia,
- zasilacze awaryjne serwerów baz danych, serwerów aplikacji oraz urządzeń pamięci masowej pozwalające na bezpieczne zamkniecie aplikacji przetwarzających dane osobowe w sposób umożliwiający poprawne zapisanie przetwarzanych danych.

Metoda i częstotliwość sprawdzania obecności wirusów komputerowych oraz metoda ich usuwania

1. Administrator bezpieczeństwa informacji zapewnia ochronę antywirusową. Zarządza systemem wykrywającym i usuwającym wirusy i inne niebezpieczne kody. System antywirusowy jest skonfigurowany w następujący sposób:

   a) *Skanowanie dysków zawierających potencjalnie niebezpieczne kody po włączeniu komputera w tle działania aplikacji.*
   b) *Skanowanie informacji przesyłanych do systemu informatycznego pod kątem pojawienia się niebezpiecznych kodów - na bieżąco.*

2. Systemy antywirusowe zainstalowane na stacjach roboczych są skonfigurowane w celu:

   a) *Zablokowania możliwości ingerencji użytkownika w ustawienia oprogramowania antywirusowego.*
   b) *Możliwości centralnego uaktualniania wzorców wirusów.*
   c) *Możliwości centralnego zbierania informacji o wynikach pracy oprogramowania.*
   d) *Możliwość centralnej konfiguracji oprogramowania.*

3. Administrator bezpieczeństwa informacji aktualizuje wzorce wirusów. System antywirusowy jest aktualizowany na podstawie materiałów publikowanych przez producenta oprogramowania.

4. W przypadku wystąpienia infekcji i braku możliwości automatycznego usunięcia wirusów przez system antywirusowy administrator bezpieczeństwa informacji podejmuje działania zmierzające do usunięcia zagrożenia. W szczególności działania te mogą obejmować:

   a) *Usunięcie zainfekowanych plików, o ile jest to akceptowalne ze względu na prawidłowe funkcjonowanie systemu informatycznego*
   b) *Odtworzenie plików z kopii awaryjnych po uprzednim sprawdzeniu, czy dane zapisane na kopiach nie są zainfekowane*
   c) *Samodzielną ingerencję w zawartość pliku - w zależności od posiadanych narzędzi i oprogramowania.*

Sposób i czas przechowywania nośników informacji, w tym kopii informatycznych i wydruków

1. Nośniki danych osobowych zarówno w postaci elektronicznej, jak i papierowej powinny być zabezpieczone przed dostępem osób nieupoważnionych, nie-autoryzowaną modyfikacją i zniszczeniem.

2. Dane osobowe mogą być zapisywane na nośnikach przenośnych w przypadku tworzenia kopii awaryjnych lub gdy istnieje konieczność przeniesienia tych danych w postaci elektronicznej.

3. Wydruki z danymi osobowymi oznaczane są w sposób zgodny z oznaczeniami używanymi w schemacie organizacyjnym urzędu oraz oznaczeniami używanymi przez poszczególne referaty.

4. Administrator bezpieczeństwa informacji prowadzi ewidencję wydruków danych osobowych ze szczególnym uwzględnieniem faktu przekazania wydruku poza urząd. Ewidencja zawiera numer ewidencyjny wydruku oraz nazwisko i imię osoby wydającej i odbierającej wydruk.

5. Nośniki danych osobowych oraz wydruki przechowuje się w zamkniętych szafkach wewnątrz obszaru przeznaczonego do przetwarzania danych osobowych i nie powinny być bez uzasadnionej potrzeby wynoszone poza ten obszar.

6. Przekazywanie nośników danych osobowych i wydruków poza obręb urzędu może odbywać się za wiedzą i zgodą administratora bezpieczeństwa informacji.

7. W przypadku, gdy nośnik danych osobowych nie jest dłużej potrzebny, należy przeprowadzić zniszczenie nośnika albo usunięcie danych z nośnika zgodnie ze szczegółowymi wytycznymi. Jeżeli wydruk danych osobowych nie jest dłużej potrzebny, należy przeprowadzić zniszczenie wydruku przy użyciu odpowiedniej niszczarki dokumentów.

8. W zależności od rodzaju przechowywanych informacji administrator bezpieczeństwa informacji określa wymagany czas przechowywania nośników danych osobowych, wydruków, jak również danych osobowych w systemie informatycznym.

Sposób dokonywania przeglądów i konserwacji systemu i zbioru danych osobowych

1. Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe muszą uwzględniać zachowanie wymaganego poziomu zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych. Prace serwisowe mogą być wykonywane wyłącznie w siedzibie urzędu. W przypadku uszkodzenia zestawu komputerowego nośnik informacji danych, na których są przechowywane dane osobowe zostaje zabezpieczony przez administratora danych osobowych przed dostępem osób nieuprawnionych.

2. Pracownicy winni zgłaszać wszelkie niesprawności systemu informatycznego zgodnie z „Instrukcją postępowania w sytuacji naruszenia ochrony danych osobowych".

3. W przypadku konieczności przeprowadzenia prac serwisowych poza siedzibą przedsiębiorstwa dane z naprawianego urządzenia muszą zostać w sposób trwały usunięte. Od poniższego wymagania możliwe jest odstępstwo, jeżeli urządzenie, podczas przechowywania poza siedzibą przedsiębiorstwa, będzie pod stałym nadzorem osoby upoważnionej do dostępu do danych na nim przetwarzanych, wskazanej przez administratora bezpieczeństwa informacji.

