ZARZĄDZENIE Nr RO.SO.0050.27.2018
Burmistrza Dobrej
z dnia 29 czerwca 2018 roku

w sprawie wprowadzenia w Urzędzie Miejskim w Dobrej „Polityki bezpieczeństwa" oraz „Instrukcji zarządzania systemem służącym do przetwarzania danych osobowych"

Na podstawie Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE tzw. RODO zarządza się, co następuje:

§ 1

1. Wprowadzam i wdrażam do stosowania w Urzędzie Miejskim w Dobrej „Politykę bezpieczeństwa", stanowiącą załącznik Nr 1 do niniejszego zarządzenia
2. Wprowadzam i wdrażam do stosowania w Urzędzie Miejskim w Dobrej „Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych Urzędu Miejskiego w Dobrej, stanowiącą załącznik Nr 2 do niniejszego zarządzenia.

§ 2

Wszystkie osoby, które zostały dopuszczone do przetwarzania danych osobowych powinny zostać zapoznane z wyżej wskazaną dokumentacją.

§ 3

Osoby, które zostały upoważnione do przetwarzania danych, są obowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia określone w Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych Urzędu Miejskiego w Dobrej oraz w Polityce bezpieczeństwa Urzędu Miejskiego w Dobrej.

§ 4

Wykonanie zarządzenia powierza się Inspektorowi ochrony danych osobowych Urzędu miejskiego w Dobrej.

§ 5

Traci moc zarządzenie nr 15/2011 Burmistrza dobrej z dnia 01 czerwca 2011r. w sprawie wprowadzenia i wdrożenia do stosowania instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych oraz polityki bezpieczeństwa danych osobowych.

§ 6

Zarządzenie wchodzi w życie z dniem 1 lipca 2018r.

BURMISTRZ
DOBREJ
Andrzej Piątkowski

Załącznik Nr 2
do Zarządzenia Burmistrza Dobrej nr RO.SO.0050.27.2018
z dnia 29.06.2018r.

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych Urzędu Miejskiego w Dobrej

§ 1
Wprowadzenie

1. Niniejsza instrukcja określa zasady eksploatacji i zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych Urzędu Miejskiego w Dobrej
2. Zasady opisane w niniejszym dokumencie są zgodne z obowiązującymi wymaganiami prawnymi, w szczególności:
    1) ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2014 r. poz. 1182 ze zm.), zwaną dalej „OchrDanychU",
    2) rozporządzeniem 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, zwanym dalej „DokPrzetwR".
3. W instrukcji stosuje się następujące skróty:
    1) IODO – Inspektor Ochrony Danych Osobowych, realizujący czynności określone w art. 36a OchrDanychU;
    2) ASI – Administrator Systemu Informatycznego, odpowiedzialny za administrację systemami informatycznymi.

§ 2
Poziom bezpieczeństwa

System informatyczny przetwarzający dane osobowe jest połączony z publiczną siecią telekomunikacyjną (Internet), wymagana jest ochrona na poziomie wysokim zgodnie z § 6 rozporządzenia. Niniejszy dokument opisuje niezbędny do uzyskania tego bezpieczeństwa zbiór procedur i zasad dotyczących przetwarzania danych osobowych oraz ich zabezpieczenia.

§ 3

Zasada bezpiecznego użytkowania sprzętu IT

1. Sprzęt IT służący do przetwarzania zbioru danych osobowych, składa się z komputerów stacjonarnych, laptopów, serwera, drukarek.
2. Użytkownik zobowiązany jest korzystać ze Sprzętu IT w sposób zgodny z jego przeznaczeniem i chronić go przed jakimkolwiek zniszczeniem lub uszkodzeniem.
3. Użytkownik zobowiązany jest do zabezpieczenia Sprzętu IT przed dostępem osób nieupoważnionych a w szczególności zawartości ekranów monitorów.
4. Użytkownik ma obowiązek natychmiast zgłosić zagubienie, utratę lub zniszczenie powierzonego mu Sprzętu IT.
5. Samowolne otwieranie (demontaż) Sprzętu IT, instalowanie dodatkowych urządzeń (np. twardych dysków, pamięci) do lub podłączanie jakichkolwiek niezatwierdzonych urządzeń do systemu informatycznego jest zabronione.
6. Pracownicy nie mogą korzystać z prywatnego sprzętu IT (np. laptopów, nośników typu pendrive) do wykonywania zadań służbowych.

