Zarządzenie Nr 0050.103.2020
Wójta Gminy Słubice
z dnia 8 września 2020 r.

w sprawie: wprowadzenia polityki bezpieczeństwa i ochrony danych osobowych w Urzędzie Gminy Słubice.

Na podstawie art. 31 oraz art. 33 ust. 1 ustawy z dnia 8 marca 1990 r. roku o samorządzie gminnym (Dz. U. z 2020 r. poz. 713) w związku z art. 24 ust. 2 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. U. UE.L nr 119.1 (Dz. U.UE L z dnia 4 maja 2016 r.), zarządza się, co następuje

Rozdział 1

Postanowienia ogólne

§ 1. Zarządzenie określa politykę bezpieczeństwa i ochrony danych osobowych przetwarzanych w Urzędzie Gminy Słubice, zwaną dalej „Polityką".

§ 2. Celem wdrożenia niniejszej Polityki jest wprowadzenie spójnych zasad zachowania bezpieczeństwa danych osobowych w Urzędzie Gminy Słubice, zapewnienie należytej ochrony danych osobowych będących w zasobach administratora danych, w szczególności adekwatnej do zagrożeń i kategorii danych osobowych objętych ochroną oraz uzyskanie optymalnego dla działalności Urzędu i zgodnego z wymogami obowiązujących aktów prawnych, sposobu przetwarzania informacji zawierających dane osobowe.

§ 3. Ochrona danych osobowych realizowana jest poprzez zabezpieczenia fizyczne, organizacyjne, stosowane oprogramowanie systemowe i oprogramowanie użytkowe oraz upoważnianie osób do przetwarzania danych, proporcjonalne i adekwatne do ryzyka naruszenia bezpieczeństwa danych osobowych, przetwarzanych w ramach prowadzonej działalności.

§ 4. Ilekroć w Polityce mowa o:

1. Administratorze – należy przez to rozumieć Wójta Gminy Słubice;
2. danych osobowych – należy przez to rozumieć wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej ("osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
3. IOD – należy przez to rozumieć Inspektora Ochrony Danych – osobę wyznaczoną przez Administratora, powołaną do monitorowania i kontrolowania zasad bezpieczeństwa i ochrony danych osobowych przetwarzanych w urzędzie;

4. organie nadzorczym – należy przez to rozumieć Prezesa Urzędu Ochrony Danych Osobowych;

5. podmiocie przetwarzającym – należy przez to rozumieć osobę fizyczną, prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora na podstawie umowy powierzenia przetwarzania danych osobowych lub innego instrumentu prawnego;

6. RCPD – należy przez to rozumieć rejestr czynności przetwarzania danych osobowych w urzędzie;

7. RODO - należy przez to rozumieć rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119, s. 1);

8. upoważnieniu – należy przez to rozumieć nadawane przez Administratora wskazujące z imienia i nazwiska osobę, która ma prawo przetwarzać dane w zakresie wskazanym w tym oświadczeniu;

9. ustawie – należy przez to rozumieć ustawę z dnia z dnia 10 maja 2018 r. o ochronie danych osobowych;

10. urzędzie- należy przez to rozumieć Urząd Gminy Słubice.

Rozdział 2

Warunki i zasady przetwarzania danych osobowych

§ 5.1. Przetwarzanie danych osobowych w urzędzie może odbywać się wyłącznie w celu realizacji zadań wynikających bezpośrednio z przepisów prawa oraz celów statutowych i regulaminowych, w przypadkach, gdy spełniony jest co najmniej jeden z warunków wymienionych w art. 6 ust. 1 lub art. 9 ust. 2 RODO.

2. Przetwarzanie odbywa się w oparciu o zasadę legalizmu co oznacza, iż ma to miejsce wyłącznie w przypadku istnienia stosownej podstawy prawnej oraz zgodnie z prawem.

§ 6. Dane osobowe przetwarzane są w urzędzie w warunkach zapewnienia ich:

1) poufności – informacje nie są udostępniane lub ujawniane nieupoważnionym osobom, podmiotom i procesom;

2) integralności – dane nie zostają zmienione lub zniszczone w sposób nieautoryzowany;

3) dostępności – istnieje możliwość wykorzystania ich na żądanie, w założonym czasie, przez autoryzowany podmiot;

4) przejrzystości -w sposób przejrzysty dla osoby, której dane dotyczą;

5) rozliczalności – administrator działa w oparciu o obowiązujące przepisy prawa i musi być w stanie wykazać ich przestrzeganie;

6) autentyczności – zapewnienie, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana;

7) czasowości – przetwarzanie odbywa się w czasie nie dłuższym niż istnieje potrzeba ich przetwarzania;

8) minimalizacji – przetwarzanie odbywa się w konkretnych i aktualnych celach;

10) adekwatności – przetwarzanie odbywa się wyłącznie w niezbędnym zakresie;

11) bezpieczeństwa – w trakcie przetwarzania niezbędne jest zapewnienie danym bezpieczeństwa przy użyciu odpowiednich środków.

§ 7.1. Dane osobowe, które nie są przydatne lub upłynął termin ich przetwarzania są usuwane.

2. Dane osobowe, których zakres uległ ograniczeniu są pseudanimizowane.

§ 8. Przetwarzanie danych osobowych w urzędzie odbywa się na podstawie upoważnienia nadanego przez Administratora lub podmiot przetwarzający, zgodnie z zakresem upoważnienia, na podstawie umowy powierzenia, albo bezpośrednio na podstawie przepisu prawa lub innego instrumentu prawnego.

§ 9. Upoważnienie, o którym mowa w § 8, nadawane jest po odbyciu przez osobę, która ma je otrzymać, szkolenia z zakresu ochrony danych osobowych oraz złożeniu przez nią oświadczenia o zachowaniu w tajemnicy informacji w zakresie przetwarzanych danych.

§ 10. Upoważnienie, o którym mowa w § 8, nadawane jest w zakresie uwzględniającym rodzaj zadań realizowanych przez osobę upoważnianą.

§ 11. Dostęp do systemów informatycznych urzędu, w których przetwarzane są dane osobowe, mogą mieć wyłącznie osoby:

1) posiadające aktualne upoważnienie do przetwarzania danych osobowych;

2) z którymi zawarto porozumienie lub umowę cywilnoprawną na powierzenie przetwarzania danych osobowych;

3) których uprawnienie do przetwarzania danych osobowych wynika bezpośrednio z przepisów prawa.