4. Administrator bezpieczeństwa informacji wykonuje okresowy przegląd zbioru danych osobowych oraz usuwa dane, których przechowywanie jest dłużej nieuzasadnione.

Sposób postępowania w zakresie komunikacji w sieci komputerowej

1. Dane osobowe są przesyłane w sieci informatycznej przystosowanej do obsługi systemu informatycznego przetwarzającego te dane. Sieć ta jest odseparowana od pozostałej infrastruktury teleinformatycznej za pomocą zapory ogniowej [firewalla] w sposób uniemożliwiający nieautoryzowane wysyłanie danych osobowych poza jej obręb.

2. Administrator bezpieczeństwa informacji jest odpowiedzialny za konfigurację zapory [firewalla].

3. W przypadkach, gdy nie jest konieczna wymiana informacji pomiędzy siecią a pozostałymi sieciami informatycznymi, zostają one fizycznie odseparowane. Administrator bezpieczeństwa informacji wskazuje rodzaje danych i sposoby transmisji danych, które wymagają szyfrowania i/lub stosowania podpisu elektronicznego.

4. W wypadku przesyłania danych osobowych poza sieć przystosowaną do transferu danych osobowych zostają zastosowane szczególne środki w zakresie bezpieczeństwa. Obejmują one:

    a) *Zatwierdzenie przez administratora bezpieczeństwa informacji celu wysłania danych osobowych.*
    b) *Zastosowanie mechanizmów szyfrowania danych osobowych.*
    c) *Zastosowanie mechanizmów podpisu elektronicznego zabezpieczającego transmisje danych osobowych oraz rejestrację transmisji wysyłania danych osobowych.*
    d) *Umożliwienie wysyłania danych osobowych tylko z wykorzystaniem określonej aplikacji i tylko przez określonych użytkowników - odpowiednia konfiguracja aplikacji i zapory ogniowej.*

5. W przypadku stosowania mechanizmów kryptograficznych administrator bezpieczeństwa informacji określa minimalne wymagania w zakresie materiału kryptograficznego stosowanego do ochrony danych osobowych. Jeżeli nie określi on innych wymagań, stosuje się:

    a) *Przy szyfrowaniu symetrycznym stosowanie minimum algorytmu typu AES z kluczem 256 bitów,*
    b) *Przy szyfrowaniu asymetrycznym stosowanie minimum algorytm RSA z kluczem 1024 bity.*

przez niego upoważnione zgodnie z zasadami opisanymi w „Instrukcji postępowania w przypadku naruszenia ochrony danych osobowych w rozdziale 3 Polityki Bezpieczeństwa".

6. Administrator bezpieczeństwa informacji tworzy konfigurację mechanizmów kryptograficznych w sposób:

   a) *Zapewniający wykorzystanie obowiązujących w urzędzie wymagań w zakresie kryptograficznej ochrony danych osobowych.*
   b) *Umożliwiający, w miarę technicznych możliwości, automatyczne szyfrowanie danych osobowych wysyłanych poza wydzieloną sieć informatyczną.*
   c) *Informujący użytkownika o dołączeniu do wysyłanych danych osobowych elektronicznego podpisu i wymagający przed wysłaniem informacji potwierdzenia podpisywanej treści.*

7. W wypadku, gdy podmiot zewnętrzny, z którym wymieniane są dane osobowe, korzysta z innych mechanizmów kryptograficznych niż stosowane w urzędzie, administrator bezpieczeństwa informacji może dopuścić zastosowanie tych mechanizmów lub mechanizmów z nimi zgodnych pod warunkiem zapewnienia zbliżonej do obowiązującej ochrony przesyłanych danych osobowych. W tym celu administrator bezpieczeństwa informacji może przeprowadzić analizę poziomu bezpieczeństwa mechanizmu kryptograficznego oraz zgodności tego mechanizmu z komponentami systemu informatycznego.

8. Administrator bezpieczeństwa informacji jest odpowiedzialny za:

   a) *Realizację procesów związanych z zarządzaniem aplikacjami kryptograficznymi oraz generowanie kluczy dostępowych do tych aplikacji.*
   b) *Wygenerowanie, w ramach posiadanej infrastruktury informatycznej klucza publicznego, kluczy publicznych użytkowników.*
   c) *Wycofywanie kluczy kryptograficznych, jeżeli istnieje uzasadnione podejrzenie, iż klucze te znalazły się w rękach osób niepowołanych.*
   d) *Sporządzenie list wycofanych z użycia materiałów kryptograficznych, w szczególności w ramach infrastruktury klucza publicznego przy użyciu list CRL.*

9. W urzędzie klucze kryptograficzne wykorzystywane w kryptografii asymetrycznej są użytkowane przez jeden rok i po tym okresie podlegają wycofaniu i wymianie. Administrator bezpieczeństwa informacji może określić inny, (ale nie dłuższy) okres ważności kluczy w kryptografii asymetrycznej, jeśli zabezpieczenie pewnego rodzaju danych osobowych będzie wymagało skrócenia czasu życia kluczy.

10. Klucze kryptograficzne w kryptografii symetrycznej mają charakter sesyjny - generowane są na potrzeby określonej sesji wymiany danych i czas ich życia jest równy czasowi trwania sesji.

11. W przypadku wystąpienia uzasadnionego podejrzenia przechwycenia kluczy kryptograficznych lub dostania się ich w niepowołane ręce pracownik zobowiązany jest poinformować o tym fakcie administratora bezpieczeństwa informacji lub osoby