§ 4

Zasady korzystania z oprogramowania

1. Użytkownik zobowiązuje się do korzystania wyłącznie z oprogramowania dopuszczonego do stosowania w Urzędzie Miejskim w Dobrej
2. Użytkownik nie ma prawa kopiować oprogramowania zainstalowanego na Sprzęcie IT przez Pracodawcę, na swoje własne potrzeby ani na potrzeby osób trzecich.
3. Instalowanie jakiegokolwiek oprogramowania na Sprzęcie IT może być dokonane wyłącznie przez osobę upoważnioną.
4. Użytkownicy nie mają prawa do instalowania ani używania oprogramowania innego, niż przekazane lub udostępnione im przez Administratora Danych Osobowych. Zakaz dotyczy między innymi instalacji oprogramowania z zakupionych dyskietek, płyt CD, programów ściąganych ze stron internetowych, a także odpowiadania na samoczynnie pojawiające się reklamy internetowe.
5. Użytkownicy nie mają prawa do zmiany parametrów systemu, które mogą być zmienione tylko przez osobę upoważnioną.
6. W przypadku naruszenia któregokolwiek z powyższych postanowień Administrator Systemu Informatycznego ma prawo niezwłocznie i bez uprzedzenia usunąć nielegalne lub niewłaściwie zainstalowane oprogramowanie.

§ 5

Zasady korzystania z Internetu

1. Użytkownik zobowiązany jest do korzystania z Internetu wyłącznie w celach służbowych.
2. Zabrania się zgrywania na dysk twardy komputera oraz uruchamia jakichkolwiek programów nielegalnych oraz plików pobranych z niewiadomego źródła. Pliki takie powinny być ściągane tylko za każdorazową zgodą Inspektora Ochrony Danych Osobowych i tylko w uzasadnionych przypadkach.
3. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z Internetu.
4. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hackerskim, pornograficznym, lub innym zakazanym przez prawo (na większości stron tego typu jest zainstalowane szkodliwe oprogramowanie, infekujące w sposób automatyczny system operacyjny komputera szkodliwym oprogramowaniem).
5. Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł.
6. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka) oraz adresu www rozpoczynającego się frazą"https:".
7. Należy zachować szczególną ostrożność w przypadku żądania lub prośby podania kodów, PIN-ów, numerów kart płatniczych przez Internet. Szczególnie tyczy się to żądania podania takich informacji przez rzekomy bank.
8. Użytkownicy mogą także korzystać z Internetu dla celów prywatnych, ale wyłącznie okazjonalnie i powinno być ono ograniczone do niezbędnego minimum.
9. Korzystanie z Internetu dla celów prywatnych nie może wpływać na jakość i ilość świadczonej przez Użytkownika pracy oraz na prawidłowe i rzetelne wykonywanie przez niego obowiązków służbowych, a także na wydajność systemu informatycznego Pracodawcy.
10. Przy korzystaniu z Internetu, Użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i prawa autorskiego.
11. W zakresie dozwolonym przepisami prawa, Administrator Danych Osobowych zastrzega sobie prawo kontrolowania sposobu korzystania przez Użytkownika z Internetu pod kątem wyżej opisanych zasad.
12. Ponadto, w uzasadnionym zakresie, Administrator Danych Osobowych zastrzega sobie prawo kontroli czasu spędzanego przez Użytkownika w Internecie.

