Zarządzenie Nr 0050.211.2018

Burmistrza Czarnego

z dnia 21 grudnia2018 roku

w sprawie: Jednolitej Analizy Kontrolnej Krajowych Ram Interoperacyjności przy przetwarzaniu danych osobowych zgodnie z ustawa o informatyzacji

Na podstawie art. 33 ust.1 i 3 ustawy o samorządzie gminnym z dnia 8 marca 1990 roku (Dz.U. 2018.994) art. 24 ust.1 i 2 oraz art. 32 ust.1 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, art 13 ust.1 i 2 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. 2018.1669 t.j.), Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. 2017.2247) oraz §4 pkt 5 w związku z § 3 ust. 1 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r., poz..100, poz. 1024) i ustawa z dnia 24 sierpnia 1991 roku o ochronie przeciwpożarowej (Dz. U. 2017, poz. 620).

§ 1

Wprowadzam w Gminie Czarne i jej jednostkach podległych jednolitą Analizę Kontrolną Interoperacyjności przy przetwarzaniu danych osobowych, której treść stanowi załącznik do niniejszego zarządzenia.

§ 2

Pracodawca zobowiązuje wszystkich pracowników do przestrzegania Jednolitej Analizy Kontrolnej Interoperacyjności przy przetwarzania danych osobowych pod groźbą konsekwencji służbowych, przewidzianych prawem.

§ 3

Wykonanie Zarządzenia powierza się Sekretarzowi Gminy Czarne.

§ 4

Zarządzenie wchodzi w życie z dniem ogłoszenia.

BURMISTRZ
mgr Piotr Zabrocki

Załącznik do Zarządzenia Nr 0050.211.2018
Burmistrza Czarnego
z dnia 21 grudnia 2018 roku

§ 1

1. Sprawnie działający system bezpieczeństwa informacji jest niezwykle istotny z uwagi na sensytywność przetwarzanych danych osobowych oraz sposób ich przetwarzania. Administrator Danych: **Burmistrza Czarnego** ma świadomość, iż zadaniem jego jest ochrona przetwarzanych danych osobowych tj. uniemożliwienie dostępu do ich treści osobom nieuprawnionym. Z uwagi na powyższe, Administrator Danych: Burmistrz Czarnego w celu wykonania sprawdzenia na jakim poziomie kształtuje się poziom ryzyka utraty danych osobowych, wdraża dokument o nazwie „Jednolita Analiza Kontrolna Krajowych Ram Interoperacyjności przy przetwarzaniu danych osobowych zgodnie w celu badania i obserwowania istniejącego środowiska przetwarzanych danych osobowych.
2. Jednolita analiza kontrolna Krajowych Ram Interoperacyjności została wprowadzona w oparciu o:
    1) ustawę o samorządzie gminnym z dnia 8 marca 1990 roku (Dz.U. 2018.994), ustawę z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. 2018.1669 t.j.), i ustawa z dnia 24 sierpnia 1991 roku o ochronie przeciwpożarowej (Dz. U. 2017, poz. 620).
    2) 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,
    Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. 2017.2247), Rozporządzenia Ministra Spraw Wewnętrznych i Administracji w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r., poz..100, poz. 1024).

§ 2

Bezpieczeństwo przetwarzanych lub przechowywanych informacji zawierające dane osobowe wymaga:

1) zapewnienia ochrony fizycznej stanowiska komputerowego przed nieuprawnionym dostępem;
2) ochrony nośników technicznych i wydruków dokumentów wytwarzanych przy pomocy sprzętu elektronicznego, w tym określenia zasad postępowania z nimi przed nieuprawnionym dostępem;
3) zabezpieczenia przed nieupoważnionym dostępem do danych osobowych znajdujących się w zasobach systemu informatycznego;
4) zapewnienia dostępności do danych osobowych znajdujących się na technicznych nośnikach informacji oraz w pamięci systemu informatycznego dla upoważnionych użytkowników;
5) zapewnienia możliwości kontroli dostępu do zasobów systemu informatycznego oraz wykonywanych na nim czynności;
6) zapewnienia możliwości kontroli nośników, na których przetwarzano lub przechowywano dane osobowe.

