**ZARZĄDZENIE Nr ON.120.32.2018**
**STAROSTY SIERPECKIEGO**
**z dnia 24 maja 2018 roku**

**w sprawie dokumentacji przetwarzania danych osobowych w Starostwie Powiatowym w Sierpcu**

Na podstawie art. 35 ust. 1 i ust. 2 ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym (Dz. U. z 2018 r. poz. 995) oraz 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 (Dz. Urz. UE L 2016, Nr 119) i § 34 ust. 1 pkt 1 Regulaminu Organizacyjnego Starostwa Powiatowego w Sierpcu stanowiącego załącznik do Załącznik do Uchwały Nr 400.81.2016 Zarządu Powiatu w Sierpcu z dnia 26 października 2016 r. zmienionego Nr 674.125.2018 Zarządu Powiatu w Sierpcu z dnia 18 stycznia 2018 r. zarządza się, co następuje:

**§ 1.** Wprowadzam **Politykę Bezpieczeństwa Przetwarzania Danych Osobowych w Starostwie Powiatowym w Sierpcu** stanowiącą Załącznik Nr 1 do niniejszego zarządzenia.

**§ 2.** 1. Wprowadzam **Instrukcję w sprawie sposobu zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji**, stanowiącą Załącznik Nr 2 do niniejszego Zarządzenia.

2. Instrukcję, o której mowa w ust. 1 stosuje się odpowiednio również do zarządzania zbiorami danych osobowych przetwarzanych w Starostwie Powiatowym w Sierpcu w formie papierowej.

**§ 3.** 1. Dla prawidłowego zabezpieczenia przetwarzania danych osobowych w systemach teleinformatycznych Starostwa Powiatowego w Sierpcu – na **Administratora Systemów Informatycznych Starostwa** powołuję **Pana Michała Chiczewskiego – starszego informatyka w Wydziale Organizacji i Nadzoru.**

2. W przypadku nieobecności Pana Michała Chiczewskiego - starszego informatyka w Wydziale Organizacji i Nadzoru, do wykonywania obowiązków Administratora Systemów Informatycznych Starostwa wyznaczam **Pana Łukasza Szpakowskiego – referenta w Wydziale Organizacji i Nadzoru.**

3. Osoba, o której mowa w ust. 2 składa Administratorowi Systemów Informatycznych relację z podejmowanych działań w czasie jego zastępstwa.

**§ 4.** Do obsługi systemów informatycznych i urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych, a także do zbiorów danych papierowych mogą być dopuszczone wyłącznie osoby upoważnione przez Administratora danych, których ewidencję w systemie elektronicznym prowadzi wyznaczony pracownik Wydziału Organizacji i Nadzoru.

**§ 5. 1.** Zobowiązuję wszystkich pracowników Starostwa Powiatowego w Sierpcu mających dostęp do danych osobowych zawartych w zbiorach Starostwa do:

1) zapoznania się z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. UE L 2016, Nr 119) oraz wydanymi na jego podstawie przepisami prawa polskiego oraz do ścisłego ich przestrzegania;
2) zapoznania się z treścią niniejszego zarządzenia oraz ścisłego jego przestrzegania;
3) złożenia oświadczenia o zapoznaniu się z treścią wyżej wymienionych przepisów prawa oraz o zachowaniu w tajemnicy treści danych osobowych, z którymi w trakcie pracy się zapoznali - według wzoru stanowiącego Załącznik Nr 3 do niniejszego Zarządzenia.

2. Zobowiązuję pracownika ds. kadr i płac do przechowywania oświadczeń, o których mowa w ust. 1 pkt 3 w aktach osobowych pracowników.

**§ 6.** Traci moc Zarządzenie Nr ON.120.28.2015 Starosty Sierpeckiego z dnia 29 czerwca 2015 r. w sprawie powołania Administratora Bezpieczeństwa Informacji i jego Zastępcy oraz zatwierdzenia dokumentacji przetwarzania danych osobowych w Starostwie Powiatowym w Sierpcu zmienione Zarządzeniem Nr ON.120.38.2015 Starosty Sierpeckiego z dnia 4 sierpnia 2015 r. i Zarządzeniem Nr ON.120.29.2016 Starosty Sierpeckiego z dnia 121 czerwca 2016 r. roku oraz Zarządzeniem Nr ON.120.25.2017 Starosty Sierpeckiego z dnia 30 maja 2017r.

**§ 7.** Wykonanie zarządzenia powierzam Naczelnikowi Wydziału Organizacji i Nadzoru.

**§ 8.** Zarządzenie wchodzi w życie z dniem 25 maja 2018 r.

STAROSTA
*Jan Laskowski*

**Załącznik Nr 1**
**do ZARZĄDZENIA Nr ON.120.32.2018**
**STAROSTY SIERPECKIEGO**
**z dnia 24 maja 2018 r.**

# POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH W STAROSTWIE POWIATOWYM W SIERPCU

## Rozdział 1.
## Postanowienia ogólne.

**§ 1.** 1. Celem Polityki Bezpieczeństwa danych osobowych, zwanej dalej Polityką Bezpieczeństwa, jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych w zakresie ochrony danych osobowych, sposobu przetwarzania w Starostwie Powiatowym w Sierpcu informacji zawierającej dane osobowe.

2. Niniejszy dokument jest zgodny z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. UE L 2016, Nr 119) zwanym dalej RODO.

3. Utrzymanie bezpieczeństwa przetwarzanych przez Starostwo Powiatowe w Sierpcu informacji rozumiane jest jako zapewnienie ich poufności, integralności i dostępności na odpowiednim poziomie. Miarą bezpieczeństwa jest wielkość ryzyka związanego z zasobem stanowiącym przedmiot niniejszej Polityki. Poniżej opisane jest rozumienie wyżej wymienionych pojęć w odniesieniu do informacji i aplikacji:

1) **poufność informacji** - rozumiana jako zapewnienie, że tylko uprawnieni pracownicy mają dostęp do informacji;
2) **integralność informacji** - rozumiana jako zapewnienie dokładności i kompletności informacji oraz metod jej przetwarzania;
3) **dostępność informacji** - rozumiane jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne;
4) **zarządzanie ryzykiem** - rozumiane jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych.

4. Dodatkowo zarządzanie bezpieczeństwem informacji wiąże się z zapewnieniem:

1) **niezaprzeczalności odbioru** - rozumianej jako zdolność systemu do udowodnienia, że adresat informacji otrzymał ją w określonym miejscu i czasie;
2) **niezaprzeczalności nadania** - rozumianej jako zdolność systemu do udowodnienia, że nadawca informacji faktycznie ją nadał lub wprowadził do systemu w określonym miejscu i czasie;
3) **rozliczalności działań** - rozumianej, jako zapewnienie, że wszystkie działania istotne dla przetwarzania informacji zostały zarejestrowane w systemie i możliwym jest zidentyfikowanie użytkownika, który działania dokonał.

5. Informacje zawierające dane osobowe są przetwarzane i składowane zarówno w postaci tradycyjnej (dokumentacja papierowa), jak i elektronicznej.

6. Zasady określone w niniejszej Polityce mają zastosowanie do całego systemu informacyjnego Starostwa Powiatowego w Sierpcu, w szczególności do:

1) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są informacje podlegające ochronie;
2) informacji będących własnością Starostwa Powiatowego w Sierpcu lub klientów Starostwa Powiatowego w Sierpcu, o ile zostały przekazane na podstawie umów;
3) wszystkich lokalizacji budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie;
4) wszystkich pracowników w rozumieniu przepisów Kodeksu Pracy, konsultantów, stażystów, praktykantów i innych osób mających dostęp do informacji podlegających ochronie, zwanych dalej pracownikami.

7. Polityka bezpieczeństwa określa tryb postępowania w przypadku, gdy:

1) stwierdzono naruszenie zabezpieczenia systemu informatycznego;
2) 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.

8. 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 Starostwa Powiatowego w Sierpcu.

9. Niezależnie od niniejszych zasad opisanych w Polityce bezpieczeństwa w zakresie bezpieczeństwa mają zastosowanie wszelkie wewnętrzne regulaminy lub instrukcje dotyczące bezpieczeństwa ludzi i zasobów informatycznych oraz indywidualne zakresy zadań pracowników zatrudnionych przy przetwarzaniu danych osobowych w określonym systemie, o ile nie są sprzeczne z zapisami niniejszej Polityki.

## Rozdział 2.
## Opis zdarzeń naruszających ochronę danych osobowych.

**§ 2.** 1. Zagrożenia dla ochrony danych osobowych przetwarzanych w Starostwie Powiatowym w Sierpcu dzielimy na:

1) **zagrożenia losowe zewnętrzne** (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;
2) **zagrożenia losowe wewnętrzne** (np. niezamierzone pomyłki operatorów, administratora systemu, awarie sprzętowe, błędy oprogramowania), może dojść do zniszczenia danych, może zostać zakłócona ciągłość systemu, może nastąpić naruszenie poufności danych;
3) **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 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. Do przypadków zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe należą głównie:

1) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu jak np.: pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej, wybuch gazu itp.;
2) niewłaściwe parametr środowiska np. nadmierna wilgotność, wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych;
3) 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 fakt pozostawienia serwisantów bez nadzoru;
4) pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu;
5) jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie;
6) nastąpiło naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie;

7) stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji);
8) nastąpiła niedopuszczalna manipulacja danymi osobowymi systemie;
9) ujawniono osobom nieupoważnionym dane osobowe lub objęte tajemnicą procedury ochrony przetwarzania albo inne strzeżone elementy systemu zabezpieczeń;
10) 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.;
11) ujawniono istnienie nieautoryzowanych kont dostępu do danych lub tzw. „bocznej furtki" itp.;
12) podmieniono lub zniszczono nośniki z danymi osobowymi bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowano lub skopiowano dane osobowe;
13) 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 osobowych 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 3.
## Procedura postępowania w przypadku stwierdzenia naruszenia ochrony danych osobowych.

**§ 3.** 1. Każdy pracownik Starostwa Powiatowe w Sierpcu, który powezmie wiadomość w zakresie naruszenia bezpieczeństwa danych przez osobę przetwarzającą dane osobowe bądź posiada informacje mogącą mieć wpływ na bezpieczeństwo danych osobowych jest zobowiązany fakt ten niezwłocznie zgłosić Administratorowi Systemu lub Naczelnikowi Wydziału Organizacji i Nadzoru.