13. Administrator Danych Osobowych może również blokować dostęp do niektórych treści dostępnych przez Internet.

§ 6

Zasady korzystania z poczty elektronicznej

1. Przesyłanie danych osobowych z użyciem maila poza Urzędem Miejskim w Dobrej może odbywać się tylko przez osoby do tego upoważnione.
2. W przypadku przesyłania informacji wrażliwych wewnątrz jednostki bądź wszelkich danych osobowych poza jednostką należy wykorzystywać mechanizmy kryptograficzne (hasłowanie wysyłanych plików, podpis elektroniczny).
3. W przypadku zabezpieczenia plików hasłem, obowiązuje minimum 8 znaków: duże i małe litery i cyfry lub znaki specjalne a hasło należy przesłać odrębnym mailem lub inną metodą, np. telefonicznie lub SMS-em.
4. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.
5. Zaleca się, aby użytkownik podczas przesyłania danych osobowych mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.
6. Nie należy otwierać załączników (plików) w mailach nadesłanych przez nieznanego nadawcę lub podejrzanych załączników nadanych przez znanego nadawcę.
7. Nie należy otwierać stron internetowych wskazanych hiperlinkami w mailach, gdyż mogą to być hiperlinki do stron zainfekowanych lub niebezpiecznych.
8. Użytkownicy nie powinni rozsyłać za pośrednictwem maila informacji o zagrożeniach dla systemu informatycznego, „łańcuszków szczęścia", itp.
9. Użytkownicy nie powinni rozsyłać, maili zawierających załączniki o dużym rozmiarze.
10. Użytkownicy powinni okresowo kasować niepotrzebne maile. Archiwizacja poczty przychodzącej oraz wychodzącej sekretariatu jest archiwizowana przez ASI.
11. Podczas wysyłania maili do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości – UDW".
12. Mail jest przeznaczony wyłącznie do wykonywania obowiązków służbowych.
13. Użytkownicy mają prawo korzystać z poczty własnej e-mail dla celów prywatnych wyłącznie okazjonalnie i powinno być to ograniczone do niezbędnego minimum.
14. Korzystanie z maila dla celów prywatnych nie może wpływać na jakość i ilość świadczonej przez Użytkownika pracy oraz na prawidłowe i rzetelne wykonywanie przez niego obowiązków służbowych.
15. Przy korzystaniu z maila, Użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i prawa autorskiego.

16. Użytkownicy nie mają prawa korzystać z maila w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania.
17. Użytkownik bez zgody Administratora Danych Osobowych nie ma prawa wysyłać wiadomości zawierających dane osobowe dotyczące pracowników, klientów, dostawców lub kontrahentów za pośrednictwem Internetu, w tym przy użyciu prywatnej elektronicznej skrzynki pocztowej.

§ 7

Ochrona antywirusowa

1. Użytkownicy zobowiązani są do skanowania plików wprowadzanych z zewnętrznych nośników programem antywirusowym.
2. Zakazane jest wyłączanie systemu antywirusowego podczas pracy systemu informatycznego przetwarzającego dane osobowe.
3. W przypadku stwierdzenia zainfekowania systemu, użytkownik obowiązany jest poinformować niezwłocznie o tym fakcie Administratora Systemów Informatycznych.

§ 8

Procedura nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności

1. Podstawą do nadania uprawnień do przetwarzania danych osobowych w systemie informatycznym Urzędu Miejskiego w Dobrej jest upoważnienie do przetwarzania danych osobowych. Upoważnienie wydawane jest przez Administratora Danych Osobowych.
2. Dostęp do systemu informatycznego służącego do przetwarzania danych osobowych może uzyskać wyłącznie osoba upoważniona do przetwarzania danych osobowych, zarejestrowana jako użytkownik w tym systemie przez ASI.
   1) Inspektor Ochrony Danych Osobowych :
   2) w przypadku gdy dana osoba otrzymuje po raz pierwszy upoważnienie do przetwarzania danych osobowych informuje ją o obowiązkach związanych z zapewnieniem ochrony danych osobowych;
   3) odbiera od powyższej osoby podpis pod upoważnieniem do przetwarzania danych osobowych i oświadczeniem o zapoznaniu się z obowiązującymi zasadami ochrony danych osobowych.