Rozdział 3

Podmioty w systemie ochrony danych osobowych

Dział I

Administrator danych osobowych

§ 12.1. Administrator dokłada należytej staranności w celu ochrony interesów osób, których dane osobowe dotyczą, w szczególności jest obowiązany zapewnić, aby dane: były przetwarzane zgodnie z prawem, zbierane dla oznaczonych celów, merytorycznie poprawne i adekwatne do celów w jakich są zbierane, przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą oraz aby zapewniona była legalność, bezpieczeństwo, prawa jednostki i rozliczalność danych.

2. Administrator w szczególności:

1) podejmuje decyzje o celach i środkach przetwarzania danych osobowych;

2) wdraża i stosuje środki techniczne i organizacyjne zapewniające ochronę danych osobowych odpowiednią do zagrożeń oraz kategorii przetwarzanych danych;

3) zapewnia system i sprzęt informatyczny umożliwiający niezawodne i bezpieczne przetwarzanie danych;

4) zabezpiecza posiadane dane przed ich udostępnieniem, zmianą, utratą, uszkodzeniem, zniszczeniem lub przetwarzaniem przez osobę nieupoważnioną;

5) wyznacza IOD i zawiadamia o tym fakcie organ nadzorczy;

6) dopuszcza do przetwarzania danych osobowych wyłącznie osoby posiadające upoważnienie do przetwarzania danych osobowych;

7) zapoznaje z przepisami o ochronie danych osobowych każdą osobę upoważnioną do przetwarzania danych osobowych;

8) prowadzi rejestr osób upoważnionych, rejestr umów powierzenia przetwarzania danych osobowych, rejestr udostępnienia danych osobowych, rejestr naruszeń;

9) należycie i terminowo udziela informacji na wniosek osób, których dane są przetwarzane i które zwróciły się z wnioskiem o udzielenie informacji zgodnie z RODO;

10) podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia przetwarzanych danych;

11) przeprowadza ocenę skutków planowanych operacji przetwarzania danych osobowych po konsultacji z IOD;

12) prowadzi RCPD i rejestr kategorii czynności przetwarzania.

Dział II

Inspektor Ochrony Danych

§ 13.1. Inspektor ochrony danych jest wyznaczany przez Administratora na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, o których mowa w art. 39 RODO.

2. IOD wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

3. IOD bezpośrednio podlega Administratorowi.

4. IOD jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań;

5. IOD może wykonywać inne zadania i obowiązki. Administrator zapewnia, by takie zadania i obowiązki nie powodowały konfliktu interesów.

§ 14. Do zadań IOD należy w szczególności:

1) informowanie administratora oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;

2) nadzorowanie i monitorowanie przestrzegania RODO, innych przepisów Unii lub państw członkowskich o ochronie danych oraz Polityki;
3) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie ich;
4) przyjmowanie zgłoszeń naruszenia bezpieczeństwa przetwarzania danych osobowych;
5) prowadzenie szkoleń z zakresu ochrony danych osobowych;
6) współpraca z Prezesem Urzędu Ochrony Danych Osobowych;
7) pełnienie funkcji punktu kontaktowego dla Prezesa Urzędu Ochrony Danych Osobowych w kwestiach związanych z przetwarzaniem danych osobowych, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

Dział III

Administrator Systemów Informatycznych

§ 15.1. Administrator Systemów Informatycznych (ASI) jest wyznaczany przez Administratora na podstawie kwalifikacji zawodowych.

2. ASI wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania
3. ASI bezpośrednio podlega Administratorowi.
4. ASI jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań
5. ASI może wykonywać inne zadania i obowiązki. Administrator zapewnia, by takie zadania i obowiązki nie powodowały konfliktu interesów.
6. Do zadań ASI należy w szczególności dbanie o bezpieczeństwo danych przetwarzanych w systemie informatycznym oraz za właściwe funkcjonowanie systemu informatycznego.

Rozdział 4

Bezpieczeństwo danych osobowych

§ **16**.1. Zbiory danych osobowych są chronione w sposób zapewniający zabezpieczenie przetwarzanych danych osobowych w systemach informatycznych i na nośnikach informacji, przed utratą poufności, integralności, dostępności i rozliczalności tych danych.
2. Systemy informatyczne, służące do przetwarzania danych osobowych, muszą spełniać wymogi wynikające z obowiązujących aktów prawnych regulujących zasady gromadzenia i przetwarzania danych osobowych.
3. Kopie bezpieczeństwa oraz dokumenty papierowe zawierające dane osobowe przechowuje się w warunkach uniemożliwiających dostęp do nich osobom nieuprawnionym.

§ 17. Administrator regularne testuje, mierzy i dokonuje oceny skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych osobowych.

§ 18.1. Do zdarzeń zagrażających bezpieczeństwu danych osobowych należą:

a) próby naruszenia ochrony danych:

– z zewnątrz - włamania do systemu, podsłuch, kradzież danych,

– z wewnątrz - nieumyślna lub celowa modyfikacja danych, kradzież danych;

b) złośliwe oprogramowanie;

c) awarie sprzętu lub uszkodzenie oprogramowania powodujące utratę lub uszkodzenie danych;

d) zabór sprzętu lub nośników z ważnymi danymi;

e) inne skutkujące utratą danych osobowych, bądź wejściem w ich posiadanie osób nieuprawnionych.

2. W przypadku powzięcia wiadomości o zdarzeniu zagrażającym bezpieczeństwu danych osobowych lub podejrzeniu jego wystąpienia pracownik urzędu zobowiązany jest poinformować IOD oraz swojego bezpośredniego przełożonego.

3. Zgłoszenie, o którym mowa w ust. 2 powinno zawierać:

1) imię i nazwisko zgłaszającego;

2) określenie sytuacji i czasu w jakim doszło do zdarzenia, o którym mowa w ust. 1;

3) przekazanie istotnych informacji mogących wskazywać przyczynę naruszenia;

4) wskazanie jakie kroki zostały podjęte w celu przywrócenia bezpieczeństwa dalszego przetwarzania danych osobowych.

4. IOD oraz bezpośredni przełożony osoby zgłaszającej zdarzenie zagrażające bezpieczeństwu informacji jest zobowiązany do niezwłocznego powiadomienia Administratora.

5. IOD niezwłocznie wszczyna postępowanie wyjaśniające i podejmuje wszystkie czynności konieczne w celu ustalenia:

a) czasu wystąpienia naruszenia, zakresu, przyczyn, skutków, szkód;

b) osób odpowiedzialnych za naruszenie;

c) opracowuje pisemny raport z przeprowadzonego postępowania zawierający wnioski na przyszłość i przedkłada go Administratorowi.