2. W razie niemożności zawiadomienia osób, o których mowa w ust. 1 pracownik powinien powiadomić bezpośredniego przełożonego.

3. Do czasu przybycia na miejsce naruszenia ochrony danych osobowych Administratora Systemu lub Naczelnika Wydziału Organizacji i Nadzoru, należy:
1) 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;

2) rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia;
3) zaniechać – o ile to możliwe – dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę;
4) podjąć inne działania przewidziane i określone w instrukcjach technicznych i technologicznych stosownie do objawów i komunikatów towarzyszących naruszeniu;
5) podjąć stosowne działania, jeśli zaistniały przypadek jest określony w dokumentacji systemu operacyjnego, dokumentacji bazy danych lub aplikacji użytkowej;
6) zastosować się do innych instrukcji i regulaminów, jeżeli odnoszą się one do zaistniałego przypadku;
7) udokumentować wstępnie zaistniałe naruszenie;
8) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Administratora Systemu lub Naczelnika Wydziału Organizacji i Nadzoru.

4. Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych, Administrator Systemu lub Naczelnik Wydziału Organizacji i Nadzoru:

1) zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy urzędu;
2) może żądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem;
3) rozważa celowość i potrzebę powiadomienia o zaistniałym naruszeniu Administratora danych;
4) nawiązuje bezpośredni kontakt, jeżeli zachodzi taka potrzeba, ze specjalistami spoza urzędu.

5. Administrator Systemu lub Naczelnik Wydziału Organizacji i Nadzoru dokumentuje zaistniały przypadek naruszenia oraz sporządza raport, który powinien zawierać w szczególności:

1) wskazanie osoby powiadamiającej o naruszeniu oraz innych osób zaangażowanych lub odpytanych w związku z naruszeniem;
2) określenie czasu i miejsca naruszenia i powiadomienia;
3) określenie okoliczności towarzyszących i rodzaju naruszenia;
4) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
5) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
6) wyszczególnienie wziętych faktycznie pod uwagę przesłanek do wyboru metody postępowania;

7) opisywać środki zastosowane lub proponowane w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków;
8) wstępną ocenę przyczyn wystąpienia naruszenia;
9) ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego.

6. Raport, o którym mowa w ust. 5, Administrator Systemu lub Naczelnik Wydziału Organizacji i Nadzoru niezwłocznie przekazuje Administratorowi Danych, a w przypadku jego nieobecności osobie upoważnionej.

7. Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu Administrator Systemu lub Naczelnik Wydziału Organizacji i Nadzoru zasięga niezbędnych opinii i proponuje postępowanie naprawcze, a w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzanych danych.

8. Zaistniałe naruszenie może stać się przedmiotem szczegółowej, zespołowej analizy prowadzonej przez Administratora Danych, Sekretarza Powiatu, Administratora Systemu, Naczelnika Wydziału Organizacji i Nadzoru oraz Pełnomocnika ds. Ochrony Informacji Niejawnych.

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

**§ 4.** 1. Jeżeli jest prawdopodobne, że naruszenie ochrony danych osobowych wiąże się z ryzykiem naruszenia praw i wolności osób fizycznych, Administrator Danych bez zbędnej zwłoki – w miarę możliwości nie później niż w terminie 72 godzin po stwierdzonym naruszeniu – zgłasza je Urzędu Ochrony Danych Osobowych.

2. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je Administratorowi.

**§ 5.** 1. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych, administrator danych – za pośrednictwem właściwego do danego naruszenia kierownika komórki organizacyjnej – bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.

2. Zawiadomienie, o którym mowa w ust. 1, nie jest wymagane, w następujących przypadkach:
1) administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;
2) administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w ust. 1;

3) wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

**§ 6.** 1. W przypadku kradzieży sprzętu informatycznego służącego do przetwarzania danych osobowych, użytkownik niezwłocznie powiadamia bezpośredniego przełożonego oraz Administratora Systemu lub Naczelnika Wydziału Organizacji i Nadzoru.

2. W sytuacji, o której mowa w ust. 1 decyzję o dalszym postępowaniu w zakresie powiadomienia właściwych organów oraz podjęcia innych, szczególnym czynności zabezpieczających podejmuje Administrator Danych po zapoznaniu się z raportem Administratora Systemu lub Naczelnika Wydziału Organizacji i Nadzoru.

**§ 7.** 1. Odtworzenie systemu informatycznego albo jego bazy danych zarządza Administrator Danych w oparciu o wniosek Administratora Systemu, określając rodzaj i numer kopii zapasowej służącej do odtworzenia.

2. Wykonane czynności opisuje się w dokumentacji systemu.

**§ 8.** 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. 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 Administratora Systemu lub Naczelnika Wydziału Organizacji i Nadzoru.

3. Orzeczona kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia Administratora Systemu lub lub Naczelnika Wydziału Organizacji i Nadzoru nie wyklucza odpowiedzialności karnej tej osoby zgodnie przepisami prawa oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

## Rozdział 4.
## Ocena skutków dla ochrony danych

**§ 9.** 1. Jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator **przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych**. Dla podobnych operacji przetwarzania danych

wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę.

2. Oceny, o której mowa w ust. 1 dokonuje kierownik komórki organizacyjnej, w której przetwarzane są przedmiotowe dane, w porozumieniu z Administratorem Systemu, Sekretarzem Powiatu, Naczelnikiem Wydziału Organizacji i Nadzoru oraz inspektorem ochrony danych osobowych.

3. Zasady dokonywania oceny skutków dla ochrony danych określa art. 35 RODO. Przepisy zarządzenia w sprawie organizacji procesu zarządzania ryzykiem w Starostwie Powiatowym w Sierpcu stosuje się odpowiednio.

4. Ocena skutków dla ochrony danych jest integralną częścią dokumentacji przetwarzania danych osobowych prowadzonej przez pracownika Wydziału Organizacji i Nadzoru wyznaczonego do prowadzenia dokumentacji ochrony danych osobowych.

## Rozdział 5.
## Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

**§ 10. 1.** W Starostwie Powiatowym w Sierpcu stosuje się środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych w systemach informatycznych, a w szczególności:

1) zabezpiecza dane przed ich udostępnieniem osobom nieupoważnionym;
2) zapobiega zabraniu danych przez osobę nieuprawnioną;
3) zapobiega przetwarzaniu danych z naruszeniem ustawy oraz zmianie, utracie, uszkodzeniu lub zniszczeniu tych danych.

2. Określone niżej sposoby zabezpieczeń dotyczą:

1) zabezpieczeń przed dostępem do danych osób nieupoważnionych na etapie eksploatacji systemu tj. wprowadzanie danych, aktualizacji lub usuwania danych, wyświetlania lub drukowania zestawień;
2) ochrony danych zarchiwizowanych na nośnikach zewnętrznych, procedur niszczenia niepotrzebnych wydruków lub nośników danych;
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;
4) monitorowania systemu zabezpieczeń;
5) zakresu obowiązków pracowników Starostwa Powiatowego w Sierpcu w części dotyczącej bezpieczeństwa danych.

3. Za nadzór nad przestrzeganiem określonych środków organizacyjnych i technicznych odpowiedzialny jest Naczelnik Wydziału Organizacji i Nadzoru.

**§ 11.** Wprowadza się następujące zabezpieczenia danych w systemie informatycznym:

1) na wszystkich stacjach roboczych, na których przetwarzane są dane osobowe wprowadza się **wysoki** poziom zabezpieczeń, polegający na wdrożeniu logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem poprzez m.in.:
   a) kontrolę przepływu informacji pomiędzy systemem informatycznym Administratora Danych a siecią publiczną,
   b) kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego Administratora Danych;
2) dostęp do systemu przetwarzania danych możliwy jest zgodnie z wdrożonym w Instrukcji przetwarzania danych - systemem nadawania identyfikatora i ustalania haseł:
   a) hasło - do systemu przetwarzającego dane - każdego użytkownika jest unikalne, składające się 8 znaków, zawiera małe i duże litery, cyfry lub znaki specjalne,
   b) hasła zmieniane są przez użytkownika co 30 dni,
   c) zasady zmiany i przechowywania haseł dostępu Administratora Systemów Informatycznych ustalane są odrębnie przez Naczelnika Wydziału Organizacji i Nadzoru, na wniosek Administratora Systemów;
3) pomieszczenia, w których stoi serwer i komputery zawierające dane osobowe i kartoteki osobowe są zabezpieczone poprzez system alarmowy i przeciwpożarowy;
4) ochronę przed awariami zasilania oraz zakłóceniami w sieci energetycznej serwera i stacji roboczych zapewniają zasilacze UPS;
5) urządzenia przenośne, w tym dyski i inne nośniki są szyfrowane;
6) prowadzona jest ścisła ewidencja sprzętu komputerowego oraz wszelkich nośników służących do przetwarzania danych osobowych.

**§ 12.** Szczegółowe wytyczne określające stosowane środki organizacyjne i techniczne określone są w Instrukcji w sprawie określenia zasad przetwarzania danych osobowych, warunków technicznych i osobowych zabezpieczenia zbiorów danych osobowych ze szczególnym uwzględnieniem wymogów bezpieczeństwa.