3. Inspektor Ochrony Danych Osobowych prowadzi, w imieniu i z upoważnienia Administratora Danych Osobowych, ewidencję osób upoważnionych do przetwarzania danych osobowych. Każda zmiana w zakresie informacji zawartych w ewidencji podlega niezwłocznemu odnotowaniu przez Inspektora ochrony Danych Osobowych.
4. Uprawnienia dostępu do systemu informatycznego nadawane są na podstawie wniosku przełożonego danego pracownika,.
5. Za nadanie uprawnień w systemie informatycznym odpowiada ASI. Uprawnienia nie mogą być nadane w przypadku, jeżeli dana osoba nie posiada upoważnienia do przetwarzania danych osobowych w wymaganym zakresie.
6. ASI informuje osobę wnioskującą o fakcie nadania lub odmowy nadania uprawnień.
7. W przypadku nadawania użytkownikowi uprawnień do danego systemu informatycznego po raz pierwszy, ASI dokonuje nadania użytkownikowi identyfikatora i generuje hasło a następnie zgłasza Inspektorowi ochrony Danych Osobowych w celu wpisania identyfikatora do ewidencji osób upoważnionych do przetwarzania danych osobowych.
8. Identyfikator użytkownika w systemie informatycznym musi być unikalny dla użytkownika. Nie może być to identyfikator, który w przeszłości był już stosowany w systemie informatycznym. Sprawdzenie unikalności identyfikatora odbywa się na podstawie ewidencji osób upoważnionych do przetwarzania danych osobowych.
9. Hasło użytkownika jest przydzielane indywidualnie każdemu z użytkowników i znane jest tylko użytkownikowi, który się nim posługuje.
10. ASI przekazuje użytkownikowi identyfikator i hasło.
11. Użytkownik jest zobowiązany do zmiany hasła przy pierwszym dostępie do systemu informatycznego.

§ 9

Procedura odbierania uprawnień do przetwarzania danych w systemie informatycznym

1. W przypadku konieczności odebrania lub zmiany zakresu upoważnienia – w związku ze zmianą zakresu obowiązków służbowych pracownika lub zakończeniem pracy – jego przełożony wnioskuje do Inspektora Ochrony Danych Osobowych o wykonanie powyższej czynności. Administrator Danych Osobowych dokonuje, na podstawie informacji przekazanej przez Inspektora Ochrony Danych Osobowych, odebrania lub zmiany zakresu upoważnienia, ASI zaś dokonuje odebrania lub zmiany zakresu uprawnień w systemie informatycznym. O powyższym Inspektora Ochrony Danych Osobowych informuje osobę wnioskującą.
2. Odebranie uprawnień może mieć charakter czasowy lub trwały.
3. Odebranie uprawnień następuje poprzez:

- zablokowanie konta użytkownika do czasu ustania przyczyny uzasadniającej blokadę (wyrejestrowanie czasowe),
- usunięcie danych użytkownika z bazy użytkowników systemu (wyrejestrowanie trwałe).

4. Czasowe wyrejestrowanie użytkownika z systemu informatycznego musi nastąpić w przypadku:
   - nieobecności użytkownika w pracy trwającej dłużej niż 21 dni kalendarzowych,
   - zawieszenia w pełnieniu obowiązków służbowych.
5. Przyczyną czasowego wyrejestrowania użytkownika z systemu informatycznego może być:
   - wypowiedzenie umowy o pracę,
   - wszczęcie postępowania dyscyplinarnego względem osoby upoważnionej do przetwarzania danych osobowych.
6. Przyczyną trwałego wyrejestrowania użytkownika z systemu informatycznego jest rozwiązanie lub wygaśnięcie stosunku pracy lub innego stosunku prawnego, w ramach którego zatrudniony był użytkownik.
7. W przypadku konieczności odebrania lub zmiany zakresu upoważnienia dla osób nie będących pracownikami Urzędu Miejskiego w Dobrej o wykonanie powyższej czynności wnioskuje pracownik koordynujący działania danej osoby.

§ 10
Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem

1. Użytkownicy systemu informatycznego przetwarzającego dane osobowe wykorzystują w procesie uwierzytelnienia identyfikatory i hasła.
2. Identyfikator jest w sposób jednoznaczny przypisany użytkownikowi i nie podlega zmianie.
3. Nowe hasło jest przekazywane użytkownikowi przez ASI.
4. Po zalogowaniu do systemu z wykorzystaniem otrzymanego hasła użytkownik jest zobowiązany do dokonania jego natychmiastowej zmiany, nawet, jeżeli system informatyczny nie wymusza takiego działania.
5. Hasła dostępu do systemu informatycznego muszą spełniać poniższe warunki:
   1) posiadać długość co najmniej 8 znaków,
   2) zawierać litery małe i duże,
   3) zawierać cyfry lub znaki specjalne.
6. Hasło jest zmieniane przez użytkownika nie rzadziej niż co 30 dni lub niezwłocznie w przypadku podejrzenia, iż mogły z nim się zapoznać nieuprawnione osoby. Hasło powinno różnić się od poprzednio używanych.