§ 3

Ilekroć w **„Jednolitej Analizie Kontrolnej Krajowych Ram Interoperacyjności przy przetwarzaniu danych osobowych"** jest mowa o:

1. **ANALIZIE RYZYKA** – systematyczne wykorzystanie informacji do zidentyfikowania źródeł i oszacowania ryzyka;
2. **SZACOWANIU RYZYKA** – proces oceny i analizy ryzyka;
3. **OCENIE RYZYKA** – proces porównania oszacowanego ryzyka z określonymi kryteriami w celu określenia znaczenia ryzyka;
4. **POSTĘPOWANIU Z RYZYKIEM** – wdrażanie środków modyfikujących ryzyko;
5. **ZARZĄDZANIU RYZYKIEM** – działania dotyczące kierowania i nadzorowania organizacją w odniesieniu do ryzyka;
6. **RYZYKU SZCZĄTKOWYM** – ryzyko pozostające po procesie postępowania z ryzykiem;
7. **AKCEPTOWANIU RYZYKA** – decyzja, aby zaakceptować ryzyko;
8. **BEZPIECZEŃSTWIE INFORMACJI** – zachowanie poufności, integralności i dostępności informacji; dodatkowo mogą być brane pod uwagę inne właściwości, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność;
9. **ZDARZENIU ZWIĄZANYM Z BEZPIECZEŃSTWEM INFORMACJI** – zdarzenie związane z bezpieczeństwem informacji jako określonym stanem systemu, usługi lub sieci, który wskazuje na możliwe naruszenie Polityki Bezpieczeństwa Informacji, błąd zabezpieczenia lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem;
10. **INCYDENCIE ZWIĄZANYM Z BEZPIECZEŃSTWEM INFORMACJI** – jest to pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, zagrażają bezpieczeństwu informacji;
11. **AKTYWACH** – wszystko, co przedstawia wartość ekonomiczną;
12. **ZAGROŻENIACH SYSTEMU** – to wszystkie niekorzystne czynniki mogące przyczynić się w trakcie przetwarzania danych osobowych do wystąpienia incydentu, mogącego mieć wpływ na ich ujawnienie bądź utratę;
13. **DOSTĘPNOŚCI** — należy przez to rozumieć właściwość określającą, że zasób systemu teleinformatycznego jest możliwy do wykorzystania na żądanie, w określonym czasie, przez podmiot uprawniony do pracy w systemie teleinformatycznym;
14. **INCYDENCIE BEZPIECZEŃSTWA TELEINFORMATYCZNEGO** — należy przez to rozumieć takie pojedyncze zdarzenie lub serię zdarzeń, związanych z bezpieczeństwem informacji niejawnych, które zagrażają ich poufności, dostępności lub integralności;
15. **INFORMATYCZNYM NOŚNIKU DANYCH** — należy przez to rozumieć materiał służący do zapisywania, przechowywania i odczytywania danych w postaci cyfrowej;
16. **INTEGRALNOŚCI** — należy przez to rozumieć właściwość określającą, że zasób systemu teleinformatycznego nie został zmodyfikowany w sposób nieuprawniony;
17. **OPROGRAMOWANIU ZŁOŚLIWYM** — należy przez to rozumieć oprogramowanie, którego celem jest przeprowadzenie nieuprawnionych lub szkodliwych działań w systemie teleinformatycznym;

18. **PODATNOŚCI** — należy przez to rozumieć słabość zasobu lub zabezpieczenia systemu teleinformatycznego, która może zostać wykorzystana przez zagrożenie;
19. **POŁĄCZENIU MIĘDZYSYSTEMOWYM** — należy przez to rozumieć techniczne albo organizacyjne połączenie dwóch lub więcej systemów teleinformatycznych, umożliwiające ich współpracę, a w szczególności wymianę danych;
20. **POUFNOŚCI** — należy przez to rozumieć właściwość określającą, że informacja nie jest ujawniana podmiotom do tego nieuprawnionym;
21. **PRZEKAZYWANIU INFORMACJI** — należy przez to rozumieć zarówno transmisję informacji, jak i przekazywanie informacji na informatycznych nośnikach danych, na których zostały utrwalone;
22. **TESTACH BEZPIECZEŃSTWA** — należy przez to rozumieć testy poprawności i skuteczności funkcjonowania zabezpieczeń w systemie teleinformatycznym;
23. **ZABEZPIECZENIU** — należy przez to rozumieć środki o charakterze fizycznym, technicznym lub organizacyjnym zmniejszające ryzyko;
24. **ZAGROŻENIU** — należy przez to rozumieć potencjalną przyczynę niepożądanego zdarzenia, które może wywołać szkodę w zasobach systemu teleinformatycznego;
25. **ZASOBACH SYSTEMU TELEINFORMATYCZNEGO** – należy przez to rozumieć informacje przetwarzane w systemie teleinformatycznym, jak również osoby, usługi, oprogramowanie, dane i sprzęt oraz inne elementy mające wpływ na bezpieczeństwo tych informacji;