**§ 13.** Strategia ochrony danych osobowych opiera się na następujących zasadach:
1) wyznaczono Inspektora Ochrony Danych Osobowych;
2) dostęp do danych osobowych mogą mieć tylko i wyłącznie pracownicy posiadający pisemne imienne upoważnienie podpisane przez Administratora Danych Osobowych;
3) pracownik Wydziału Organizacji i Nadzoru wyznaczony do prowadzenia dokumentacji ochrony danych osobowych prowadzi także ewidencję osób upoważnionych do przetwarzania danych osobowych w Starostwie Powiatowym w Sierpcu;

4) każdy z pracowników zachowuje szczególną ostrożność przy przetwarzaniu i przenoszeniu wszelkich danych osobowych;
5) wyznaczono pomieszczenia (strefy), w których przetwarzane są dane osobowe;
6) fizyczny dostęp do pomieszczeń, w których eksploatowane są systemy informatyczne blokują drzwi zamykane na klucz (w newralgicznych pomieszczeniach antywłamaniowe klasy C z podwójnymi zamkami klasy C oraz karty dostępu) i systemy alarmowe, a w pomieszczeniach zlokalizowanych na parterze zamontowane są kraty;
7) w pomieszczeniach, w których zainstalowany jest serwer i komputery zawierające bazy danych jest zainstalowany system alarmowy i przeciwpożarowy;
8) pomieszczenia serwerowni znajdują się w odrębnych strefach bezpieczeństwa od pozostałych pomieszczeń, w których eksploatowane są systemy przetwarzające dane osobowe;
9) dostęp do kluczy do pomieszczeń, w których przetwarzane są dane osobowe mają wyłącznie upoważnieni pracownicy;
10) dostęp do pomieszczeń możliwy jest tylko w godzinach pracy urzędu: kontrolowane jest otwieranie i zamykanie pomieszczeń, w których przetwarzane są dane osobowe polegające na otwarciu pomieszczenia przez pierwszą osobę, która rozpoczyna pracę oraz zamknięciu pomieszczenia przez ostatnią wychodzącą osobę i nie pozostawianiu pomieszczenia w czasie godzin pracy bez nadzoru;
11) w przypadku, gdy wymagany jest dostęp poza godzinami pracy, możliwy jest tylko za zgodą bezpośredniego przełożonego w porozumieniu z Naczelnikiem Wydziału Organizacji i Nadzoru i zaewidencjonowany w ewidencji czasu pracy pracowników (odrębna rejestracja odbywa się automatycznie w systemie alarmowym: ruch w systemie oraz ewidencja użycia kart dostępu w pomieszczeniach newralgicznych);
12) pracownik Wydziału Organizacji i Nadzoru wyznaczony do prowadzenia dokumentacji ochrony danych osobowych prowadzi ścisłą ewidencję osób upoważnionych do załączania i odblokowywania systemu alarmowego oraz osób, którym wydano karty dostępu;
13) karty dostępu poza godzinami pracy deponowane są w miejscu wyznaczonym przez Naczelnika Wydziału Organizacji i Nadzoru;
14) w przypadku pomieszczeń, do których dostęp mają również osoby nieupoważnione, mogą one przebywać w tych pomieszczeniach tylko w obecności osób upoważnionych i tylko w czasie wymaganym na wykonywanie niezbędnych czynności oraz wyłącznie za zgodą Naczelnika Wydziału Organizacji i Nadzoru;
15) każde pomieszczenie, w którym przetwarzane są dane osobowe wyposażone jest w metalową (lub w wyjątkowych przypadkach drewnianą) szafę zamykaną na klucz, w której przechowywane są zbiory papierowe oraz wydruki danych osobowych ze zbiorów informatycznych;

16) szafy, w których przechowywane są dane osobowe są zamykane na klucz, który posiadają jedynie upoważnieni pracownicy;
17) klucze do szaf, w których przechowywane są dane osobowe przechowywane są w innym pomieszczeniu niż te, w którym znajduje się szafa;
18) szafy z danymi osobowymi powinny być otwarte jedynie na czas potrzebny do dostępu do danych a następnie powinny być zamykane;
19) dane osobowe w formie papierowej mogą znajdować się na biurkach tylko na czas niezbędny na dokonanie czynności służbowych, a następnie muszą być chowane do szaf;
20) każde pomieszczenie, w którym przetwarzane są dane osobowe wyposażone jest w niszczarkę klasy 4 zapewniającą bezpieczne niszczenie zbędnych kopii dokumentów lub nośników informatycznych zawierających dane osobowe;
21) w części pomieszczeń służących do przetwarzania danych (Wydział Komunikacji) zamontowano elektroniczny system kontroli dostępu połączony z instalacją alarmową zapewniający stały i rejestrowany podgląd osób wchodzących do pomieszczeń (prowadzona jest ścisła ewidencja wydanych karty dostępu do tych pomieszczeń);
22) zagadnienia związane z ochroną danych i obowiązki stąd wynikające są ujęte w zakresach czynności pracowników przetwarzających dane osobowe;
23) każdy pracownik przed przystąpieniem do pracy przy przetwarzaniu danych osobowych jest przeszkolony w zakresie zasad przetwarzania, ochrony i udostępniania danych osobowych;
24) każdy pracownik zapoznawany jest z dokumentacją przetwarzania danych osobowych w Starostwie Powiatowym w Sierpcu oraz składa stosowne oświadczenie potwierdzające;
25) za przygotowanie i aktualność dokumentacji przetwarzania danych osobowych odpowiada Naczelnik Wydziału Organizacji i Nadzoru;
26) dostęp do komputerów, na których przetwarzane są dane osobowe mogą mieć wyłącznie upoważnieni pracownicy zgodnie z procedurą nadawania uprawnień do dostępu do systemów;
27) stacje komputerowe, na których przetwarzane są dane powinny mieć tak ustawione monitory, aby osoby nieupoważnione nie miały wglądu w dane;
28) po zakończeniu pracy komputery przenośne zawierające dane osobowe powinny być zabezpieczone w zamkniętych na klucz szafach;
29) komputery przenośne zawierające dane osobowe mogą być wynoszone z urzędu tylko wyjątkowo i na podstawie odrębnego upoważnienia;
30) komputery przenośne zabezpiecza się dodatkowo poprzez szyfrowany dostęp do dysków;
31) nie należy udostępniać sprzętu komputerowego służbowego osobom nieupoważnionym;

32) w przypadku potrzeby przeniesienia danych osobowych pomiędzy komputerami dokonuje tego Administrator Systemu lub osoba przez niego wyznaczona;
33) nośniki użyte do przeniesienia danych należy następnie wyczyścić za pomocą specjalnego oprogramowania, aby nie zostały na nim dane osobowe;
34) w przypadku niemożliwości skasowania danych z nośnika należy taki nośnik zniszczyć fizycznie;
35) niezabezpieczonych danych osobowych nie można przesyłać drogą elektroniczną;
36) podstawowym sposobem zabezpieczania danych i dostępu do nich jest system definiowania użytkowników, grup użytkowników oraz haseł; są to zabezpieczenia programowe zaimplementowane w eksploatowane systemy uniemożliwiające dostęp do systemu osobom nieupoważnionym;
37) dodatkowym systemem zabezpieczenia jest stosowanie kryptograficznej ochrony danych, jaką oferuje system operacyjny;
38) kopie zapasowe (bezpieczeństwa) danych zarchiwizowane są na macierzy i bibliotece dyskowej, dyskach lub płytach CD i są przechowywane w innym pomieszczeniu niż to, w którym przetwarzane są dane osobowe (w ramach odrębnej strefy ochrony) chronione są w ten sposób na wypadek pożaru, zalania lub zatopienia, innej klęski żywiołowej lub katastrofy czy kradzieży;
39) prowadzona jest ścisła ewidencja nośników, o których mowa w pkt 38.

## Rozdział 6.
## Rejestrowanie czynności przetwarzania oraz pozostała dokumentacja przetwarzania danych

**§ 14.** 1. Pracownik Wydziału Organizacji i Nadzoru wyznaczony do prowadzenia dokumentacji ochrony danych osobowych prowadzi i aktualizuje:
1) rejestr czynności przetwarzania danych osobowych;
2) rejestr kategorii czynności przetwarzania danych osobowych w imieniu administratora, który powierzył przetwarzanie danych Starostwu;
3) wykaz zbiorów danych osobowych przetwarzanych w Starostwie Powiatowym w Sierpcu ze wskazaniem programów zastosowanych do przetwarzania danych;
4) wykaz miejsc wyznaczonych do przetwarzania danych osobowych w Starostwie Powiatowym w Sierpcu;
5) ewidencje osób upoważnionych do przetwarzania danych osobowych;
6) ewidencję umów powierzenia przetwarzania danych osobowych;
7) ewidencję osób upoważnionych do załączania i odblokowywania systemu alarmowego;
8) ewidencję wydanych kart dostępu do pomieszczeń wyposażonych w elektroniczny system kontroli;

9) wykaz szkoleń pracowników Starostwa z zakresu ochrony danych osobowych;
10) dokumentację oceny skutków dla ochrony danych osobowych;
11) dokumentację współpracy z Inspektorem Ochrony Danych Osobowych;
12) dokumentację kontrolną i nadzorczą w zakresie ochrony danych osobowych w Starostwie Powiatowym w Sierpcu.

2. Administrator Systemu prowadzi i aktualizuje:

1) ewidencję konserwacji, remontów, awarii sprzętu i oprogramowania komputerowego;
2) ewidencję nośników danych służących do przechowywania lub przenoszenia danych osobowych;
3) ewidencję infrastruktury informatycznej, wraz z przypisanymi do niej danymi upoważnionych pracowników oraz nadanych im identyfikatorów;
4) dokumentację postępowań w sprawie naruszeń ochrony danych osobowych, w tym rejestr incydentów i naruszeń;
5) dokumentację w zakresie opisu struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi systemami, a także inną dokumentację techniczną systemów służących do przetwarzania danych osobowych.

3. Kierownicy komórek organizacyjnych są odpowiedzialni za zgłaszanie wniosków w zakresie aktualizowania danych, w dokumentach o których mowa w ust. 1 i 2 w zakresie podległej komórki organizacyjnej.

4. Dokumentacja, o której mowa w ust. 1 i 2 może być prowadzona również w formie elektronicznej, o ile pozwala na określenie historii dokonywanych w niej zmian.

**Załącznik Nr 2**
**do ZARZĄDZENIA Nr ON.120.32.2018**
**STAROSTY SIERPECKIEGO**
**z dnia 24 maja 2018 r.**

# Instrukcja

**w sprawie określenia sposobu zarządzania systemem informatycznym służącym do przetwarzania danych osobowych ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji (zwana dalej Instrukcją zarządzania).**

## Rozdział 1.
## Informacje ogólne

**§ 1. 1.** Niniejsza instrukcja określa ogólne zasady zarządzania każdym systemem informatycznym służącym do przetwarzania danych osobowych oraz stanowi podstawę do opracowania instrukcji szczegółowych uwzględniających specyfikę poszczególnych systemów informatycznych funkcjonujących w Starostwie Powiatowym w Sierpcu.

2. Instrukcję, o której mowa w ust. 1 stosuje się odpowiednio również do zarządzania zbiorami danych osobowych przetwarzanych w Starostwie Powiatowym w Sierpcu w formie papierowej.