6. Ponadto, w przypadku naruszenia ochrony danych osobowych, IOD:

a) zawiadamia osobę, której dane osobowe przetwarzane przez Administratora zostały naruszone, o każdym przypadku naruszenia jej danych osobowych przetwarzanych przez Administratora w stopniu skutkującym możliwością zaistnienia wysokiego ryzyka naruszenia praw lub wolności tej osoby fizycznej, chyba że przepisy obowiązującego prawa nie obligują IOD do dokonania takiego zawiadomienia;

b) w przypadkach przewidzianych przepisami prawa, dokonuje zgłoszenia naruszenia ochrony danych osobowych organowi nadzorczemu oraz współpracuje z nim w toku wszczętego postępowania;

c) współpracuje z organem nadzorczym we wszelkich prowadzonych przez niego postępowaniach związanych z naruszeniem ochrony danych osobowych.

Rozdział 5

Przetwarzanie danych osobowych

§ 19.1. Dane osobowe przetwarzane w urzędzie mogą być pozyskiwane bezpośrednio od osób, których te dane dotyczą. Administrator podczas pozyskiwania tych danych podaje informacje, wynikające z obowiązku informacyjnego, o którym mowa w § 20 ust. 1.

2.Jeżeli dane osobowe są zbierane nie od osoby, której te dane dotyczą, należy ustalić, że istnieje podstawa prawna przetwarzania tych danych oraz spełnić obowiązek informacyjny o którym mowa w § 20 ust. 1.

§ 20.1. W przypadku, gdy przetwarzanie danych osobowych odbywa się na podstawie zgody osoby której dane dotyczą, Administrator zobowiązany jest do jej uzyskania przed rozpoczęciem przetwarzania tych danych.

2. Zgoda, o której mowa w ust. 1, musi być konkretna, wyraźna, udzielona świadomie i dobrowolnie, a jej uzyskanie poprzedzone realizacją obowiązku informacyjnego.

3. Administrator dopuszcza wprowadzanie przez pracowników urzędu i innych użytkowników danych osobowych prywatnych do użytkowanych przez nich komputerów i innych urządzeń wyłącznie w przypadku uprzedniego wyrażenia przez te osoby zgody na przetwarzanie tych danych.

4. Osoba, której dane dotyczą, musi zostać poinformowana o prawie wycofania w każdym czasie zgody, a wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem.

§ 21.1. Administrator oraz osoby pozyskujące dane osobowe w urzędzie odpowiadają za zgodne z przepisami realizowanie obowiązku informacyjnego, o którym mowa w art. 13 lub 14 RODO.

2. W przypadku dalszego przetwarzania danych osobowych, w celu innym niż ten w którym dane zostały zebrane, Administrator realizuje obowiązek informacyjny.

3. Administrator nie realizuje obowiązku informacyjnego, o którym mowa w art. 13 ust. 3 i art. 14 ust. 1, 2 i 4 RODO, jeżeli zmiana celu przetwarzania, służy realizacji zadania publicznego i niespełnienie obowiązku informacyjnego jest zgodne z art. 3 i 4 ustawy.

§ 22.1. Przetwarzanie szczególnych kategorii danych osobowych jest dopuszczalne jedynie na zasadach określonych w art. 9 RODO.

2. Administrator jest zobowiązany do identyfikowania przypadków, w których przetwarza lub może przetwarzać dane osobowe szczególnych kategorii oraz stosowania mechanizmów zapewnienia zgodności z prawem ich przetwarzania.

§ 23.1. Osoby upoważnione do przetwarzania danych osobowych mogą przetwarzać dane tylko w wyznaczonych do tego miejscach poprzez odpowiednio zabezpieczony sprzęt informatyczny.

2. Przetwarzanie danych osobowych poza obszarem urzędu odbywa się wyłącznie za zgodą Administratora.

3. Wynoszenie nośników danych osobowych może mieć miejsce wyłącznie pod warunkiem zabezpieczenia ich przed nieuprawnionym udostępnieniem, kradzieżą, utratą lub zniszczeniem.

§ 24. Administrator prowadzi RCPD i rejestr kategorii czynności przetwarzania, które są na bieżąco aktualizowane.

Rozdział 6

Prawa osób, których dane dotyczą

§ 25.1. Każdej osobie przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych osobowych przetwarzanych w urzędzie.

2. Na wniosek osoby, której dane dotyczą, Administrator zapewnia możliwości zrealizowania przysługujących jej praw określonych w art. 15-22 RODO.

3. Administrator prowadzi rejestr wniosków, o których mowa w ust. 2.

Rozdział 7

Powierzenie przetwarzania danych osobowych i udostępnienie danych osobowych

§ 26.1. Administrator może powierzyć przetwarzanie danych osobowych innemu podmiotowi, który zapewnia wdrożenie odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi przepisów prawa i chroniło prawa osób, których dane dotyczą.

2. Podmiot, któremu powierzono przetwarzanie danych osobowych, może przetwarzać te dane wyłącznie w zakresie i celu przewidzianym w umowie lub innym instrumencie prawnym, o którym mowa w art. 28 ust. 3 RODO, oraz zgodnie z określonymi tam zasadami przetwarzania i zabezpieczeniami.

3. Umowy powierzenia przetwarzania danych osobowych oraz inne instrumenty prawne, na podstawie których dokonano powierzenia przetwarzania danych podlegają ewidencji w rejestrze umów powierzenia przetwarzania danych osobowych.

§ 27.1. Administrator może udostępnić dane osobowe innemu administratorowi, jeżeli udostępnienie następuje na mocy przepisu prawa lub zgody osoby, której dane dotyczą.

2. Administrator prowadzi rejestr udostępniania danych osobowych.

Rozdział 8

Przekazywanie danych do państwa trzeciego

§ 28. Administrator nie będzie przekazywał danych do państwa trzeciego, poza sytuacjami w których następuje to na wniosek podmiotów takich jak sądy, urzędy, organy ścigania lub osoby, której dane dotyczą.

Rozdział 9

Analiza ryzyka utraty bezpieczeństwa danych osobowych

§ 29.1. Administrator przeprowadza analizę ryzyka utraty bezpieczeństwa danych osobowych dla czynności przetwarzania danych osobowych, której głównym celem jest wyznaczenie kierunków działania kierownictwa oraz priorytetów zarządzania ryzykami i zabezpieczeniami.

2. Analiza, o której mowa w ust. 1, przeprowadzana jest:

1) przed rozpoczęciem przetwarzania danych osobowych dla planowanych czynności przetwarzania danych osobowych;

2) w trakcie przetwarzania danych osobowych:

a) w każdej sytuacji zmiany warunków, w jakich funkcjonuje Administrator, mającej wpływ na poziom ryzyk odnoszących się do celów przetwarzania ujętych w rejestrze czynności przetwarzania oraz rejestrze kategorii czynności przetwarzania,

b) do dnia 30 czerwca każdego roku kalendarzowego.