7. Użytkownik zobowiązany jest do:
   1) nieujawniania hasła innym osobom, w tym innym użytkownikom,
   2) zachowania hasła w tajemnicy, również po jego wygaśnięciu,
   3) niezapisywania hasła,
   4) postępowania z hasłami w sposób uniemożliwiający dostęp do nich osobom trzecim,
   5) przestrzegania zasad dotyczących jakości i częstości zmian hasła,
   6) wprowadzania hasła do systemu w sposób minimalizujący podejrzenie go przez innych użytkowników systemu.
8. W przypadku zapomnienia hasła użytkownik powinien zwrócić się do ASI o wygenerowanie nowego hasła.
9. W przypadku podejrzenia zapoznania się z hasłem przez osobę nieuprawnioną użytkownik jest zobowiązany do natychmiastowej zmiany hasła oraz powiadomienia o zaistniałym fakcie Inspektora Ochrony Danych Osobowych.
10. Zabronione jest zapisywanie haseł w sposób jawny.
11. Zabrania się użytkownikom systemu udostępniania swojego identyfikatora i hasła innym osobom oraz korzystania przez osoby upoważnione do przetwarzania danych osobowych z identyfikatora lub hasła innego użytkownika. Wyjątki są dopuszczalne za zgodą Administratora Danych Osobowych i pod nadzorem Administratora Systemu Informacji.
12. Hasło administratora systemu przechowywane jest w szafie zamykanej na klucz, do której dostęp ma wyłącznie Administrator Danych Osobowy, ewentualnie osoba przez niego wskazana.

§ 11

Procedura rozpoczęcia, zawieszenia i zakończenia pracy przeznaczona dla użytkowników systemu

1. Rozpoczynając pracę w systemie informatycznym przetwarzającym dane osobowe, użytkownik:
   1) uruchamia komputer,
   2) wprowadza niezbędne do pracy identyfikatory i hasła,
   3) hasła są wprowadzane w sposób minimalizujący ryzyko podejrzenia ich przez osoby trzecie,
   4) w przypadku problemów z rozpoczęciem pracy, spowodowanych odrzuceniem przez system wprowadzonego identyfikatora i hasła, natychmiast kontaktuje się z ASI,
   5) w przypadku niestandardowego zachowania aplikacji przetwarzającej dane osobowe pracownik natychmiast powiadamia o zaistniałym fakcie ASI.

2. Zawieszając pracę w systemie informatycznym (w tym odchodząc od stanowiska pracy), użytkownik blokuje stację roboczą. Kontynuacja pracy może nastąpić po odblokowaniu stacji roboczej po wprowadzeniu hasła, w sposób gwarantujący jego niepodejrzenie przez osoby trzecie.
3. Opuszczając pomieszczenie, w którym przetwarzane są dane osobowe, pracownik zobowiązany jest do zamknięcia pomieszczenia na klucz, jeżeli w pomieszczeniu tym nie przebywa inna osoba upoważniona do przebywania w tym pomieszczeniu. Zabronione jest pozostawianie bez nadzoru w pomieszczeniach, w których przetwarzane są dane osobowe, osób nieupoważnionych.
4. Kończąc pracę w systemie informatycznym pracownik wylogowuje się ze wszystkich aplikacji, z których korzystał, wyłącza stację roboczą i zabezpiecza nośniki danych. W przypadku gdy pracownik jest ostatnią osobą opuszczającą pomieszczenie, sprawdza zamknięcie okien, zamyka na klucz drzwi do pomieszczenia.