## Rozdział 2.
## Podmioty odpowiedzialne za ochronę danych osobowych w Starostwie Powiatowym w Sierpcu

**§ 2.** Za zapewnienie właściwego zarządzania systemami informatycznymi przetwarzającymi dane osobowe w Starostwie Powiatowym w Sierpcu odpowiada Wydział Organizacji i Nadzoru, do którego należy w szczególności:

1) opracowanie i aktualizacja dokumentacji przetwarzania danych osobowych oraz nadzór nad przestrzeganie zasad w niej określonych;
2) fizyczne zabezpieczenie danych osobowych oraz obiektów (pomieszczeń), w których przetwarzane są dane osobowe;
3) organizacyjne zabezpieczenie oraz nadzór nad obiegiem dokumentów zawierających dane osobowe;
4) zapewnienie zapoznania się osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych;
5) nadzorowanie, aktualizację i utrzymanie zbioru upoważnień dla osób upoważnionych do przetwarzania danych osobowych;
6) nadzorowanie i monitorowanie kierowników komórek organizacyjnych i samodzielne stanowiska pracy w zakresie wnioskowania oraz aktualizowania upoważnień dla ich pracowników;
7) nadawanie, modyfikacja i odbieranie uprawnień w systemach teleinformatycznych Starostwa;

8) nadzorowanie podpisywania oraz ewidencjonowanie umów i porozumień z osobami oraz podmiotami zewnętrznymi mającymi przetwarzać dane osobowe znajdujące się w Starostwie, lub którym takie przetwarzanie ma zostać powierzone;
9) prowadzenie rejestru czynności przetwarzania danych osobowych oraz rejestru kategorii czynności przetwarzania danych osobowych;
10) podjęcie natychmiastowych działań zabezpieczających dane osobowe w przypadku otrzymania informacji o naruszeniu ochrony danych osobowych;
11) niezwłoczne informowanie Administratora Danych o przypadkach naruszenia przepisów ustawy o ochronie danych osobowych;
12) analiza sytuacji, okoliczności i przyczyn, które doprowadziły do naruszenia bezpieczeństwa danych, jeśli takie wystąpiło, oraz proponowanie Administratorowi Danych zmian procedur i zasad postępowania obowiązujących w Starostwie Powiatowym w Sierpcu, mających zapobiec powstaniu podobnej sytuacji w przyszłości;
13) współpraca z Inspektorem Ochrony Danych w całym zakresie powierzonych zadań;
14) inne obowiązki przewidziane w ustawie o ochronie danych osobowych, a nie wymienione w niniejszym zarządzeniu.

**§ 3. 1.** Dla prawidłowego wykonywania zadań z zakresu ochrony danych osobowych w Starostwie Powiatowym w Sierpcu powołano **Administratora Systemu Informatycznego** (zwanego dalej: **Administratorem Systemu**), do którego zadań należy m.in.:

1) inicjowanie i przeprowadzanie kontroli systemu informatycznego oraz prawidłowości pracy poszczególnych użytkowników w systemie informatycznym zgodnie z przyjętą Polityką bezpieczeństwa;
2) wykonywanie kopii bezpieczeństwa zbiorów danych osobowych, prowadzenie ewidencji oraz właściwe ich przechowywanie;
3) rejestracja użytkowników w systemie oraz nadawanie im identyfikatora i uprawnień w zakresie ustalonym w przyjętej strategii bezpieczeństwa dla danego stanowiska oraz zgodnie z przyznanym upoważnieniem, z wyłączeniem systemu CEPiK;
4) aktualizacja i usuwanie praw dostępu do systemu informatycznego;
5) zapewnienie takiej konfiguracji systemu informatycznego, która uniemożliwi wprowadzanie lub uzyskanie danych z systemu przez niepowołane osoby oraz uniemożliwi działanie oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu, a także zabezpieczy przed utratą danych w przypadku awarii lub zakłócenia w pracy sieci;
6) administrowanie sieci informatycznej Starostwa Powiatowego w Sierpcu, w tym monitorowania sieci pod kątem zabezpieczenia przed dostępem osób nieupoważnionych oraz przestrzegania przyjętych w urzędzie zasad ochrony danych osobowych;

7) zarządzanie sprzętem komputerowym oraz oprogramowaniem służącym do przetwarzanie danych osobowych (prowadzenie i aktualizacja ewidencji) oraz konfiguracją systemu i urządzeń zgodnie z przyjętymi zasadami bezpieczeństwa;
8) nadzorowanie i kontrolowanie zabezpieczeń oraz monitorowanie zmian środowiska w tym pojawienie się nowych zagrożeń;
9) realizacja kontroli antywirusowej;
10) reagowanie na incydenty w zakresie bezpieczeństwa oraz wnioskowanie w sprawie poprawy bezpieczeństwa przetwarzania danych (ocena prawdopodobieństwa wystąpienia zdarzenia, wycena możliwości szkód, wybór poziomu zaakceptowanego ryzyka);
11) niezwłoczne informowanie Administratora Danych oraz Inspektora Ochrony Danych o przypadkach naruszenia prawa oraz zasad w zakresie ochronie danych osobowych;
12) podejmowanie działań, w tym również polegających na wyłączeniu systemu lub częściowym ograniczeniu dostępu do niego, w przypadku gdy istnieje bezpośrednie zagrożenie dla bezpieczeństwa systemu informatycznego;
13) czuwanie nad wdrażaniem zasad bezpieczeństwa w systemach informatycznych, w których przetwarzane są dane osobowe oraz dbanie o bieżące ich uaktualnianie stosownie do zmieniających się technologii informatycznych oraz zagrożeń bezpieczeństwa systemów informatycznych jednostki;
14) prowadzenie dziennika Administratora Systemu Informatycznego zawierającego wszystkie zdarzenia mające wpływ na bezpieczeństwo danych osobowych przetwarzanych w systemach teleinformatycznych Starostwa;
15) planowanie i wdrażanie technicznych środków zapobiegających naruszeniu ochrony danych osobowych;
16) przygotowywanie – w fazie projektowania systemów - propozycji rozwiązań w celu realizacji zasad ochrony danych osobowych;
17) dokonywanie przeglądów i konserwacji systemu i zbiorów danych osobowych oraz nadzorowanie takich przeglądów i konserwacji wykonywanych przez podmioty trzeciej;
18) współpraca z Inspektorem Ochrony Danych w całych zakresie powierzonych zadań;
19) inne obowiązki przewidziane w ustawie o ochronie danych osobowych.

2. Jeżeli specyfika poszczególnych systemów informatycznych oraz zapewnienie właściwego bezpieczeństwa danych tego wymaga Administrator Danych na wniosek Administratora Systemu może również wyznaczyć Administratorów Systemów Teleinformatycznych dla poszczególnych systemów informatycznych funkcjonujących w Starostwie Powiatowym w Sierpcu.

**§ 4.** Kierownik komórki organizacyjnej jest zobowiązany do:

1) każdorazowego informowania Administratora Systemu lub wyznaczonego pracownika Wydziału Organizacji i Nadzoru o planowanych przemieszczeniach sprzętu komputerowego i pracowników między pokojami lub budynkami Starostwa, gdzie dokonuje się czynności przetwarzania danych osobowych;
2) nadzorowania podległych pracowników w zakresie przestrzegania przez nich zasad ochrony przetwarzanych danych osobowych;
3) wnioskowania w sprawach odpowiednich warunków organizacyjno – technicznych w zakresie wyposażenia stanowisk pracy przetwarzających dane osobowe, umożliwiających zachowanie poufności informacji;
4) nadzorowania warunków przechowywania wydruków zawierających dane osobowe, ich archiwizacji i okresowego niszczenia oraz przechowywania danych osobowych na nośnikach danych;
5) wnioskowania o przyznanie podległemu pracownikowi sprzętu komputerowego, niezbędnego do wykonywania czynności w systemie informatycznym;
6) wnioskowanie o nadanie, zmianę lub wycofanie upoważnienia do przetwarzania danych osobowych dla podległego pracownika oraz przyznanie, modyfikację lub wycofanie uprawnień do pracy w systemie informatycznym, w tym nadanie identyfikatora;
7) przygotowywanie projektów oceny skutków dla ochrony danych dla planowanych operacji przetwarzania danych osobowych;
8) przygotowywanie projektów rejestrów czynności i kategorii czynności przetwarzania danych osobowych w podległych zbiorach danych;
9) wykonywanie zadań związanych z realizacją obowiązków Administratora, o których mowa w art. 13-22 (obowiązek informacyjny oraz prawo dostępu do danych, sprostowania, ograniczenia i usunięcia danych) w zakresie podległej komórki organizacyjnej;
10) wnioskowanie o zawarcie umowy powierzenia danych osobowych, z uwzględnieniem przedmiotu i zakresu umowy;
11) ścisła współpracy z Wydziałem Organizacji i Nadzoru, Inspektorem Ochrony Danych oraz Administratorem Systemu przy użytkowaniu systemu informatycznego przez podległych pracowników, w tym w sytuacji naruszenia ochrony danych osobowych.

**§ 5.** Osoby upoważnione do przetwarzania danych osobowych przez Administratora Danych są zobowiązane do:

1) wykonywania poleceń Administratora Systemu w zakresie zarządzania podległymi systemami informatycznymi;
2) nieprzekazywania osobom trzecim swojego identyfikatora oraz hasła ani innych informacji mających wpływ na bezpieczeństwo systemów informatycznych przetwarzających dane osobowe;
3) czuwania nad właściwym eksploatowaniem podległych im systemów informatycznych;

4) informowania Administratora Systemu o zdarzeniach wpływających na bezpieczeństwo systemów informatycznych, w tym m.in. wirusów, koni trojańskich, dialerów, spyware itp., oprogramowania nielegalnego lub zainstalowanego bez upoważnienia, awarii systemu informatycznego lub jego nieprawidłowego działania, stwierdzenia faktu korzystania z systemu informatycznego przez osobę niepowołaną, awarii zasilania itd.;
5) kontrolowania i zabezpieczenia prawidłowości przebiegu czynności serwisowych w podległych systemach informatycznych; przy czym urządzenia, dyski lub inne nośniki zawierające dane osobowe, pozbawiają przed naprawą zapisu tych danych lub nadzorują ich naprawę;
6) pozbawiania zapisu danych osobowych z nośników, które przeznaczone są do przekazywania innemu podmiotowi, nieuprawnionemu do otrzymania tych danych;
7) pozbawiania zapisu danych osobowych lub uszkadzania w sposób uniemożliwiający odczytanie nośników, które przeznaczone są do likwidacji;
8) zgłaszania Administratorowi Systemu potrzeb w zakresie zabezpieczenia podległych im systemów informatycznych;
9) postępowania zgodnie z procedurą w sytuacji naruszenia ochrony danych osobowych;
10) niszczenia wydruków, które zawierają dane osobowe i są przeznaczone do usunięcia – w stopniu uniemożliwiającym ich odczytanie.