Rozdział 10

Postanowienia końcowe

§ 30. 1. Niniejsza Polityka obowiązuje wszystkich pracowników urzędu.
2. Polityka obowiązuje od dnia jej wprowadzenia w życie w sposób przyjęty w urzędzie. Wszelkie zmiany Polityki obowiązują od dnia ich wprowadzenia w życie w sposób przyjęty w urzędzie.
3. Każdy kto przetwarza dane posiadane przez urząd zobowiązany jest do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Polityce.
4. W sprawach nieuregulowanych w niniejszej Polityce mają zastosowanie przepisy powszechnie obowiązującego prawa, w tym w szczególności przepisy ustawy oraz RODO.

Ustala się wykaz załączników do Polityki:

1. Wzór oświadczenia pracownika o zachowaniu poufności - zał. Nr 1
2. Wykaz środków fizycznych technicznych i organizacyjnych stosowanych przez urząd w celu realizacji Polityki - zał. Nr 2
3. Wykaz budynków i pomieszczeń, w których przetwarzane są dane osobowe - zał. Nr 3
4. Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych - zał. Nr 4
5. Instrukcja zarządzania systemami informatycznymi – zał. Nr 5

Wójt
mgr Jacek Kozłowski

Załącznik Nr 1do Zarządzenia nr 0050.103.2020 Wójta Gminy Słubice z dnia 8 września 2020r.

.....
imię i nazwisko

.....
stanowisko

OŚWIADCZENIE O ZACHOWANIU POUFNOŚCI

Niniejszym oświadczam, że zapoznałam/em się z przepisami dotyczącymi ochrony danych osobowych, w tym z rozporządzeniem 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 (ogólne rozporządzenie o ochronie danych osobowych (Dz. Urz. UE.L. 2016.119/1) oraz ustawą z dnia z dnia 10 maja 2018r. o ochronie danych osobowych (Dz.U. z 2018r., poz.1000 ze zm.).

Zobowiązuję się do zachowania w tajemnicy danych osobowych przetwarzanych w Urzędzie Gminy Słubice oraz sposobu ich zabezpieczenia również po ustaniu zatrudnienia w Urzędzie Gminy Słubice lub zakończeniu realizacji powierzonych zadań.

Przyjmuję do wiadomości, że:

1) w związku ze złożeniem niniejszego oświadczenia i nadaniem mi upoważnienia do przetwarzania danych osobowych wraz z poleceniem ich przetwarzania, moje działania w systemie informatycznym Urzędu Gminy Słubice mogą być na bieżąco monitorowane oraz w całości lub części rejestrowane;
2) postępowanie sprzeczne z niniejszym oświadczeniem może być uznane za naruszenie obowiązków pracowniczych w rozumieniu Kodeksu pracy.

.....
(czytelny podpis osoby składającej oświadczenie)

Załącznik nr 2 do Zarządzenie Wójta Gminy Słubice Nr 0050.103.2020 z dnia 8 września 2020 r.

WYKAZ ŚRODKÓW FIZYCZNYCH, TECHNICZNYCH I ORGANIZACYJNYCH niezbędnych dla zapewnienia integralności, poufności oraz rozliczalności przetwarzania danych osobowych w Urzędzie Gminy Słubice.

1. Wprowadzone środki fizyczne.
1. 2. 3. 4. 5. 6. 7. 8. 9. 10. 11. 12.
2. Wprowadzone środki techniczne.
1. 2. 3. 4. 5. 6. 7. 8. 9. 10. 11. 12.
3. Wprowadzone środki organizacyjne.
1. 2. 3. 4. 5. 6. 7. 8. 9. 10. 11. 12.

Załącznik Nr 3 do Zarządzenia Wójta Gminy Słubice Nr 0050.103.2020 z dnia 8 września 2020 r.

Wykaz budynków i pomieszczeń, w których przetwarzane są dane osobowe W Urzędzie Gminy Słubice

L.p.	Adres	Nr pokoju lub/i nazwa działu/pomieszczenia
1	Urząd Gminy Słubice, ul. Płocka 32, 09-533 Słubice	
2	Urząd Gminy Słubice, ul. Płocka 32, 09-533 Słubice	
3	Urząd Gminy Słubice, ul. Płocka 32, 09-533 Słubice	
4	Urząd Gminy Słubice, ul. Płocka 32, 09-533 Słubice	
5	Urząd Gminy Słubice, ul. Płocka 32, 09-533 Słubice	
6	Urząd Gminy Słubice, ul. Płocka 32, 09-533 Słubice	
7	Urząd Gminy Słubice, ul. Płocka 32, 09-533 Słubice	
8	Urząd Gminy Słubice, ul. Płocka 32, 09-533 Słubice	
9	Urząd Gminy Słubice, ul. Płocka 32, 09-533 Słubice	
10	Urząd Gminy Słubice, ul. Płocka 32, 09-533 Słubice	
11	Urząd Gminy Słubice, ul. Płocka 32, 09-533 Słubice	
12	Urząd Gminy Słubice, ul. Płocka 32, 09-533 Słubice	
13	Urząd Gminy Słubice, ul. Płocka 32, 09-533 Słubice	
14	Urząd Gminy Słubice, ul. Płocka 32, 09-533 Słubice	
15	Urząd Gminy Słubice, ul. Płocka 32, 09-533 Słubice	
16	Urząd Gminy Słubice, ul. Płocka 32, 09-533 Słubice	
17	Urząd Gminy Słubice, ul. Płocka 32, 09-533 Słubice	
18	Urząd Gminy Słubice, ul. Płocka 32, 09-533 Słubice	
19	Urząd Gminy Słubice, ul. Płocka 32, 09-533 Słubice	

INSTRUKCJA POSTĘPOWANIA W PRZYPADKU NARUSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

§1

Celem instrukcji jest określenie sposobu postępowania gdy:

1. Stwierdzono naruszenie zabezpieczeń danych osobowych.

2. W przypadku danych przetwarzanych w formie tradycyjnej stan pomieszczeń, szaf, okien, drzwi, dokumentów lub inne zaobserwowane symptomy mogą wskazywać na naruszenie bezpieczeństwa danych osobowych.

3. W przypadku danych przetwarzanych w formie elektronicznej stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu, jakość komunikacji lub inne zaobserwowane symptomy mogą wskazywać na naruszenie bezpieczeństwa danych osobowych.