§ 4

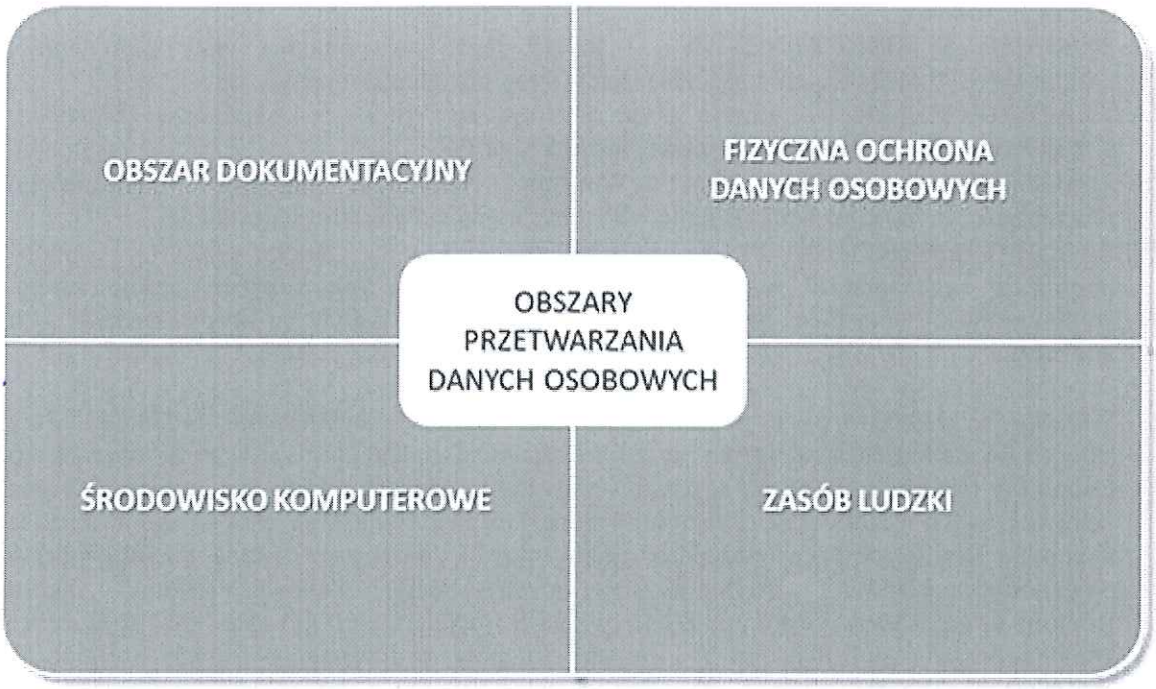
1. Skuteczność zastosowanych środków powinna podlegać cyklicznym badaniom. Przy stosowaniu zabezpieczeń powinno się też uwzględniać zmieniające się warunki oraz postęp techniczny (informatyczny), co może powodować konieczność zmiany czy modernizowania wprowadzonych wcześniej przez Administratora Danych systemów ochrony. Jednolita Analiza Kontrolna Krajowych Ram Interoperacyjności, określa środki zastosowane dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych. Jednolita Analiza Kontrolna Krajowych Ram Interoperacyjności odnosi się głównie do środowiska komputerowego, czyli jednego z czterech obszarów przetwarzania danych osobowych, natomiast nie można wykonać całościowej oceny systemu bezpieczeństwa informacji bez uwzględnienia pozostałych zakresów ochrony danych osobowych. Zarządzanie ryzykiem ma na celu zidentyfikowanie i oszacowanie ryzyka związanego z naruszeniem poufności, integralności czy dostępności danych osobowych. Obszary przetwarzania danych osobowych określa **Załącznik nr 1** Jednolitej Analizy Kontrolnej Krajowych Ram Interoperacyjności.
2. Zagrożenia występujące w systemach informatycznych, określa **Załącznik nr 2** Jednolitej Analizy Kontrolnej Krajowych Ram Interoperacyjności.
3. Podatność systemu na zagrożenia, określa **Załącznik nr 3** Jednolitej Analizy Kontrolnej krajowych Ram Interoperacyjności.
4. Jednolita Analiza Kontrolna Krajowych Ram Interoperacyjności – określenie poziomu ryzyka określona została w **Załączniku nr 4** Jednolitej Analizy Kontrolnej Krajowych Ram Interoperacyjności.
5. Wnioski i działania naprawcze, określa **Załącznik nr 5** Jednolitej Analizy Kontrolnej Krajowych Ram Interoperacyjności.
6. Plan postępowania z ryzykiem w związku z przeprowadzoną Jednolitą Analizą Kontrolną Krajowych Ram Interoperacyjności przy przetwarzaniu danych osobowych, określa **Załącznik nr 6** Jednolitej Analizy Kontrolnej krajowych Ram Interoperacyjności.
7. Pytania kontrolne oraz tabela szacowania ryzyka została określona w **Załączniku nr 7** Jednolitej Analizy Kontrolnej Krajowych Ram Interoperacyjności.