**§ 6.** W przypadku systemów informatycznych działających w środowisku sieciowym Administrator Systemu:
1) dokonuje wyboru lub migracji do technologii minimalizującej zagrożenie uzyskania dostępu do sieci osobom nie upoważnionym;
2) zakupuje oprogramowanie umożliwiające rejestrowanie identyfikatorów i czas logowania użytkowników sieci;
3) nadzoruje proces monitorowania sieci pod kątem zabezpieczenia przed dostępem osób nie upoważnionych.

## Rozdział 3.
## Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osób odpowiedzialnych za poszczególne czynności

**§ 7.** 1. Przetwarzać dane osobowe w systemach teleinformatycznych, jak i zbiorach papierowych może wyłącznie osoba posiadająca pisemne upoważnienie do przetwarzania danych osobowych zgodnie z wzorem stanowiącym Załącznik Nr 1 do niniejszej instrukcji.

2. Wydanie upoważnienia oraz rejestracja konta i nadanie uprawnień w systemach informatycznych Starostwa Powiatowego następuje na podstawie wniosku bezpośredniego przełożonego określonego w Załączniku Nr 2 do niniejszej instrukcji.

3. Wniosek, o którym mowa w ust. 2 składany jest do Naczelnika Wydziału Organizacji i Nadzoru, który podejmuje czynności nadania uprawnień oraz wydania upoważnienia.

4. Oryginał upoważnienia zostaje przekazany pracownikowi za potwierdzeniem odbioru, kopia zostaje dołączona do akt osobowych pracownika oraz przekazana do wiadomości przełożonemu pracownika.

5. Identyfikator i hasło do systemu informatycznego przetwarzającego dane osobowe są przydzielone użytkownikowi tylko w przypadku, gdy posiada on pisemne upoważnienie do przetwarzania danych osobowych wydane przez Administratora Danych z zachowaniem procedury opisanej w niniejszej instrukcji.

6. Za przydzielenie i wygenerowanie identyfikatora i hasła użytkownikowi, który pierwszy raz będzie korzystał z systemu informatycznego, odpowiada Administrator Systemu.

7. Hasło, o którym mowa w ust. 6 przekazywane przez Administratora Systemu jest na piśmie lub ustnie, z obowiązkiem jego zmiany w momencie pierwszego logowania do systemu, zgodnie z zasadami określonymi w § 9 ust. 2 pkt 7.

7. Wyrejestrowanie użytkownika lub modyfikacja jego uprawnień w systemie informatycznym (wycofanie lub zmiana upoważnienia) następuje odpowiednio na wniosek bezpośredniego przełożonego z zgodnie z procedurą opisaną w ust. 1-3.

8. Wyrejestrowanie użytkownika z systemu informatycznego (wycofanie upoważnienia) może nastąpić na wniosek:

1) Administratora Danych;
2) przełożonego użytkownika lub koordynatora zadania, na rzecz którego były wykonywane czynności związane z przetwarzaniem danych osobowych;
3) Inspektora Ochrony Danych lub Administratora Systemu – w przypadku rażącego naruszenia zasad bezpieczeństwa danych osobowych.

9. Rejestracji, modyfikacji uprawnień i wyrejestrowania użytkownika z systemu dokonuje Administrator Systemu lub wyznaczona przez niego osoba.

**§ 8. 1.** Ewidencję osób upoważnionych do przetwarzania danych w systemie informatycznym prowadzi pracownik Wydziału Organizacji i Nadzoru wyznaczony do prowadzenia dokumentacji przetwarzania danych osobowych.

2. Ewidencja zawiera imię i nazwisko, datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych, a w przypadku osób wykorzystujących do przetwarzania danych osobowych system informatyczny dodatkowo identyfikator użytkownika przypisany danej osobie w systemie informatycznej.

nadzwyczajne do Wydziału Komunikacji i Transportu poza godzinami pracy);

4) karty awaryjnej może użyć jedynie upoważniony pracownik i konieczne jest dokonanie adnotacji w rejestrze o przyczynach użycia tej karty (karta awaryjna w czasie pracy urzędu jest deponowana u wyznaczonego pracownika Wydziału Organizacji i Nadzoru);
5) karta niedobrana przez pracownika z dyżurki jest deponowana w Wydziale Komunikacji i Transportu z odpowiednią adnotacją w rejestrze karty („karta zdeponowana w Wydziale Komunikacji i Transportu z uwagi na nieobecność pracownika");
6) Rejestr kart w Wydziale Komunikacji i Transportu nadzoruje Naczelnik Wydziału Komunikacji i Transportu.

**§ 13.** 1. Przed rozpoczęciem pracy, w trakcie rozpoczęcia pracy z systemem informatycznym oraz w trakcie pracy każdy użytkownik obowiązany jest do szczególnej staranności i uwagi, czy nie wystąpiły symptomy mogące świadczyć o naruszenia ochrony danych osobowych. Szczegółowy opis takich symptomów oraz sposób postępowania w przypadku ich wykrycia opisany jest w procedurze postępowania w przypadku naruszenia ochrony danych osobowych zawartej w „Polityce Bezpieczeństwa Starostwa Powiatowego w Sierpcu".

2. Zaczynając pracę z systemem należy przejść przez proces uwierzytelniania: najpierw należy uruchomić komputer hasłem, następnie do sieci lokalnej zabezpieczenie użytkownikiem i hasłem), a później do odpowiedniego systemu zabezpieczonego identyfikatorem i minimum 8-znakowym hasłem zwierającym małe i wielkie litery oraz cyfry lub znaki specjalne.

3. Użytkownik systemu wprowadza dane, o których mowa w ust. 2 w sposób minimalizujący ryzyko podejrzenia przez osoby nieuprawnione oraz ogólne stwierdzenie poprawności działania systemu.

4. Maksymalna ilość prób wprowadzenia hasła przy logowaniu się do systemu przetwarzającego dane wynosi trzy. Po przekroczeniu tej liczby prób logowania system blokuje dostęp do zbioru danych na poziomie tego użytkownika. Odblokowania konta może dokonać jedynie Administrator Systemu w porozumieniu z bezpośrednim przełożonym pracownika.

**§ 14.** 1. Użytkownik może posługiwać się jedynie programami autoryzowanymi, wprowadzonymi do systemu informatycznego przez Administratora Systemu.

2. Szczegółowe zasady zarządzanie sprzętem informatycznym oraz oprogramowaniem określa odrębne zarządzenie.

**§ 15.** 1. W trakcie pracy użytkownik systemu informatycznego służącego do przetwarzania danych osobowych wykonuje wydruki związane z przetwarzaniem danych wyłącznie w zakresie i ilości niezbędnej dla celów zawodowych w uzgodnieniu z przełożonym.

2. Użytkownik przechowuje wydruki z danymi osobowymi w zamkniętych, metalowych (lub wyjątkowo drewnianych) szafach.

3. Wszelkie wydruki z systemu i dokumenty zawierające dane osobowe zbędne dla dalszego przetwarzania są niszczone w niszczarce klasy 4 będącej na wyposażeniu każdego pomieszczenia, w którym przetwarzane są dane osobowe.

**§ 16.** 1. Po 5 minutach tymczasowego zaprzestania pracy lub opuszczenia stanowiska, system winien wstąpić w stan nieaktywności i wyłączenia monitora lub uruchomienia wygaszacza.

2. Ponowne uruchomienie ekranu monitora możliwe jest jedynie po ponownym wpisaniu hasła.

3. W przypadku, gdy przerwa w pracy na stacji roboczej trwa dłużej niż 60 minut użytkownik obowiązany jest wylogować się z aplikacji i systemu stacji roboczej, na której pracuje oraz sprawdzić czy nie zostały pozostawione bez zamknięcia nośniki informacji zawierające dane osobowe.

**§ 17.** 1. Zmianę użytkownika stacji roboczej każdorazowo musi poprzedzać wylogowanie się poprzedniego użytkownika.

2. Niedopuszczalne jest, aby dwóch lub większa liczba użytkowników wykorzystywała wspólnie jedno konto użytkownika.

**§ 18.** 1. Ekrany monitorów urządzeń przetwarzających dane osobowe, gdzie przebywają osoby postronne, powinny być ustawione w taki sposób, aby uniemożliwić tym osobom wgląd w dane.

2. W pomieszczeniach, gdzie przebywają osoby postronne monitory stanowisk dostępu do danych osobowych powinny być ustawione w taki sposób, aby uniemożliwić tym osobom wgląd w dane.

3. W przypadku podejrzenia naruszenia bezpieczeństwa systemu użytkownik powinien niezwłocznie poinformować o tym Administratora Systemu lub Naczelnika Wydziału Organizacji i Nadzoru.

**§ 19.** Zakończenie pracy użytkownika w systemie informatycznym obejmuje wylogowanie się użytkownika z aplikacji.

**§ 20.** 1. Szafy z danymi osobowymi powinny być otwarte tylko na czas potrzebny na dostęp do danych, a następnie powinny być zamykane.

2. Dane osobowe w formie papierowej mogą znajdować się na biurkach tylko na czas niezbędny na dokonanie czynności służbowych, a następnie muszą być chowane do metalowych szaf.

3. Niedopuszczalne, pod karą dyscyplinarną jest pozostawianie dokumentów zawierających dane osobowe po zakończeniu pracy na danym stanowisku.