§ 12

Procedura tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

1. Za tworzenie i przechowywanie kopii zapasowych odpowiedzialny jest ASI.
2. Kopie zapasowe systemów przetwarzających dane osobowe są codziennie zapisywane na taśmy magnetyczne. Zapis odbywa się w godzinach 16–20.
3. Nośniki kopii zapasowych oznaczane są w sposób umożliwiający określenie daty utworzenia kopii oraz nazwy systemu.
4. Nośniki z kopiami zapasowymi przechowywane są w miejscu zabezpieczonym.
5. Utworzone kopie zapasowe podlegają weryfikacji ze względu na sprawdzenie możliwości odczytu danych.
6. ASI odpowiada za prowadzenie ewidencji wykonania kopii zapasowych.
7. Inspektor Ochrony Danych Osobowych określa czas przechowywania poszczególnych kopii zapasowych, w zależności od celu przetwarzania danych zapisanych na kopiach zapasowych.
8. ASI odpowiedzialny jest za realizację działań odtworzeniowych w przypadku konieczności podjęcia takich działań w związku z awarią systemu informatycznego Urzędu Miejskiego w Dobrej . Po odtworzeniu systemu informatycznego ASI odpowiedzialny jest za przeprowadzenie testów poprawności działania systemu przed jego oddaniem do użytkowania.
9. ASI przeprowadza weryfikację możliwości odtworzenia danych zapisanych na kopiach zapasowych. Weryfikacja taka powinna być przeprowadzana nie rzadziej niż raz na pół roku.

§ 13

Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz nośników kopii zapasowych

1. Dane osobowe przechowywane są w postaci elektronicznej na:
    1) nośnikach elektronicznych wbudowanych w sprzęt informatyczny lub stanowiących element tego systemu,
    2) przenośnych nośnikach elektronicznych (wymienne twarde dyski, pendrive, płyty CD, DVD).
2. Dane przechowywane są na nośnikach przenośnych jedynie w przypadkach, gdy jest to konieczne, przez czas niezbędny do spełnienia celu, w jakim zostały one na nośniku zapisane. Po ustaniu czasu przechowywania zawartość nośnika podlega skasowaniu przy użyciu narzędzi zaakceptowanych do użycia w Urzędzie Miejskim w Dobrej a w przypadku nośników optycznych stosuje się niszczenie w niszczarkach umożliwiających niszczenie tego typu nośników.
3. Dane osobowe w systemie informatycznym przechowywane są przez czas wymagany do spełnienia celu, dla którego są one przetwarzane. Po jego upływie dane podlegają skasowaniu lub anonimizacji.
4. Przenośne elektroniczne nośniki informacji zawierające dane osobowe są przechowywane przez pracowników w sposób minimalizujący ryzyko ich uszkodzenia lub zniszczenia, w szczególności w zamykanych szafach i meblach biurowych. Inspektor Ochrony Danych Osobowych wyznacza pomieszczenia, w których mogą być przechowywane takie nośniki.
5. Użytkownicy nie mogą wynosić na zewnątrz organizacji wymiennych elektronicznych nośników informacji z zapisanymi danymi osobowymi bez zgody Inspektora Ochrony Danych Osobowych.
6. Dane osobowe wynoszone poza organizację muszą być zaszyfrowane.
7. W przypadku uszkodzenia lub zużycia nośnika zawierającego dane osobowe należy dokonać jego fizycznego zniszczenia lub trwałego usunięcia znajdujących się na nim danych.
8. Przekazywanie nośników z danymi osobowymi powinno być przeprowadzone z uwzględnieniem zasad bezpieczeństwa. Adresat powinien zostać powiadomiony o przesyłce, zaś nadawca powinien sporządzić kopię przesłanych danych. Adresat powinien powiadomić nadawcę o otrzymaniu przesyłki. Jeżeli nadawca nie otrzyma potwierdzenia, zaś adresat twierdzi, że nie otrzymał przesyłki, użytkownik będący nadawcą powinien poinformować o zaistniałej sytuacji Inspektora Ochrony Danych Osobowych.

9. W przypadku wycofania sprzętu komputerowego z użycia dane osobowe na nim zapisane są kasowane przy użyciu dedykowanego oprogramowania do bezpiecznego usuwania danych zaakceptowanego do użycia w Urzędzie Miejskim w Dobrej. W przypadku braku możliwości programowego usunięcia danych dysk podlega fizycznemu zniszczeniu. Za zniszczenie danych odpowiada ASI. Zniszczenie nośnika potwierdzane jest protokołem przechowywanym przez Inspektora Ochrony Danych Osobowych.
10. Dopuszcza się powierzenie niszczenia nośników danych wyspecjalizowanym podmiotom zewnętrznym, pod warunkiem:
    1) zawarcia umowy, o której mowa w art. 31 OchrDanychU,
    2) zagwarantowania poufności danych przez usługodawcę,
    3) umożliwienia prowadzenia nadzoru nad procesem niszczenia nośników przez Inspektora Ochrony Danych Osobowych lub upoważnionego przez niego pracownika,
    4) udokumentowania faktu zniszczenia nośników protokołem.