BURMISTRZ
mgr Piotr Zabrocki

.....
(Podpis Administratora Danych)

Załącznik Nr 1 Jednolitej Analizy Kontrolnej Krajowych Ram Interoperacyjności stanowiącej zalacznik do Zarządzenia Nr 0050.211.2018 Burmistrza Czarnego z dnia 21 grudnia 2018 r.

W ramach przetwarzania danych osobowych określamy co najmniej cztery obszary systemu bezpieczeństwa informacji (schemat poniżej).



1) **Fizyczna ochrona danych osobowych:** przykładowy katalog zabezpieczeń w ramach fizycznej ochrony danych osobowych:
    a) drzwi zwykłe (niewzmocnione, nie przeciwpożarowe),
    b) drzwi o podwyższonej odporności ogniowej w USC,
    c) drzwi o podwyższonej odporności na włamanie,
    d) zbiory w zamkniętych niemetalowych, metalowych szafach,
    e) kopie zapasowe zamknięte w szafach opisanych powyżej,
    f) pomieszczenia korytarzy wyposażone w gaśnicę.
2) **Środowisko komputerowe:** przykładowy katalog zabezpieczeń środowiska komputerowego:
    a) zastosowano urządzenia typu UPS, wydzielono sieć elektroenergetyczną,
    b) dostęp do danych osobowych, przetwarzanych w programie komputerowym bazodanowym, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą hasła,
    c) hasło – jego zmiana nie następuje rzadziej, niż co 30 dni, co najmniej 8 znaków – ma zawierać małe i wielkie litery oraz cyfry lub znaki specjalne,
    d) wdrożone zostały mechanizmy wymuszające okresową zmianę haseł,

e) zastosowano macierz dyskową,

f) jeżeli dostęp do danych przetwarzania w systemie informatycznym, mają co najmniej 2 osoby, wówczas każdy powinien mieć własny identyfikator,

g) stosuje się programy antywirusowe,

h) stosuje się wygaszacze ekranów komputerów,

i) monitory komputerów ustawione są w taki sposób, że uniemożliwia to dostęp osobom postronnym do danych osobowych ich nie dotyczących.

3) **Zasób ludzki:**

a) osoby przetwarzające dane osobowe zostały przeszkolone w zakresie działania systemu bezpieczeństwa informacji oraz zobowiązane do zachowania ich w tajemnicy,

b) osoby przetwarzające dane osobowe stosują się do powszechnie obowiązujących przepisów prawa w ramach bezpieczeństwa informacji,

c) Administrator Danych lub Inspektor Ochrony Danych przeprowadzają cykliczne spotkania z pracownikami.

BURMISTRZ
mgr Piotr Zabrocki

.....
(Podpis Administratora Danych)

Załącznik Nr 2 Jednolitej Analizy Kontrolnej Krajowych Ram Interoperacyjności stanowiącej załacznik do Zarządzenia Nr 0050.211.2018 Burmistrza Czarnego z dnia 21 grudnia 2018 r.

Zagrożenia występujące w systemach informatycznych

§ 1

W myśl Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), każdy Administrator Danych powinien zapewnić takie warunki pracy w systemie, aby cechował się on poufnością, integralnością i rozliczalnością.

§ 2

Każde zauważone zagrożenie związane z poufnością, integralnością lub rozliczalnością, powinno być niezwłocznie zgłoszone Administratorowi Danych bądź wyznaczonemu Inspektorowi Ochrony Danych.

§ 3

1. Poufność, to zapewnienie danym osobowym niemożności ich udostępniania nieupoważnionym osobom czy podmiotom.
2. Zapewnienie poufności wartości informacyjnych wynika z obowiązku wypełnienia nakładanych na Administratora Danych zadań, wynikających z przepisów prawa, ustaw, wraz z wszelkimi konsekwencjami organizacyjnymi i prawnymi.
3. Strategiczną częścią zabezpieczania danych w systemach informatycznych przed utratą poufności jest odpowiednio prowadzony system szkoleń dla pracowników merytorycznych mających dostęp do danych osobowych.
4. Na Inspektorze Ochrony Danych spoczywa obowiązek informowania Administratora Danych oraz pracowników, którzy przetwarzają dane osobowe o zadaniach, które nakłada na nich ogólne rozporządzenie ochrony danych i inne przepisy prawa.
5. Utrata poufności informacji o zasadach funkcjonowania systemów i sieci oraz mechanizmach zabezpieczeń jest niezwykle ważna oraz wymaga położenia nacisku na przestrzeganie procedur przez osoby sprawujące opiekę nad systemami i siecią.