**§ 21.** 1. Użytkownik systemu informatycznego zobowiązany jest zawiadomić niezwłocznie - bezpośrednio lub za pośrednictwem bezpośredniego przełożonego - Administratora Systemu lub Naczelnika Wydziału Organizacji

i Nadzoru o każdym naruszeniu zabezpieczenia systemu, polegającym w szczególności na:

1) naruszeniu hasła dostępu (system nie reaguje na hasło lub je ignoruje – usunięty mechanizm hasła),
2) częściowym lub całkowitym braku bazy danych,
3) braku możliwości uruchomienia właściwej aplikacji (programu komputerowego),
4) zmianie położenia sprzętu komputerowego lub możliwości połączenia wszystkich urządzeń.

2. Szczegółowy tryb postępowania w przypadku naruszenia ochrony przy przetwarzaniu danych osobowych określa Polityka bezpieczeństwa.

## Rozdział 6.
## Procedury tworzenia i przechowywania kopii zapasowych (bezpieczeństwa) zbiorów danych osobowych oraz programów i narzędzi programowych służących do ich przetwarzania

**§ 22.** 1. Dane osobowe przetwarzane w systemach informatycznych podlegają zabezpieczeniu poprzez tworzenie kopii zapasowych (bezpieczeństwa).

2. Za proces tworzenia kopii zapasowych odpowiada Administrator Systemu, który prowadzi ich ewidencję.

3. Administrator System sporządzania kopie zapasowe baz danych na nośniku wymiennym i centralne je przechowuje w Serwerowni głównej lub Wydziału Komunikacji Starostwa Powiatowego w Sierpcu.

4. Kopie bezpieczeństwa baz danych systemów informatycznych służących do przetwarzania danych osobowych, których bazy danych znajdują się na Serwerze Głównym, wykonuje raz w tygodniu Administrator Systemu i przechowuje na odrębnym dysku.

5. W przypadku lokalnego przetwarzania danych osobowych na stacjach roboczych użytkownicy systemu informatycznego zobowiązani są do centralnego przechowywania kopii zapasowych. Przez centralne przechowywanie kopii danych rozumie się cotygodniowe przegranie przez Użytkownika zbioru danych na specjalnie wydzielony do tego obszar dysku na serwerze. Administrator Systemu wykonuje - raz w miesiącu - kopie bezpieczeństwa przechowywanych na serwerze zbiorów, a nośniki kopii (CD lub dysk zewnętrzny) przechowuje w szafie metalowej zamykanej na klucz w Serwerowni Głównej lub Wydziału Komunikacji.

6. W zależności od potrzeb częstotliwość tworzenia kopii zapasowych może ulec zmianie. Harmonogram ich wykonywania ustala Administrator Systemu Informatycznego, w porozumieniu z kierownikiem komórki organizacyjnej właściwej dla danego zbioru danych osobowych.

**§ 23. 1.** Kopie bezpieczeństwa programów służących do przetwarzania danych wraz z wszystkimi zmianami aplikacji przechowywane są centralnie,

w metalowej szafie zamykanej na klucz, przez Administratora Systemu, z zastrzeżeniem ust. 2. Nie wykonuje się cyklicznych kopii oprogramowania.

2. Nie przechowuje się kopii bezpieczeństwa programów ogólnie dostępnych bądź których odzyskanie reguluje umowa z dostawcą systemu,

**§ 24.** 1. Kopie należy okresowo sprawdzać pod kątem ich dalszej przydatności do odtworzenia danych w przypadku awarii systemu.

2. Czas przechowywania kopii zapasowych ustala się na:

1) kopia codzienna (jeżeli jest wymagana) - 1 tydzień;
2) kopia tygodniowa - 1 miesiąc;
3) kopia miesięczna - 1 rok;
4) kopia roczna (ostatni dzień okresu bilansowego) - 5 lat.

3. Kopię należy bezzwłocznie usuwać po ustaniu ich użyteczności. Przepis § 28 stosuje się odpowiednio.

4. Dostęp do kopii zapasowych ma Administrator Systemu oraz Naczelnik Wydziału Organizacji i Nadzoru.

## Rozdział 7.
## Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe

**§ 25.** Nośniki danych osobowych, zarówno w postaci elektronicznej, jak i papierowej powinny być zabezpieczone przed dostępem osób nieupoważnionych, nieautoryzowaną modyfikacją i zniszczeniem.

**§ 26.** 1. Dane osobowe przechowuje się na dyskach twardych komputerów stacjonarnych lub dyskach serwerów, w zależności od zastosowanego systemu, w tym również w chmurze oraz w postaci wydruków.

2. Przechowywanie danych osobowych w chmurze odbywa się na podstawie umowy powierzenia przetwarzania danych osobowych, z zachowaniem zasad bezpieczeństwa zgodnych z Rozporządzeniem RODO.

3. Dane osobowe mogą być zapisane na nośnikach przenośnych tylko w przypadku tworzenia kopii zapasowych lub gdy istnieje konieczność przeniesienia tych danych w postaci elektronicznej, a wykorzystanie do tego celu sieci informatycznej jest nieuzasadnione, niemożliwe lub zbyt niebezpieczne. Ewidencję nośników prowadzi Administrator Systemu.

4. Nośniki danych, inne niż zawierające kopie zapasowe oraz wydruki powinny być przechowywane w zamkniętych szafach wewnątrz obszaru przeznaczonego do przetwarzania danych osobowych i nie powinny być bez uzasadnionej przyczyny wynoszone poza ten obszar.

5. Wydruki zawierające dane osobowe sporządzone w związku z realizacją zadań publicznych przechowuje się w zamkniętych szafach, w dokumentacji merytorycznej urzędu, przez okres wskazany w instrukcji kancelaryjnej i jednolitym rzeczowym wykazie akt.

6. Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia należy zniszczyć niezwłocznie w stopniu uniemożliwiającym ich

## Rozdział 4.
## Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem

**§ 9.** 1. 1. Dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła.

2. Systemy informatyczne służące do przetwarzania danych osobowych w Starostwie Powiatowym w Sierpcu wyposażone są w mechanizmy uwierzytelnienia użytkownika, a także kontroli dostępu do danych, przy czym:

1) za właściwy nadzór nad funkcjonowaniem tych mechanizmów odpowiada Administrator Systemu;
2) rejestracji użytkowników w systemie oraz nadania im identyfikatorów i uprawnień w zakresie ustalonym na wniosek bezpośredniego przełożonego - dokonuje Administrator Systemu;
3) każdy użytkownik systemu informatycznego, w którym przetwarza się dane osobowe, posiada ustalony, odrębny **identyfikator i hasło**;
4) identyfikator wpisuje się wraz z imieniem i nazwiskiem do ewidencji użytkowników prowadzonej przez Administratora Systemu oraz rejestruje w systemie informatycznym;
5) identyfikator składa się minimalnie z pięciu znaków, nie rozdzielonych spacjami ani znakami interpunkcyjnymi oraz nie zawiera polskich liter;
6) bezpośredni dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła;
7) hasło użytkownika powinno być zmieniane nie rzadziej niż co 30 dni i składać się z 8 znaków (małe i duże litery, znaki specjalne, cyfry);
8) identyfikator użytkownika nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego nie powinien być przydzielany innej osobie;
9) hasła użytkownika, umożliwiające dostęp do systemu informatycznego, utrzymuje się w tajemnicy, również po upływie ich ważności;
10) identyfikator osoby, która utraciła uprawnienia do dostępu do danych osobowych, należy niezwłocznie wyrejestrować z danego systemu informatycznego, unieważnić jej hasło oraz podjąć inne stosowne działania w celu zapobieżenia dalszemu dostępowi tej osoby do danych.

**§ 10.** 1. 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.

2. Identyfikatory 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.

3. Zarządzanie hasłami Administratora Systemu, w tym sposób ich zmiany, częstotliwość oraz sposób przechowywania - odbywa się na zasadach ustalonych indywidualnie.

4. W przypadku nieobecności Administratora Systemu, informacje o którym mowa w ust. 3 przechowywane są u Naczelnika Wydziału Organizacji i Nadzoru, a ich awaryjne użycie następuje za zgodą Administratora Danych lub osoby przez niego upoważnionej.

## Rozdział 5.
## Procedury rozpoczęcia, zawieszenia i zakończenia pracy przy przetwarzaniu danych osobowych

**§ 11.** 1. W pomieszczeniach, w których dokonuje się czynności przetwarzania danych, mogą przebywać jedynie osoby upoważnione.

2. Do pomieszczeń objętych szczególnym nadzorem (Wydział Komunikacji) dostęp mają wyłącznie osoby posiadające karty dostępu – wydane i ewidencjonowane przez pracownika Wydziału Organizacji i Nadzoru wyznaczonego do prowadzenia dokumentacji przetwarzania danych osobowych.

3. Osoby nieuprawnione do dostępu do danych osobowych mogą przebywać w pomieszczeniach, o których mowa w ust. 1 wyłącznie w obecności osoby zatrudnionej przy przetwarzaniu tych danych osobowych, przy czym wejście do strefy objętej szczególnym nadzorem musi zostać zaewidencjonowane w „Ewidencji wejść" ze wskazaniem osoby odpowiadającej za wprowadzenie osoby nieupoważnionej.

4. Pomieszczenia, o którym mowa w ust. 1 na czas nieobecności w nich osób upoważnionych muszą być zamykane w sposób uniemożliwiający dostęp do nich osób postronnych.

**§ 12.** Do pomieszczeń objętych specjalnym nadzorem, tj. Wydziału Komunikacji i Transportu ustanawia się następującą procedurę zarządzania kartami dostępu:

1) po godzinach pracy wszyscy pracownicy Wydziału Komunikacji i Transportu deponują karty w Wydziale Komunikacji i Transportu (zapisy w rejestrze wewnętrznym), a jeden z upoważnionych pracowników dokonuje kodowania alarmu i deponowania karty u pracownika Wydziału Organizacji i Nadzoru (zapis w rejestrze na dyżurce);
2) na drugi dzień, przed rozpoczęciem godzin pracy, upoważniony pracownik Wydziału Komunikacji i Transportu odbiera kartę od pracownika Wydziału Organizacji i Nadzoru (zapis w rejestrze na dyżurce) i odblokowuje alarm, następnie do pomieszczeń Wydziału Komunikacji i Transportu wpuszcza jedynie tych pracowników, którym wydaje imienne karty (zapis w rejestrze Wydziału Komunikacji i Transportu);
3) z uwagi na niezaplanowaną nieobecność pracownika, który zamykał pomieszczenia i którego karta znajduje się w dyżurce, aby dostać się do pomieszczeń Wydziału Komunikacji i Transportu należy użyć karty awaryjnej znajdującej się na dyżurce (podobnie jeśli konieczne jest wejście

odczytanie. Pomieszczenia, w których wykonywane są wydruki zawierające dane osobowe wyposaża się w niszczarki do dokumentów klasy 4.