§2

Instrukcja określa zasady postępowania wszystkich osób zatrudnionych przy przetwarzaniu danych osobowych w przypadku naruszenia bezpieczeństwa tych danych.

§3

Naruszeniem zabezpieczenia danych osobowych jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych osobowych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia lub usunięcia, a w szczególności:

a) nieautoryzowany dostęp do danych,

b) nieautoryzowane modyfikacje lub zniszczenie danych,

c) udostępnienie danych nieautoryzowanym podmiotom,

d) nielegalne ujawnienie danych,

e) pozyskiwanie danych z nielegalnych źródeł.

§4

1. W przypadku stwierdzenia naruszenia zabezpieczeń lub zaistnienia sytuacji, które mogą wskazywać na naruszenie zabezpieczenia danych osobowych, każdy pracownik zatrudniony przy przetwarzaniu danych osobowych w jest zobowiązany przerwać przetwarzanie danych osobowych i niezwłocznie zgłosić ten fakt bezpośredniemu przełożonemu oraz Inspektorowi Ochrony Danych , a następnie postępować stosownie do podjętej przez niego decyzji.

2. Zgłoszenie naruszenia zabezpieczeń danych osobowych powinno zawierać:

a) opisanie symptomów naruszenia zabezpieczeń danych osobowych,

b) określenie sytuacji i czasu w jakim stwierdzono naruszenie zabezpieczeń danych osobowych,

c) określenie wszelkich istotnych informacji mogących wskazywać na przyczynę naruszenia,

d) określenie znanych danej osobie sposobów zabezpieczenia systemu oraz wszelkich kroków podjętych po ujawnieniu zdarzenia.

§5

Inspektor Ochrony Danych lub inna upoważniona przez niego osoba podejmuje wszelkie działania mające na celu:

a) minimalizację negatywnych skutków zdarzenia,

b) wyjaśnienie okoliczności zdarzenia,

c) zabezpieczenie dowodów zdarzenia,

d) umożliwienie dalszego bezpiecznego przetwarzania danych.

§6

W celu realizacji zadań wynikających z niniejszej instrukcji Inspektor Ochrony Danych ma prawo do podejmowania wszelkich działań dopuszczonych przez prawo, a w szczególności:

a) żądania wyjaśnień od pracowników,

b) korzystania z pomocy konsultantów,

c) nakazania przerwania pracy, zwłaszcza w zakresie przetwarzania danych osobowych.

§7

Polecenia Inspektora Ochrony Danych lub innej upoważnionej przez niego osoby wydawane w celu realizacji zadań wynikających z niniejszej instrukcji są priorytetowe i winny być wykonywane przed innymi poleceniami, zapewniając ochronę danych osobowych.

§8

Odmowa udzielenia wyjaśnień lub współpracy z Inspektorem Ochrony Danych lub inną upoważnioną przez niego osobą traktowana będzie jako naruszenie obowiązków pracowniczych.

§9

Inspektor Ochrony Danych po zażegnaniu sytuacji naruszającej bezpieczeństwo danych osobowych opracowuje raport końcowy, w którym przedstawia przyczyny i skutki zdarzenia oraz wnioski, w tym kadrowe, ograniczające możliwość wystąpienia zdarzenia w przyszłości.

§10

Nieprzestrzeganie zasad postępowania określonych w niniejszej instrukcji stanowi naruszenie obowiązków pracowniczych i może być przyczyną odpowiedzialności dyscyplinarnej określonej w Kodeksie Pracy.

§11

Jeżeli skutkiem działania określonego w §10 jest ujawnienie informacji osobie nieupoważnionej, sprawca może zostać pociągnięty do odpowiedzialności karnej wynikającej z przepisów Kodeksu Karnego.

§12

Jeżeli skutkiem działania określonego w §10 jest szkoda, sprawca ponosi odpowiedzialność materialną na warunkach określonych w przepisach Kodeksu Pracy oraz Prawa Cywilnego.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

w Urzędzie Gminy Słubice

§ 1.

POSTANOWIENIA OGÓLNE

1. Instrukcja zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych w Urzędzie Gminy Słubice, zwaną dalej „Instrukcją, określa:

1) zasady, tryb postępowania i zalecenia Administratora Systemów Informatycznych, które należy stosować w trakcie przetwarzania danych osobowych w systemie informatycznym;
2) zasady dostępu użytkowników do systemu informatycznego w Urzędzie Gminy Słubice, w tym sposób przydziału haseł dla użytkowników i częstotliwość ich zmiany oraz osoby odpowiedzialne za te czynności, sposób rejestrowania i wyrejestrowywania użytkowników oraz osoby odpowiedzialne za te czynności,
3) zasady i procedury rozpoczynania i kończenia pracy,
4) zasady i częstotliwość tworzenia kopii bezpieczeństwa,
5) zasady korzystania i przechowywania elektronicznych nośników informacji oraz sporządzania wydruków,
6) sposoby zabezpieczenia danych w systemie informatycznym,
7) zasady korzystania z oprogramowania, Internetu, bankowości elektronicznej, poczty elektronicznej,
8) zasady dokonywania przeglądów i konserwacji systemu i zbioru danych,
9) zasady postępowania w przypadku naruszenia bezpieczeństwa systemu informatycznego w urzędzie.
2. Instrukcja została przyjęta w celu wykazania, że dane w systemie informatycznym Urzędu Gminy Słubice przetwarzane są w sposób zgodny z przepisami prawa w zakresie ochrony danych osobowych, bezpieczeństwa informatycznego, w tym zgodnie z zasadami rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej: RODO).

§ 2.

DEFINICJE

Terminom używanym w niniejszej Instrukcji nadaje się znaczenia określone w Polityce.

§ 3.

ZASADY DOSTĘPU UŻYTKOWNIKA DO SYSTEMU

1. Za bezpieczeństwo danych przetwarzanych w systemie informatycznym oraz za właściwe funkcjonowanie systemu informatycznego odpowiedzialny jest Administrator Systemów Informatycznych (ASI)

2. Do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania, mogą być dopuszczeni wyłącznie Użytkownicy.

3. Po upoważnieniu osoby do przetwarzania danych w systemie informatycznym Użytkownikowi zostaje jej nadany odrębny Identyfikator oraz Hasło. Z chwilą nadania Identyfikatora Użytkownik może uzyskać dostęp do systemu informatycznego w zakresie wynikającym z jego upoważnienia.

4. Dostęp do systemu informatycznego mają także inne podmioty tylko i wyłącznie w zakresie i na zasadach określonych w Umowach powierzenia przetwarzania danych osobowych pod nadzorem Administratora Systemów Informatycznych.

§ 4.