§ 4

Zagrożenia, jakie można wyróżnić ze względu na utratę poufności w systemie informatycznym:

1. nieuprawniony dostęp do pomieszczenia, w którym przetwarzane są dane osobowe;
2. ujawnienie haseł dostępu do stanowiska komputerowego, na którym przetwarzane są dane osobowe;
3. nieuprawnione przeniesienie informacji zawierających dane osobowe na inny nośnik;
4. utrata nośnika zawierającego dane osobowe;
5. klęska żywiołowa, w wyniku której utracono poufność danych osobowych;
6. nieuprawnione wyniesienie danych osobowych zawartych na nośniku elektronicznym;
7. udostępnianie danych osobowych osobom nieupoważnionym;
8. wejście w posiadanie danych osobowych przez osobę nieupoważnioną;

9. pokonanie zabezpieczeń fizycznych lub programowych;
10. niekontrolowana obecność osób nieuprawnionych w obszarze przetwarzania danych osobowych;
11. niedyskrecja osób uprawnionych do przetwarzania danych osobowych;
12. nieuprawnione kopiowanie danych na nośniki informacji (CD, DVD, pendrive, itp.);
13. niekontrolowane wynoszenie poza obszar przetwarzania danych osobowych nośników informacji i komputerów przenośnych;
14. naprawy i konserwacje systemów lub sieci teleinformatycznej służących do przetwarzania danych osobowych przez osoby nieuprawnione do przetwarzania danych osobowych;
15. podsłuch lub podgląd danych osobowych;
16. elektromagnetyczna emisja ujawniająca;
17. podsłuch akustyczny i podsłuch emisji ujawniającego promieniowania elektromagnetycznego;
18. stosowanie korupcji oraz szantażu w celu wydobycia określonych informacji od wybranych pracowników firmy;
19. zagubienie dokumentów lub utrata przetwarzanych informacji.

§ 5

Skala identyfikacji skutków utraty zasobów dla atrybutu poufności danych osobowych.

WARTOŚĆ	SKUTKI
1	Niski skutek utraty poufności
<1 – 2,5≥	Średni skutek utraty poufności
<2,5 – 4>	Wysoki skutek utraty poufności
4	Całkowita utrata poufności

§ 6

1. Integralność to zapewnienie, aby wszelkie modyfikacje wykonywane w systemie informatycznym, w systemie jego katalogów oraz indywidualnych plikach posiadające w sobie dane osobowe były skutkiem rozważnych i zaplanowanych działań użytkowników systemu.
2. Integralność, to cecha zapewniająca, że dane nie zostały zmodyfikowane lub zniszczone w sposób nieautoryzowany.
3. Integralność danych dotyczy przede wszystkim wartości informacyjnych przetwarzanych w postaci elektronicznej. Dlatego tak ważne jest zachowanie integralności dla bezpieczeństwa systemu i sieci. Administrator Danych powinien objąć procedurami weryfikacji i rozliczania pracowników sprawujących opiekę nad systemami i siecią oraz wprowadzić bieżącą, regularną detekcję prób ingerencji do systemu informatycznego oraz wszelkie próby naruszenia jego struktury, ponieważ skutkiem takich działań jest uszkodzenie bazy danych i w rezultacie naruszenie zapisów ustawy.

§ 7

Zagrożenia, jakie można wyróżnić ze względu na utratę integralności przez system informatyczny:

1. nielegalny dostęp do danych osobowych, w tym do stanowiska komputerowego;
2. błędy, pomyłki;
3. brak mechanizmów uniemożliwiających skasowanie lub zmianę logów przez administratora lub innego użytkownika;
4. wadliwe działanie systemu operacyjnego;
5. brak w wykorzystywanych aplikacjach mechanizmów zapewniających integralność danych;
6. uszkodzenie, celowe lub przypadkowe systemu operacyjnego lub urządzeń sieciowych;
7. celowe lub przypadkowe uszkodzenie, zniszczenie lub nieuprawniona modyfikacja danych;
8. działanie złośliwego oprogramowania (wirusy);
9. pożar, zalanie, ekstremalna temperatura, itp.;
10. zagrożenia zewnętrzne (np. klęski żywiołowe, atak terrorystyczny).

§ 8

Skala identyfikacji skutków utraty zasobów dla atrybutu integralności danych osobowych.

WARTOŚĆ	SKUTKI
1	Niski skutek utraty integralności
<1 – 2,5≥	Średni skutek utraty integralności
<2,5 – 4>	Wysoki skutek utraty integralności
4	Bezwzględny skutek utraty integralności

§ 9

Rozliczalność to cecha zapewniająca działanie podmiotu przetwarzającego dane osobowe, która może być przypisana w sposób jednoznaczny tylko temu, jednemu podmiotowi.