**§ 27.** 1. Nośniki informacji oraz wydruki z danymi osobowymi, które są przeznaczone do udostępniania, przechowuje się w warunkach uniemożliwiających dostęp do nich osobom niepowołanym, w zabezpieczonych - przed dostępem osób nieupoważnionych – szafach oraz w pomieszczeniach innych, niż te, gdzie przechowywane są zbiory danych osobowych eksploatowane na bieżąco.

2. Przekazywanie nośników danych osobowych poza budynek Starostwa odbywa się za wiedzą Administratora Systemów.

3. W przypadku zaistnienia okoliczności uzasadniającej konieczność wyniesienia nośnika poza obszar przetwarzania danych osobowych, jego użytkownik zobowiązany jest do zachowania szczególnej ostrożności i zabezpieczenia nośnika przed dostępem osób nieupoważnionych, utratą, modyfikacją lub zniszczeniem.

4. Przekazanie nośnika zawierającego dane osobowe podmiotowi zewnętrznemu może nastąpić tylko na podstawie przepisów prawa lub zawartej umowy, protokolarnie za pośrednictwem wyznaczonego, upoważnionego pracownika.

5. Nośniki zawierające dane osobowe wykorzystywane w celu przeniesienia danych przechowuje się przez okres niezbędny do bezpiecznego przeniesienia danych, nie dłużej niż 1 miesiąc. Przepis § 28 stosuje się odpowiednio.

6. Dane osobowe z systemów informatycznych mogą być udostępniane także za pośrednictwem szyfrowanych połączeń VPN – pod nadzorem Administratora Systemu.

**§ 28.** Urządzenia, dyski lub inne nośniki informatyczne zawierające dane osobowe przeznaczone do:

1) **likwidacji** - pozbawia się wcześniej zapisu tych danych za pomocą specjalnego oprogramowania do bezpiecznego usuwania zapisanych danych, a w przypadku, gdy nie jest to możliwe, uszkadza się je w sposób uniemożliwiający odczyt danych,
2) **przekazania** innemu podmiotowi, nieuprawnionemu do ich otrzymania wcześniej pozbawia się zapisu tych danych za pomocą specjalnego oprogramowania do bezpiecznego usuwania zapisanych danych, w sposób uniemożliwiający ich odzyskanie,
3) **naprawy** – pozbawia się zapisu tych danych za pomocą specjalnego oprogramowania do bezpiecznego usuwania zapisanych danych albo naprawia się je pod nadzorem osoby upoważnionej przez Administratora Systemu.

**§ 29.** 1. W przypadku, gdy nośnik danych osobowych nie jest dłużej potrzebny, należy przeprowadzić zniszczenie nośnika lub usunięcie danych z nośnika zgodnie z procedurą opisaną w § 28.

2. Jeżeli wydruk danych osobowych nie jest dłużej potrzebny należy przeprowadzić zniszczenie wydruku przy użyciu niszczarki dokumentów.

3. W przypadku, gdy kopia zapasowa nie jest dłużej potrzebna należy przeprowadzić jej zniszczenie lub usunięcie danych z nośnika zgodnie z § 28.

**§ 30.** 1. Administrator Systemu zobowiązany jest do corocznej inwentaryzacji infrastruktury informatycznej Starostwa, z której raport - przechowywany przez pracownika Wydziału Organizacji i Nadzoru wyznaczonego do prowadzenia dokumentacji ochrony danych osobowych - stanowi integralną część systemu zarządzania bezpieczeństwem informacji.

2. W przypadku wystąpienia nieudokumentowanych w Wydziale Organizacji i Nadzoru różnic w stosunku do poprzedniej inwentaryzacji, Administrator Systemu sporządzona raport, który przekazuje Administratorowi Danych.

## Rozdział 8.
## Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

**§ 31.** 1. W celu zabezpieczenia systemu informatycznego przed atakami z zewnątrz wprowadza się na stanowiskach pracujących na zbiorach danych osobowych **całkowite odizolowanie** od części sieci zewnętrznej.

2. W przypadku konieczności wymiany informacji z serwerami zewnętrznymi na stanowiskach pracujących na zbiorach danych osobowych – dopuszcza się dostęp do sieci zewnętrznej przy zastosowaniu dodatkowych zabezpieczeń na poziomie wysokim.

3. Decyzję, o której mowa w ust. 2 podejmuje Administrator Danych po zasięgnięciu pozytywnej opinii Administratora Systemu.

**§ 32.** 1. Sprzęt informatyczny służący do przetwarzania danych w Starostwie Powiatowym w Sierpcu jest sprawdzany automatyczne i codziennie pod kątem obecności wirusów komputerowych poprzez obowiązkowe włączenie tzw. aktywnej ochrony rezydentalnej, monitorującej system – w celu wykluczenia ataków zarówno w sieci, jak i innych nośników podczas pracy.

2. W przypadku korzystania z nośników elektronicznych, pochodzących od podmiotu zewnętrznego, użytkownik jest zobowiązany do sprawdzenia go programem antywirusowym.

3. Do ochrony antywirusowej w Starostwie stosuje się oprogramowanie specjalistyczne spełniające wymagania Rozporządzenia RODO.

**§ 33.** 1. Sieć informatyczna urzędu jest zabezpieczona urządzeniem brzegowym UTM, w którym funkcjonuje zapora firewall kontrolująca przepływ informacji między systemami a sieciami, w tym zewnętrzną oraz monitoruje działania zewnętrzne w stosunku do systemów informatycznych urzędu.

2. Serwery obsługujące sieć informatyczną Starostwa pracują dokonując operacji w wydzielonych i zabezpieczonych pomieszczeniach, do których prawo dostępu posiadają wyłącznie upoważnieni przez Administratora Systemu pracownicy.

**§ 34.** Sieć wewnętrzna urzędu jest odseparowana między sobą w sposób programowy na przełącznikach w tzw. VLANY. Poszczególny, dedykowany VLAN jest widoczny tylko dla osób pracujących na danej podsieci. Zastosowanie VLAN-ów jest dodatkowym zabezpieczeniem przed ingerencją wewnątrz sieci urzędu i powoduje, że nawet fizyczne podpięcie się do sieci nie spowoduje włamania do wszystkich zasobów.

**§ 35.** 1. Komputery przenośne, na których znajdują się dane osobowe muszą być zabezpieczone hasłem systemowym i być przechowywane w wyznaczonym do tego, zabezpieczonym miejscu na terenie Starostwa Powiatowego w Sierpcu.

2. W Starostwie obowiązuje zakaz wynoszenia komputerów przenośnych, jak i dysków oraz nośników danych, na których przetwarzane lub przechowywane są dane osobowe z urzędu, z zastrzeżeniem § 27 ust. 2 -4.

**§ 36.** 1. Administrator Systemu jest zobowiązany na bieżąco informować Administratora Danych oraz bezpośredniego przełożonego pracownika o przypadkach awarii programowych wynikających z:

1) posługiwania się przez użytkowników nieautoryzowanymi programami;
2) nie przestrzegania zasad używania programów antywirusowych w określonych okolicznościach;
3) niewłaściwego wykorzystania sprzętu komputerowego.

2. Administrator Systemu składa Administratorowi Danych okresowo, nie rzadziej niż raz w roku, kompleksową analizę zarządzania systemem informatycznym służącym przetwarzaniu danych osobowych oraz założenia strategii i polityki zabezpieczenia systemów informatycznych.

**§ 37.** Urządzenia służące do przetwarzania danych osobowych zasilane energią elektryczną powinny być zabezpieczone przed utratą tych danych – w wyniku awarii zasilania lub zakłóceń w sieci zasilającej – zasilaniem awaryjnym – chroniącym przed skasowaniem lub zniszczeniem na skutek zaniku energii lub skoków napięcia (UPS).

## Rozdział 9.
## Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych

**§ 38.** 1. Wszelkie prace związane z naprawami i konserwacją sprzętu i systemu informatycznego przetwarzającego dane osobowe muszą uwzględniać wymagany poziom zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych, w celu wyeliminowania:

1) możliwości wykonania kopii danych osobowych przez osoby nie upoważnione;
2) przemieszczania urządzeń komputerowych i ich sieci służących do przetwarzania danych osobowych poza obszarem objętym ochroną;
3) podmiany elementów sprzętu komputerowego lub oprogramowania na inne, zawierające cechy ukryte.

2.Celem wykonywania przeglądów i konserwacji jest:
1) zapewnienie ciągłości pracy systemów poprzez eliminowanie niespodziewanych awarii wskutek naturalnego zużycia się urządzeń;
2) wykrywanie i eliminacja ewentualnych zagrożeń wynikających z pracy systemów bez okresowej kontroli;
3) dostrzeganie potrzeb modyfikacji istniejącej infrastruktury;
4) wykrywanie niesprawnych nośników powodujących problemy lub wprowadzających przekłamania przy przenoszeniu danych.

3. Wykonywania przeglądów i konserwacji obejmuje swym zakresem:
1) wszystkie systemy informatyczne;
2) oprogramowanie systemowe, a także oprogramowanie biurowe w ogólnym zakresie;
3) wszystkie komputery, z wyjątkiem tych, które są objęte wyłączną gwarancją producenta;
4) drukarki, skanery, monitory, dyski twarde, a także inny sprzęt peryferyjny poddawany jest jedynie ogólnym przeglądom, a wszelkie czynności serwisowe wykonywane są przez specjalistyczne punkty serwisowe.

**§ 39.** 1. Przeglądów i konserwacji sprzętu i systemu służącego do przetwarzania zbioru danych osobowych dokonuje Administrator Systemu lub osoba upoważniona – w obecności i pod nadzorem Administratora Systemu lub wskazanej przez niego osoby.

2. Czynności, o których mowa w ust. 1 dokumentowane są w rejestrze z konserwacji, remontów, awarii sprzętu i oprogramowania, prowadzonym i przechowywanym przez Administratora Systemu.

3. Przed rozpoczęciem prac serwisowych przez osoby spoza Starostwa Powiatowego w Sierpcu konieczne jest potwierdzenie tożsamości serwisantów.