METODY I ŚRODKI UWIERZYTELNIANIA ORAZ ZARZĄDZANIE NIMI

1. W systemie informatycznym stosowane jest uwierzytelnianie na poziomie dostępu do systemu operacyjnego. Do uwierzytelnienia stosowane są Identyfikator oraz Hasło.

2. Identyfikator składa się z minimum sześciu znaków. W identyfikatorze pomija się polskie znaki diakrytyczne.

3. Identyfikator nowego użytkownika nie może być zmieniany, a po wyrejestrowaniu Użytkownika z systemu informatycznego nie może być przydzielony innej osobie.

4. Identyfikator przydzielony Użytkownikowi, który utracił uprawnienie dostępu do systemu informatycznego, winien zostać niezwłocznie zablokowany. W takim wypadku Administrator podejmuje również inne działania, które okażą się konieczne w celu zapobieżenia nieuprawnionemu dostępowi do systemu informatycznego oraz naruszeniu zasad ochrony danych.

5. Hasło powinno składać się z unikalnego zestawu co najmniej ośmiu znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.

6. Hasło nie może być identyczne z identyfikatorem użytkownika, ani z jego imieniem lub nazwiskiem.

7. Zabrania się użytkownikom systemu udostępniania swojego identyfikatora i hasła innym osobom. Hasła utrzymywane są w tajemnicy również po upływie ich ważności.

8. Hasła nie mogą być przechowywane w formie jawnej w żadnej postaci: elektronicznej lub tradycyjnej (pliki tekstowe, zapisy w skryptach logowania, makrach, zdefiniowane jako klawisze funkcyjne terminali, inne dowolne zapisy tradycyjne).

9. W przypadku przechowywania w formie niejawnej, hasła nie mogą być przechowywane szczególnie w miejscach, gdzie może dojść do nieautoryzowanego dostępu ze strony osób trzecich.

10. Hasła muszą być natychmiast zmienione jeśli istnieje podejrzenie, że zostały odkryte lub wiadomo, że znajdują się w posiadaniu osoby nieupoważnionej.

11. Zmiana Hasła Użytkownika powinna być automatycznie wymuszana oprogramowaniem.

12. Zabrania się używania Identyfikatora lub Hasła innego Użytkownika.

13. Użytkownicy odpowiedzialni są za administrowanie programem wygaszacza ekranu zabezpieczającym dostęp do komputera w momencie nieobecności na stanowisku pracy.

14. Wygaszacz musi być zabezpieczony hasłem, automatycznie uruchamiany po określonym czasie braku aktywności Użytkownika.

15. Użytkownicy odpowiadają również za utworzenie haseł na poziomie aplikacji i oprogramowania systemowego.

§ 5.

OBOWIĄZKI ZWIĄZANE Z ROZPOCZĘCIEM, ZAWIESZENIEM I ZAKOŃCZENIEM PRACY W SYSTEMIE INFORMATYCZNYM

1. Przed uruchomieniem komputera Użytkownik winien sprawdzić, czy nie zostało do niego podłączone żadne niezidentyfikowane urządzenie.

2. Przed przystąpieniem do pracy w systemie informatycznym, Użytkownik winien upewnić się, że spełnione są podstawowe warunki bezpieczeństwa wymagane przy przetwarzaniu danych w systemie informatycznym, a w szczególności ustawienie urządzenia odtwarzającego obraz ze stacji roboczej (np. monitora) w sposób uniemożliwiający osobom trzecim wgląd w dane.

3. Po uruchomieniu komputera Użytkownik dokonuje Uwierzytelnienia się przy pomocy Identyfikatora oraz Hasła.

4. Przy każdorazowym opuszczeniu stanowiska komputerowego Użytkownik powinien dopilnować, aby na ekranie nie były wyświetlane dane.

5. Wychodząc z pomieszczenia, w którym przetwarzane są dane z systemu informatycznego Użytkownik powinien sprawdzić czy zamknięte są okna i wejście do pomieszczenia.

6. Przy opuszczaniu stanowiska komputerowego Użytkownik zobowiązany jest ustawić wygaszacz ekranu.

7. Na każdym komputerze w ramach sieci lokalnej wygaszacz ekranu uruchamia się po 3 minut braku aktywności.

8. Po zakończeniu pracy w systemie informatycznym Użytkownik obowiązany jest wylogować się z tego systemu.

§ 6.

WYREJESTROWANIE UŻYTKOWNIKA

1. Wyrejestrowania użytkownika z systemu informatycznego dokonuje Administrator Systemów Informatycznych na wniosek kierownika komórki organizacyjnej.

2. Wyrejestrowanie, o którym mowa w ust. 1, może mieć charakter czasowy lub trwały.

3. Wyrejestrowanie następuje poprzez zablokowanie konta użytkownika.

4. Przyczyną zablokowania użytkownika z systemu informatycznego jest:

1) nieobecność w pracy trwająca dłużej niż 31 dni kalendarzowych,

2) zawieszenie w pełnieniu obowiązków służbowych,

3) zwolnienie z pełnienia obowiązków służbowych.

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

§ 7.

ZASADY I CZĘSTOTLIWOŚĆ TWORZENIA KOPII ZAPASOWYCH

1. Dla zabezpieczenia integralności danych Administrator Systemów Informatycznych wykonuje kopie zapasowe poprzez archiwizację wszystkich danych zapisanych w systemie informatycznym, w tym danych osobowych.

2. Kopie awaryjne tworzy się z następującą częstotliwością:

1) kopie systemu finansowo-księgowego – raz na dobę

2) kopie pozostałe - nie rzadziej niż raz na miesiąc.

3. Administrator Systemów Informatycznych przegląda okresowo kopie awaryjne i ocenia ich przydatność do odtworzenia zasobów systemu w przypadku jego awarii.

4. Administrator Systemów Informatycznych zabezpiecza nośniki z kopiami zapasowymi przed dostępem do nich osób nieupoważnionych oraz przed ich zniszczeniem

5. Zabrania się przechowywania kopii awaryjnych w pomieszczeniach przeznaczonych do przechowywania zbiorów danych pozostających w bieżącym użytkowaniu.

§ 8.

ZASADY KORZYSTANIA I PRZECHOWYWANIA ELEKTRONICZNYCH NOŚNIKÓW INFORMACJI ORAZ SPORZĄDZANIA WYDRUKÓW

1. Osoby użytkujące przenośne nośniki informatyczne, służące do przetwarzania danych osobowych, obowiązane są niezwłocznie informować Administratora Systemów Informatycznych o zakresie, rodzaju zbieranych danych osobowych oraz celu ich przetwarzania.