§ 10

Zagrożenia, jakie można wyróżnić ze względu na utratę rozliczalności systemu informatycznego:

1. brak kontroli nad dokumentami wykonywanymi na stanowisku komputerowym w zakresie ich kopiowania i drukowania;
2. wyparcie się pracy na stanowisku komputerowym, gdzie przetwarza się dane osobowe;
3. wprowadzenie zmian w treści dokumentu zawierającego dane osobowe;
4. błędy oprogramowania lub sprzętu;
5. nieprzydzielenie użytkownikom indywidualnych identyfikatorów;
6. niewłaściwa administracja systemem informatycznym;
7. niewłaściwa konfiguracja systemu informatycznego;

8. zniszczenie lub sfałszowanie logów systemowych;
9. brak rejestracji udostępnienia danych osobowych;
10. podszywanie się pod innego użytkownika;
11. niespełnienie przez system wymagań ustawowych.

§ 11

Skala identyfikacji skutków utraty zasobów dla atrybutu rozliczalności danych osobowych.

WARTOŚĆ	SKUTKI
1	Niski skutek utraty rozliczalności
<1 – 2,5≥	Średni skutek utraty rozliczalności
<2,5 – 4>	Wysoki skutek utraty rozliczalności
4	Bezwzględny skutek utraty rozliczalności

§ 12

Dla systemów informatycznych szczególnie niebezpieczne są występujące zagrożenia stanowisk komputerowych, które występują przeważnie ze względu na ingerencję:

1. **SIŁY NATURY** (to zdarzenia niewynikające z działalności człowieka), mogą to być:
   1) uderzenie pioruna;
   2) pożar będący konsekwencją ww. uderzenia **pioruna;**
   3) starzenie się sprzętu;
   4) starzenie się nośników pamięci;
   5) smog, kurz;
   6) katastrofy budowlane;
   7) ulewny deszcz;
   8) huragan;
   9) ekstremalne temperatury, wilgotność;
   10) epidemia.
2. **LUDZI** (mogą to być pracownicy lub osoby z zewnątrz, które działają w sposób celowy lub przypadkowy), mogą to być:
   1) błędy i pomyłki użytkowników;
   2) błędy i pomyłki administratorów;
   3) błędy utrzymania systemu w poufności, integralności i rozliczalności;
   4) zaniedbania użytkowników przy przesyłaniu, udostępnianiu i kopiowaniu;

5) zagubienie nośnika zawierającego dane osobowe;

6) niewłaściwe zniszczenie nośnika;

7) nielegalne użycie oprogramowania;

8) choroba ważnych osób i nieuprawnione zastępstwo;

9) epidemia kadry i brak osób upoważnionych do dostępu;

10) podpalenie obiektu;

11) zalanie wodą;

12) katastrofa budowlana będąca konsekwencją przypadkowego działania człowieka;

13) zakłócenia elektromagnetyczne, radiotechniczne;

14) podłożenie i wybuch bomby, ładunku wybuchowego;

15) użycie broni;

16) zmiany napięcia w sieci;

17) utrata prądu;

18) zbieranie się ładunków elektrostatycznych;

19) niedobór pracowników;

20) defekty oprogramowania;

21) szpiegostwo;

22) terroryzm;

23) wandalizm;

24) destrukcja zbiorów i programów impulsem elektromagnetycznym;

25) kradzież;

26) włamanie do systemu;

27) wyłudzenie, fałszowanie dokumentów;

28) podszycie się pod uprawnionego użytkownika;

29) podsłuch;

30) użycie złośliwego oprogramowania;

31) wykorzystanie promieniowania ujawniającego.

BURMISTRZ
mgr Piotr Zabrocki

.....

(Podpis Administratora Danych)

Załącznik Nr 3 Jednolitej Analizy Kontrolnej Krajowych Ram Interoperacyjności stanowiącej załacznik do Zarządzenia Nr 0050.211.2018 Burmistrza Czarnego z dnia 21 grudnia 2018 r.

Podatność systemu na zagrożenia

§ 1

Podatność systemu na zagrożenia może wynikać z:

1. **Dostępności systemu wynikającego np. z braku ochrony fizycznej budynku lub znacznej liczby personelu, mającego potencjalnie dostęp do systemu oraz wiedzę, jak obsługiwać system.**

Fizyczna ochrona danych osobowych to jeden z podstawowych obszarów w zakresie przetwarzania danych osobowych. Osoba przetwarzająca dane osobowe bardzo często nie zdaje sobie sprawy, jak ważne jest przestrzeganie chociażby „zasady czystego biurka", która wielokrotnie jest marginalizowana i zwyczajnie nieprzestrzegana. Zazwyczaj nieświadomość pracowników w tej materii wiąże się z negatywnymi konsekwencjami dla podmiotu, np. kwestia złożenia skargi, której przedmiotem jest niedochowywanie należytej staranności w zakresie fizycznej ochrony danych osobowych. Proces wdrażania w placówce „kodeksu dobrych praktyk" w kontekście ochrony danych osobowych jest procesem długoletnim i dynamicznym, ale bezsprzecznie powinno się w pierwszej kolejności uwrażliwiać na fizyczną ochronę danych osobowych. Ponadto, tylko i wyłącznie osoby upoważnione do przetwarzania danych osobowych powinny posiadać wiedzę o tym, w jaki sposób obsługiwać system informatyczny, będący integralnym elementem placówki.