4. Czynności, o których mowa w ust. 1 wykonywane są na terenie Starostwa Powiatowego w Sierpcu. W przypadku wykonywania czynności poza terenem Starostwa przepis § 28 stosuje się odpowiednio.

5. W przypadku zdalnego dostępu do komputera (np. w celu wykonania czynności serwisowych na komputerze) użytkownik komputera musi potwierdzić przejęcie pulpitu komputera oraz nadzorować wszelkie czynności wykonywane przez Administratora Systemu lub osobę, której zostały zlecono stosowne działania. Czynności dokumentuje się w rejestrze, o którym mowa w ust. 2.

**§ 40.** 1. W przypadku wykonywania przeglądów i konserwacji nośników informacji służących do przetwarzania danych stosuje się odpowiednio § 39, z zastrzeżeniem ust. 2.

2. Dopuszcza się możliwość dokonania czynności przeglądu i konserwacji nośników informacji poza terenem Starostwa z zachowaniem procedury określonej w § 27 ust. 2 -4 i § 28.

**§ 41.** 1. Ustala się następującą częstotliwość wykonywania przeglądów i konserwacji:

1) sprzętu komputerowego, w tym stacji roboczych, monitorów i urządzeń peryferyjnych - co najmniej raz w roku;
2) elementów infrastruktury sieciowej - co najmniej raz w roku;
3) systemów informatycznych - co najmniej raz na miesiąc.

2. W zależności od potrzeb harmonogram, o którym mowa w ust. 1 może ulec zmianie, za zgodą Administratora Systemu.

## Rozdział 10.
## Zabezpieczenie pomieszczeń i budynków, w których przetwarzane są dane osobowe zawarte w systemie informatycznym

**§ 42.** Szczegóły dotyczące zabezpieczenia pomieszczeń i budynków, w którym przetwarzane są dane osobowe m.in. z użyciem stacjonarnego sprzętu komputerowego określa **Polityka Bezpieczeństwa Przetwarzania Danych Osobowych w Starostwie Powiatowym w Sierpcu** oraz dokumentacja prowadzona przez wyznaczonego pracownika Wydziału Organizacji i Nadzoru

## Rozdział 11.
## Przekazywanie danych osobowych za pomocą urządzeń służących do teletransmisji danych

**§ 43.** 1. Przekazywanie danych osobowych za pomocą urządzeń służących do teletransmisji danych może nastąpić jedynie przy pomocy oprogramowania zapewniającego bezpieczną transmisję danych, w tym ograniczającego osobom nieupoważnionym możliwość dostępu do tych danych.

2. W szczególności system, o którym mowa w ust. 1 winien zapewniać szyfrowanie danych i opierać się na stosowaniu przez osoby upoważnione:

1) certyfikowanego podpisu elektronicznego wykonanego przy użyciu klucza znajdującego się na karcie;
2) kodu PIN zabezpieczającego kartę.

**§ 44.** W celu ochrony antywirusowej urządzeń służących do teletransmisji danych – konfiguracja systemu przesyłania danych powinna uniemożliwiać użytkownikom nieupoważnionym dostępu do stacji napędu dyskietek, CD-ROM oraz posiadać zabezpieczenie hasłem.

**§ 45.** 1. Osoby upoważnione przez Administratora Danych Osobowych do transmisji danych posiadają kartę elektroniczną zawierającą:
1) certyfikat;
2) indywidualny klucz;
3) PIN.

2. Okres ważności certyfikatu ustala Administrator Danych.

3. Każdorazowa zmiana certyfikatu wiąże się ze zmianą karty elektronicznej oraz klucza wraz z PIN-em.

4. Użytkownik karty elektronicznej powinien:
1) chronić kod PIN od swojej karty;
2) postępować zgodnie z instrukcją posługiwania się kartą.

5. Użytkownik karty elektronicznej nie powinien pozostawiać bez opieki stacji roboczej oraz zainstalowanego na nim oprogramowania w trakcie pracy.

## Rozdział 12.
## Przekazywanie danych osobowych do państwa trzeciego

**§ 46.** Przekazanie danych osobowych, które są przetwarzane lub mają być przetwarzane po przekazaniu do państwa trzeciego lub organizacji międzynarodowej, następuje na zasadach określonych w Rozdziale 15 RODO.

## Rozdział 13.
## Powierzenie przetwarzania danych innemu podmiotowi

**§ 47.** Administrator danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych zgodnie z postanowieniami art. 28 RODO.

## Rozdział 14.
## Kontrola przestrzegania zasad przetwarzania danych osobowych w Starostwie Powiatowym w Sierpcu

**§ 48.** Kontrolę przestrzegania przepisów o ochronie danych osobowych w Starostwie Powiatowym w Sierpcu przeprowadza:
1) Urząd Ochrony Danych Osobowych;
2) Inspektor Ochrony Danych Osobowych Starostwa Powiatowego w Sierpcu;
3) Administrator Systemu;
4) pracownik wyznaczony przez Administratora Danych na podstawie imiennego upoważnienia.

**Załącznik nr 1**
**do Instrukcji w sprawie określenia sposobu zarządzania systemem informatycznym służącym do przetwarzania danych osobowych ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji**
**- Wzór upoważnienia do przetwarzania danych osobowych**

Sierpc, dnia.....

.....
(nazwa komórki organizacyjnej)

## UPOWAŻNIENIE Nr ON.077. . 20 ..

Działając na podstawie art.29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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. Urz. UE L 119, s. 1)

z dniem .....

upoważniam Panią / Pana* .....

zatrudnioną/ego na stanowisku .....

do przetwarzania danych osobowych w zbiorach:

1) papierowych:

.....

w zakresie .....

2) informatycznych:

.....

w zakresie .....

### Jednocześnie zobowiązuję:

Do zastosowania niezbędnych środków technicznych i organizacyjnych określonych w przepisach obowiązujących, w celu zapewnienia ochrony przetwarzania danych osobowych na danym stanowisku pracy.

Upoważnienie ważne jest na czas określony/trwania stosunku pracy/obowiązywania umowy*.

.....
(podpis Administratora Danych Osobowych)

Kwituję odbiór:

.....

(data i podpis pracownika)

Do wiadomości:
Bezpośredni przełożonych/ koordynator wnioskujący o przyznanie upoważnienia
* wybrać właściwe

**Załącznik Nr 2**
**do Instrukcji w sprawie określenia sposobu zarządzania systemem informatycznym służącym do przetwarzania danych osobowych ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji**
**- Wzór wniosku o wydanie, zmianę lub wycofanie upoważnienia do przetwarzania danych osobowych oraz o nadanie, modyfikację lub odebranie uprawnień w systemie informatycznym**

Sierpc, dnia.....

.....

( nazwa komórki organizacyjnej)

**Część I.**

**Wniosek**

**o wydanie, zmianę lub wycofanie upoważnienia do przetwarzania danych osobowych**

☐ *** wydanie upoważnienia** ☐ *** zmiana upoważnienia** ☐ *** wycofanie upoważnienia**

1. Imię i nazwisko osoby upoważnionej:.....
2. Stanowisko: .....
3. Okres ważności upoważnienia[1]:.....
4. Zakres upoważnienia:

zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie[2] danych osobowych.

5. Krótkie uzasadnienie wniosku (nazwy zbiorów i czynności przetwarzania danych osobowych, a w przypadku wycofania upoważnienia, dodatkowo należy podać datę i powód ustania upoważnienia do przetwarzania danych osobowych):

.....

.....

.....

.....

.....

.....

(podpis bezpośredniego przełożonego)

* Wstawić znak „X" we właściwym miejscu.
1) Dla zatrudnionych na czas nieokreślony wpisać „bezterminowo", a dla zatrudnionych na czas określony wpisać na jaki czas zawarto umowę o pracę.
2) Niepotrzebne skreślić.

## Część II.

## Wniosek

## o rejestrację, modyfikację lub odebranie uprawnień w systemie informatycznym służącym do przetwarzania danych osobowych

☐ * nowy użytkownik ☐ * modyfikacja uprawnień ☐ * odebranie uprawnień

Imię i nazwisko osoby upoważnionej:.....

Stanowisko: .....

Opis zakresu uprawnień użytkownika w systemie informatycznym i krótkie uzasadnienie[1]):

.....

.....

.....

.....

.....

(podpis naczelnika wydziału)

Decyzja Administratora Bezpieczeństwa Informacji:

.....

(data i podpis Administratora Bezpieczeństwa Informacji)

Czynności podjęte przez Administratora Systemu[2]):

..... (nadany identyfikator)

.....

(data i podpis Administratora Systemu)

** Właściwy kwadrat zaznaczyć „X".*

*1) podać nazwę systemu informatycznego służącego do przetwarzania danych osobowych.*

*2) Wpisać datę zarejestrowania użytkownika w systemie informatycznym, datę przeszkolenia użytkownika sytemu oraz identyfikator użytkownika w systemie informatycznym.*

**Załącznik Nr 3**
**do ZARZĄDZENIA Nr ON.120.31.2018**
**STAROSTY SIERPECKIEGO**
**z dnia 24 maja 2018 r.**

# OŚWIADCZENIE

## osoby upoważnionej do przetwarzania danych osobowych

## w Starostwie Powiatowym w Sierpcu

Oświadczam, że zapoznałam/em się i rozumiem zasady dotyczące ochrony danych osobowych obowiązujące w Starostwie Powiatowym w Sierpcu i opisane w:

1) Rozporządzeniu 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 (Dz. Urz. UE L 2016, Nr 119) oraz wydanymi na jego podstawie przepisami prawa polskiego;
2) dokumentacji przetwarzania danych osobowych w Starostwie Powiatowym w Sierpcu (Polityce bezpieczeństwa przetwarzania danych osobowych w Starostwie Powiatowym w Sierpcu i Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Starostwie Powiatowym w Sierpcu)

oraz zobowiązuję się do ich przestrzegania.

Ponadto oświadczam, że zobowiązuję się do zachowania w tajemnicy danych osobowych, z którymi zapoznałam/em się w trakcie ich przetwarzania, a także sposobu ich zabezpieczenia, zarówno w trakcie, jak i po ustaniu zatrudnienia w Starostwie Powiatowym w Sierpcu.

Sierpc, dn. .....  .....

(czytelny podpis)