2. Użytkownicy zobowiązani są przechowywać wszelkie elektroniczne nośniki informacji, które nie są przeznaczone do udostępnienia, w warunkach uniemożliwiających dostęp do nich osobom nieuprawnionym. Nośniki te winny być przechowywane w zamkniętych szafkach znajdujących się w pomieszczeniach biurowych na terenie Urzędu Gminy.

3. Dane zapisane na elektronicznych nośnikach informacji mogą być usuwane albo poprzez fizyczne zniszczenie nośnika albo poprzez wielokrotny zapis nieistotnych informacji w obszarze zajmowany przez dane kasowane.

4. Użytkownicy nie są upoważnieni do wynoszenia elektronicznych nośników informacji, na których zapisane są Dane, z Urzędu, chyba że jest to uzasadnione celami Przetwarzania. O takiej sytuacji bezwzględnie musi być powiadomiony Administrator Systemów Informatycznych. W takim przypadku elektroniczne nośniki informacji muszą być zabezpieczone w sposób zapewniający poufność i integralność danych.

5. Administrator Systemów Informatycznych może żądać usunięcia danych, co do których zachodzi uzasadnione podejrzenie, że nie są przetwarzane zgodnie z zasadami określonymi w przepisach o ochronie danych osobowych.

6. Osoba użytkująca przenośny komputer, służący do przetwarzania danych osobowych, obowiązana jest zachować szczególną ostrożność podczas transportu i przechowywania tego komputera poza obszarem ochrony danych w celu zapobieżenia dostępowi do tych danych osobie niepowołanej.

7. Użytkownik sporządzający wydruki, które zawierają dane osobowe jest odpowiedzialny za zachowanie szczególnej ostrożności przy korzystaniu z nich, a zwłaszcza za zabezpieczenie ich przed dostępem osób nie posiadających imiennego upoważnienia oraz nieuprawnionych do wglądu.

8. Wydruki zawierające dane osobowe, które są przeznaczone do usunięcia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie.

§ 9.

ZABEZPIECZENIE DANYCH W SYSTEMIE INFORMATYCZNYM

1. Administrator Systemów Informatycznych stosuje zabezpieczenie danych poprzez ochronę systemu informatycznego przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawionego dostępu do systemu informatycznego oraz przed działaniami inicjowanymi z sieci zewnętrznej.

2. Administrator Systemów Informatycznych stosuje również fizyczne zabezpieczenie danych, które polega na tym, że:

a) jednostki komputerowe podłączone są pod zasilacze UPS;

b) ochrona serwera przed zanikiem zasilania polega na stosowaniu zasilacza zapasowego UPS;

c) ochrona przed utratą zgromadzonych danych polega na tworzeniu kopii zapasowych na zewnętrznym dysku sieciowym;

d) ochrona przed awarią podsystemu dyskowego, systemu operacyjnego oraz serwera polega na wykorzystywaniu macierzy dyskowych.

3. W celu zabezpieczenia przed nieautoryzowanym dostępem do baz danych Administratora Danych Osobowych poprzez sieć Internet Administrator Systemów Informatycznych stosuje:

a) firewall sprzętowy Stormshield

b) firewall programowy oraz oprogramowanie antywirusowe monitorujące próby włamania oraz skanujące pocztę elektroniczną;

c) blokowanie i filtrowanie niektórych usług;

d) monitorowanie przez system antywirusowy danych ściąganych z sieci Internet;

e) zabezpieczenie kluczami WPA2 elementów sieci bezprzewodowej.

4. Zabezpieczenie danych obejmuje:

a) stacje robocze – system antywirusowy oraz firewall

b) poczta e-mail – system antywirusowy

c) siec wewnętrzna - system antywirusowy oraz firewall

5. System informatyczny jest automatycznie skanowany przez program antywirusowy przynajmniej raz na 24 godziny

6. Do obowiązków Administratora Systemów Informatycznych należy aktualizacja oprogramowania służącego do sprawdzania w systemie obecności wirusów komputerowych.

7. Użytkownik jest uprawniony do dostępu do systemu informatycznego wyłącznie przy zastosowaniu komputera, na którym uruchomiony jest program antywirusowy z włączoną ochroną systemu plików w czasie rzeczywistym.

8. W przypadku wykrycia wirusa Użytkownik powinien:

a) usunąć wirusa z systemu przy wykorzystaniu programu antywirusowego,

b) zeskanować system informatyczny przy zastosowaniu programu antywirusowego.

9. Jeżeli operacja usunięcia wirusa się nie powiedzie Użytkownik powinien:

a) zakończyć pracę w systemie informatycznym,

b) odłączyć zainfekowany komputer od sieci lokalnej,

c) powiadomić Administratora Systemów Informatycznych lub Inspektora Ochrony Danych.

10. Komputery i inne urządzenia oraz elektroniczne nośniki informacji, na których zapisane są dane, przekazywane poza pomieszczenia biurowe Urzędu Gminy muszą być zabezpieczone w sposób zapewniający poufność i integralność danych.

11. Hasło umożliwiające dostęp do sieci bezprzewodowej jest udostępniane przez Administratora Systemów Informatycznych wyłącznie Użytkownikom.

§ 10.

ZASADY KORZYSTANIA Z OPROGRAMOWANIA

1. Użytkownik zobowiązany jest do korzystania wyłącznie z oprogramowania dopuszczonego do stosowania w Urzędzie Gminy.

2. Użytkownicy nie mają prawa do instalowania ani używania oprogramowania innego, niż przekazane lub udostępnione im przez Administratora Systemów Informatycznych. Zakaz dotyczy między innymi instalacji oprogramowania z zakupionych płyt CD, programów ściąganych ze stron internetowych, a także odpowiadania na samoczynnie pojawiające się reklamy internetowe.

§ 11.

ZASADY KORZYSTANIA Z INTERNETU

1. Dopuszcza się korzystanie przez pracowników ze stron Internetowych w celach służbowych, a także okazjonalnie w celach prywatnych. Podczas korzystania z sieci internetowych niedozwolone jest przeglądanie, a także ściąganie materiałów, których treści są prawnie zakazane, naruszają dobre obyczaje lub uznawane są za obraźliwe.

2. Od pracowników wymaga się także zachowania szczególnej ostrożności w przypadku żądania lub prośby podania kodów, PIN-ów, hasła, numerów kart płatniczych przez Internet, w szczególności tyczy się to żądania podania takich informacji przez rzekomy bank.

3. W zakresie dozwolonym przepisami prawa, Administrator zastrzega sobie prawo kontrolowania sposobu korzystania przez użytkownika z Internetu pod kątem wyżej opisanych zasad oraz ma prawo blokować dostęp do wybranych stron internetowych.