2. **Dostępności informacji znajdujących się w systemie za pośrednictwem połączeń zewnętrznych.**

System informatyczny w podmiocie powinien być odpowiednio zabezpieczony, również jeśli dostęp do niego jest możliwy za pośrednictwem połączeń zewnętrznych. Niezależnie od zastosowanych rozwiązań teletransmisyjnych, system ten powinien być „szczelny", to znaczy wystarczająco odporny na wszelkiego rodzaju zewnętrzne zagrożenia.

3. **Możliwości celowego wprowadzania luk w sprzęcie i oprogramowaniu lub wprowadzania wirusów komputerowych.**

Możność nieuprawnionego działania na sprzęcie, czy oprogramowaniu może być wynikiem zastosowanej manipulacji, podsłuchu czy podstawienia. Podsłuch polega na tym, że charakter poufności przekazywanych treści zostaje naruszony. Manipulacja z kolei, będzie działaniem, które ukierunkowane jest na uzyskanie dostępu do treści danych i nieuprawnioną ingerencję w nie. Natomiast podstawienie, polega między innymi na wprowadzeniu drugiej strony w błąd, co do swojej tożsamości, po to tylko, by uzyskać konkretne informacje. Kadra powinna być odpowiednio uwrażliwiona na otrzymywanie korespondencji mailowej, co do której zaistnieje podejrzenie, że została przesłana w celu wprowadzenia wirusa komputerowego.

4. **Możliwości awarii sprzętu lub oprogramowania ze względu na uszkodzenia, błędy projektowe lub umyślną interwencję.**

Sprzęt informatyczny powinien być cyklicznie odpowiednio serwisowany, tak by wyeliminować zagrożenia. Należy zaznaczyć, iż z firmą informatyczną zewnętrzną, nie podpisujemy upoważnienia do przetwarzania danych osobowych, ale umowę powierzenia danych osobowych.

5. **Przesyłania informacji przez niezabezpieczone łącza telekomunikacyjne**.

Brak zabezpieczeń kryptograficznych łącza telekomunikacyjnego czy nieefektywność fizycznych zabezpieczeń, również stanowi zagrożenie utraty poufności danych osobowych.

§ 2

1. Podatność systemu na zagrożenia została ograniczona poprzez:
   1) ochronę fizyczną stanowisk komputerowych;
   2) kontrolę dostępu do pomieszczeń, gdzie przetwarzane są dane osobowe;
   3) wydzielenie stref ochronnych;
   4) ograniczenie liczby personelu, mającego potencjalnie dostęp do stanowisk komputerowych oraz wiedzę, jak je obsługiwać;
   5) zbudowanie stabilnej sieci zasilającej;
   6) przeglądy okresowe nośników;
   7) kontrolę zmian konfiguracji;
   8) testowanie oprogramowania;
   9) audyt;
   10) zabezpieczanie haseł;
   11) użycie oprogramowania antywirusowego;
   12) backupy.
2. By maksymalnie wyeliminować zagrożenie dla całego systemu ochrony danych osobowych, należy wdrożyć procedury kontrolne, które nie będą zorientowane tylko i wyłącznie na jeden obszar przetwarzania danych osobowych, tj. środowisko komputerowe. Warunkiem wyeliminowania działań cyberprzestępców, jest pełne współdziałanie wszystkich obszarów przetwarzania danych osobowych:
   1) prowadzenie odpowiedniej dokumentacji;
   2) fizyczna ochrona danych osobowych;
   3) środowisko komputerowe;

§ 3

W celu wdrażania systemu ochrony danych osobowych w taki sposób, by uniemożliwić działanie nieuprawnione na danych osobowych, Administrator Danych zobowiązuje pracowników podmiotu o nazwie: **Urząd Miasta i Gminy Czarne** do stosownego zachowania w trakcie przetwarzania danych osobowych.

§ 4

W celu oszacowania potencjalnych strat wynikających z utraty (ujawnienia) danych osobowych przetwarzanych na stanowiskach komputerowych, wykonano analizę ryzyka na podstawie przewidywanych zagrożeń dla zasobów. Jednolita Analiza Kontrolna Krajowych Ram Interoperacyjności musi być wykonywana okresowo przez Administratora Systemu Informatycznego - raz do roku na tej podstawie aktualizowana jest tabela ryzyka znajdująca poniżej - § 6.