§ 14

Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem działania jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

1. W celu zabezpieczenia systemu informatycznego przed działaniem niebezpiecznego oprogramowania zabrania się:
    1) uruchamiania jakiegokolwiek oprogramowania, które nie zostało zatwierdzone do użytku;
    2) samowolnego korzystania z nośników przenośnych;
    3) otwierania poczty elektronicznej, której tytuł nie sugeruje związku z pełnionymi obowiązkami służbowymi; w przypadkach wątpliwych należy skonsultować się z Inspektorem Ochrony Danych Osobowych;
    4) korzystania z Internetu w celach nie związanych z pełnionymi obowiązkami służbowymi;
    5) podłączania komputerów do sieci zewnętrznych za pośrednictwem modemów.
2. W przypadku zauważenia objawów mogących wskazywać na obecność niebezpiecznego oprogramowania użytkownik jest zobowiązany powiadomić ASI. Do objawów powyższych można zaliczyć:
    1) istotne spowolnienie działania systemu informatycznego,
    2) nietypowe działanie aplikacji,
    3) nietypowe komunikaty,
    4) utratę danych lub modyfikację danych.

3. System informatyczny jest zabezpieczony przed działaniem niebezpiecznego oprogramowania poprzez:
   1) oprogramowanie antywirusowe,
   2) zaporę sieciową,
   3) aktualizację oprogramowania systemowego,
   4) konfigurację oprogramowania minimalizującą ryzyko naruszenia bezpieczeństwa.
4. ASI jest odpowiedzialny za nadzór nad działaniem powyższych zabezpieczeń, a w szczególności za:
   1) weryfikację aktualności sygnatur systemu antywirusowego i podejmowanie ewentualnych działań korekcyjnych,
   2) weryfikację logów systemu antywirusowego i podejmowanie działań korekcyjnych,
   3) przegląd logów zapory sieciowej oraz podejmowanie działań mających na celu zablokowanie ataków sieciowych,
   4) weryfikację poprawności aktualizacji oprogramowania systemowego.

§ 15
Odnotowanie informacji o udostępnieniu danych osobowych

1. Urząd Miejski w Dobrej udostępnia dane osobowe jedynie w przypadkach prawnie dopuszczalnych.
2. Odnotowanie faktu udostępnienia danych następuje:
   1) w przypadku [...] poprzez wprowadzenie przez użytkownika w polu [...] informacji o udostępnieniu danych,
3. Przy odnotowywaniu przez użytkownika informacji o udostępnieniu danych, użytkownik wprowadza zapis „Dane osobowe w zakresie ››zakres‹‹ udostępniono ››odbiorca‹‹ w dniu ››data‹‹", wprowadzając zamiast zapisów w nawiasach klamrowych odpowiednie informacje.

§ 16
Procedura wykonywania przeglądu i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych

1. Przegląd i konserwacja sprzętu informatycznego realizowany jest przez upoważnionych pracowników lub przez właściwe podmioty zewnętrzne.