§ 12.

ZASADY KORZYSTANIA Z BANKOWOŚCI ELEKTRONICZNEJ

1. Użytkownicy, którzy w zakresie obowiązków maja za zadanie korzystania z bankowości elektronicznej, zobowiązani są do regularnej zmiany hasła oraz nieprzechowywania go w formie pisemnej wraz z loginem.

2. Zabrania się opuszczania stanowiska pracy bez wylogowania się i zamknięcia przeglądarki.

3. Użytkownik logujący się do bankowości elektronicznej nie powinien korzystać z nieznanych sieci bezprzewodowych.

4. W celu zalogowania się do systemu bankowości elektronicznej pracownik nie powinien wchodzić na stronę internetową banku za pośrednictwem linków znajdujących się w korespondencji elektronicznej.

§ 13.

ZASADY KORZYSTANIA Z POCZTY ELEKTRONICZNEJ

1. Użytkownik jest zobowiązany do korzystania z przyznanego mu adresu mailowego wyłącznie w celach służbowych.

2. Podczas przesyłania danych należy zachować szczególną ostrożność przy wpisywaniu adresu odbiorcy dokumentu. Zaleca się, aby użytkownik podczas przesyłania danych osobowych pocztą elektroniczną zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.

3. W przypadkach gdy wiadomość jest kierowana jednocześnie do kilku adresatów należy używać metody „Ukryte do wiadomości -UDW".

4. Administrator może poznawać treść wiadomości elektronicznych znajdujących się we wszystkich systemach internetowych Administratora, jeżeli zostały one wysłane lub odebrane przez Użytkowników

5. Zabronione jest otwieranie wiadomości e-mail pochodzących od nieznanego nadawcy bądź z podejrzanym tytułem (tzw. phishing e-mail).

6. Zabronione jest otwieranie linków bądź pobieranie plików zapisanych w wiadomości email od nieznanego nadawcy. Zabrania się także rozsyłania za pośrednictwem poczty elektronicznej „łańcuszków szczęścia", itp.

7. Do przesyłania danych przy połączeniach w sieci publicznej (Internet), z uwagi na przekazywane dane osobowe, powinny być wykorzystywane tylko kanały transmisji wykorzystywane przez autoryzowane programy wykorzystywane również w innych urzędach oraz instytucjach państwowych i w oparciu o przepisy prawne regulujące sposób wysyłania tych danych.

8. Użytkownicy powinni okresowo kasować niepotrzebne wiadomości (tj. spam, oferty handlowe).

9. Użytkownicy nie mają prawa korzystać z maila w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania.

§ 14.

PRZEGLĄDY I KONSERWACJE SYSTEMU INFORMATYCZNEGO

1. Doraźnych przeglądów i konserwacji systemu informatycznego dokonuje Administrator Systemów Informatycznych.

2. Urządzenia informatyczne służące do przetwarzania danych osobowych można przekazać do naprawy, do likwidacji dopiero po uprzednim uzyskaniu zgody Administratora Systemów Informatycznych.

3. Bardziej skomplikowane i szczegółowe przeglądy oraz konserwacje systemu informatycznego powinny być wykonywane przez profesjonalne podmioty w oparciu o umowy zawarte na piśmie, w tym umowy powierzenia przetwarzania danych osobowych.

4. Przy dokonywaniu przeglądów i konserwacji systemu informatycznego należy przestrzegać następujących zasad:

a) przed rozpoczęciem prac serwisowych dane znajdujące się w systemie informatycznym, powinny zostać zarchiwizowane lub

b) w inny zabezpieczone przed ich usunięciem lub zmianą,

c) prace serwisowe powinny być wykonywane w obecności Administratora Systemów Informatycznych,

d) prace serwisowe należy ewidencjonować w książce zawierającej informacje o rodzaju prac serwisowych, datach rozpoczęcia i zakończenia prac oraz osobach dokonujących prac serwisowych.

§ 15.

NARUSZENIE BEZPIECZEŃSTWA SYSTEMU INFORMATYCZNEGO

1. Każdy przypadek naruszenia ochrony danych osobowych, które mogą wskazywać na naruszenie bezpieczeństwa podlega zgłoszeniu do Administratora Systemów Informatycznych, a w szczególności:

1) naruszenia bezpieczeństwa systemu informatycznego,

2) stwierdzenia objawów (stanu urządzeń, sposobu działania programu lub jakości komunikacji w sieci).

2. Administratorowi Systemów Informatycznych zgłasza się w szczególności przypadki:

1) użytkowania stacji roboczej przez osobę nie będącą użytkownikiem systemu,

2) usiłowania logowania się do systemu (sieci) przez osobę nieuprawnioną,

3) usuwania, dodawania lub modyfikowania bez wiedzy i zgody użytkownika jego dokumentów (rekordów),

4) przebywania osób nieuprawnionych w obszarze, w którym przetwarzane są dane osobowe, w trakcie nieobecności osoby zatrudnionej przy przetwarzaniu tych danych i bez zgody Administratora Danych, pozostawiania bez nadzoru otwartych pomieszczeń, w których przetwarzane są dane osobowe,

5) udostępniania osobom nieuprawnionym stacji roboczej lub komputera przenośnego, służących do przetwarzania danych osobowych,

6) niezabezpieczenia hasłem dostępu do komputera służącego do przetwarzania danych osobowych,

7) przechowywania nośników informacji oraz wydruków z danymi osobowymi, nieprzeznaczonymi do udostępniania, w warunkach umożliwiających do nich dostęp osobom nieuprawnionym.

2. Obowiązek dokonania zgłoszenia, o którym mowa w ust 1, spoczywa na każdym użytkowniku, który powziął wiadomość o naruszeniu ochrony danych osobowych.

3. W przypadku naruszenia integralności bezpieczeństwa sieciowego, obowiązkiem Administratora Systemów Informatycznych jest natychmiastowe wstrzymanie udostępniania zasobów dla użytkowników i odłączenie serwerów od sieci.

4. Użytkownik sieci i Administrator Systemów Informatycznych w porozumieniu z Inspektorem Ochrony Danych Osobowych ustalają przyczyny naruszenia integralności bezpieczeństwa sieciowego.

5. Przywrócenie udostępniania zasobów użytkownikom może nastąpić dopiero po ustaleniu i usunięciu przyczyny naruszenia integralności bezpieczeństwa sieciowego.

§ 16.

PRZEPISY KOŃCOWE

W sprawach nieuregulowanych w niniejszej Instrukcji mają zastosowanie przepisy ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej: RODO), ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.