2. Wszelkie naprawy urządzeń komputerowych oraz zmiany w systemie informatycznym Administratora Danych, przeprowadzane są – o ile to możliwe – przez Administratora Systemu Informatycznego.
3. Prace serwisowe wykonywane na terenie jednostki przez podmioty zewnętrzne podlegają bezpośredniemu nadzorowi ASI.
4. Przekazanie sprzętu teleinformatycznego do naprawy poza teren jednostki jest dopuszczalne, jeżeli spełnione zostaną poniższe warunki:
   1) sprzęt przekazywany jest bez nośników zawierających dane osobowe, zaś fakt usunięcia nośników danych lub stwierdzenia braku nośników danych jest potwierdzany protokołem,
   2) przekazanie sprzętu potwierdzane jest protokołem, pozwalającym na jednoznaczne wskazanie osoby przekazującej i osoby odbierającej sprzęt.
5. Protokoły, o których mowa w punkcie 3, lub ich kopie przechowywane są przez ASI.
6. Wszelkie prace serwisowe wykonywane przez podmioty zewnętrzne wymagają sporządzenia protokołu serwisowego, zawierającego co najmniej poniższe informacje:
   1) wskazanie osoby przeprowadzającej prace serwisowe oraz podmiotu, którego osoba ta jest pracownikiem,
   2) wskazanie osoby nadzorującej przebieg prac serwisowych (dotyczy sytuacji, gdy prace realizowane są w siedzibie),
   3) przedmiot prac serwisowych (w szczególności identyfikator sprzętu w przypadku prac serwisowych dotyczących sprzętu),
   4) zakres prac serwisowych i ich wynik,
   5) czas przeprowadzania prac serwisowych.
7. Jeśli nośnik danych (dysk, płyta lub inne) zostanie uszkodzony i nie można go odczytać ani usunąć z niego danych, należy go zniszczyć mechanicznie w niszczarce lub innym urządzeniu gwarantującym trwałe usunięcie danych.

§ 17
Postanowienia końcowe

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest zapoznać się przed dopuszczeniem do przetwarzania danych z niniejszą instrukcją oraz złożyć stosowne oświadczenie, potwierdzające znajomość jej treści.
2. Niezastosowanie się do procedur określonych w niniejszej instrukcji przez pracowników upoważnionych do przetwarzania danych osobowych może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych.

Załączniki do Instrukcji zarządzania systemem informatycznym:

1. Załącznik nr. 1 Rejestr nośników komputerowych zawierających dane osobowe.
2. Załącznik nr. 2 Ewidencja udostępniania danych.
3. Załącznik nr. 3 Metryka hasła.
4. Załącznik nr.4 Rejestr napraw i przeglądów.

BURMISTRZ
Andrzej Piątkowski

Załącznik nr 1 - rejestr nośników komputerowych zawierających dane osobowe

REJESTR NOŚNIKÓW KOMPUTEROWYCH ZAWIERAJĄCYCH DANE OSOBOWE

URZĄD MIEJSKI W DOBREJ

Oznaczenie nośnika	Data wpisania w rejestr	Opis nośnika	Miejsce przechowywania nośnika	Imię i nazwisko użytkownika	Uwagi

BURMISTRZ DOBREJ
Andrzej Piątkowski

Załącznik nr 2 - ewidencja udostępniania danych

EWIDENCJA UDOSTĘPNIANIA DANYCH

URZĄD MIEJSKI W DOBREJ

Lp.	Data udostępnienia danych	Podmiot, któremu dane udostępniono (nazwa, adres)	Podstawa prawna udostępnienia danych	Zakres udostępnionych danych	Podpis pracownika

BURMISTRZ DOBREJ
Andrzej Piątkowski

Załącznik nr 3 - metryka hasła do Instrukcji zarządzania systemem informatycznym

Nazwa systemu / Rodzaj hasła	Hasło	Data utworzenia	Podpis Administratora

BURMISTRZ
DOBRE...
Andrzej Piątkowski

Załącznik nr 4 – Rejestr napraw, przeglądów i konserwacji systemów informatycznych

REJESTR NAPRAW, PRZEGLĄDÓW I KONSERWACJI SYSTEMÓW INFORMATYCZNYCH

W URZĘDZIE MIEJSKIM W DOBREJ

Lp.	Data zdarzenia	Numer umowy	System informatyczny, którego zdarzenie dotyczy	Rodzaj usługi	Podpis wykonującego usługę	Podpis Administratora Danych

BURMISTRZ
DOBREJ
Andrzej Piątkowski

Załącznik nr 5 - rejestr programów komputerowych

REJESTR PROGRAMÓW KOMPUTEROWYCH ZAWIERAJĄCYCH DANE OSOBOWE

URZĄD MIEJSKI W DOBREJ

Lp.	Nazwa programu	Miejsce przechowywania	Imię i nazwisko użytkownika	Uwagi

BURMISTRZ
DOBREJ
Andrzej Piątkowski