§5

Identyfikacja podatności systemu informatycznego na określone zagrożenia.

WARTOŚĆ	SKUTKI
1	Niski poziom podatności
<1 – 2,5≥	Średni poziom podatności
<2,5 – 4>	Wysoki poziom podatności
4	Ekstremalny poziom podatności

BURMISTRZ
mgr Piotr Zabrocki

.....
(Podpis Administratora Danych)

Załącznik Nr 4 Jednolitej Analizy Kontrolnej Krajowych Ram Interoperacyjności stanowiącej załacznik do Zarządzenia Nr 0050.211.2018 Burmistrza Czarnego z dnia 21 grudnia 2018 r.

Jednolita Analiza Kontrolna Krajowych Ram Interoperacyjności – określenie poziomu ryzyka

§ 1

Administrator Danych, aby poprawnie przeprowadzić jednolitą analizę kontrolną, powinien określić:

1. **ZASOBY** - które będzie chronić:
   1) sprzęty komputerowe przechowujące dane - dyski twarde,
   2) dane osobowe przetwarzane w formie papierowej i elektronicznej,
   3) aplikacje, w których przetwarzane są dane osobowe,
   4) pomieszczenia, w których pracują osoby przetwarzające dane osobowe;
2. **ZAGROŻENIA** - czynniki, które mogą powodować wystąpienie incydentu;
3. **PODATNOŚĆ** - słabość zasobów, która może być wykorzystana przez potencjalne zagrożenie;
4. **SKUTKI** - jaki wpływ będzie miał zaistniały incydent na utratę danych osobowych.

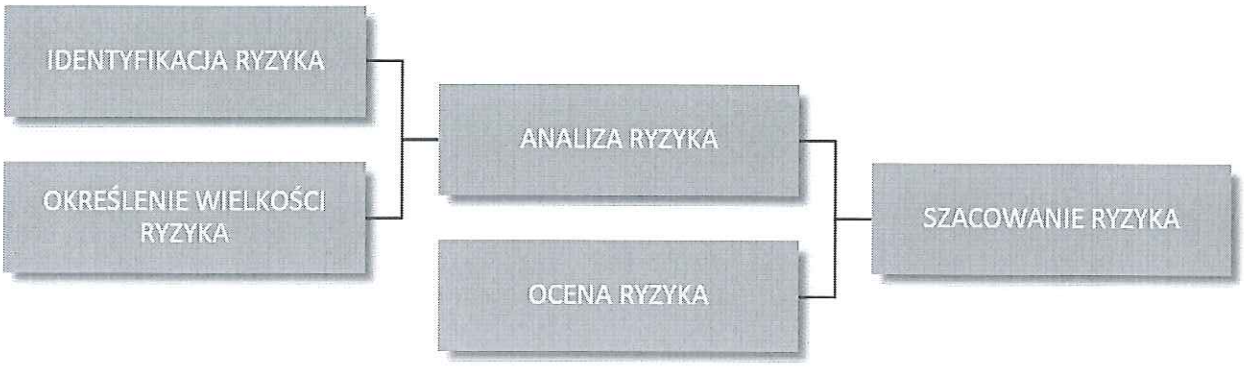
§ 2

Ryzyko to funkcja dwóch zmiennych:

1) prawdopodobieństwa wystąpienia negatywnego zdarzenia oraz
2) konsekwencji wystąpienia negatywnego zdarzenia.

§ 3

Poniższy schemat obrazuje prawidłowy tok szacowania i postępowania z ryzykiem, jakie podejmuje Administrator Danych.



§ 4

1. Analiza ryzyka jest częścią szacowania ryzyka. Jest ona pojęciem węższym niż szacowanie ryzyka, nie zawiera bowiem oceny ryzyka.
2. Ocena ryzyka, czyli określenie, które ryzyka są akceptowalne poprzez porównanie wyznaczonych poziomów ryzyka z tymi, które można zaakceptować.

3. Szacowanie ryzyka obejmuje analizę ryzyka i ocenę ryzyka.

§ 5

Oceny ryzyka należy dokonywać poprzez odniesienie się do dwóch miar tj:

1) konsekwencji negatywnego zdarzenia oraz

2) częstotliwości występowania negatywnego zdarzenia.

§ 6

1. **Konsekwencje naruszenia systemu bezpieczeństwa informacji będzie rozpatrywać się następująco:**

   1) **Niskie** – niewielki lub praktycznie brak wpływu negatywnego zdarzenia na realizację zadań organizacji;

   2) **Średnie** – negatywne zdarzenie ma zauważalny wpływ na realizację zadań organizacji;

   3) **Wysokie** – negatywne zdarzenie ma znaczący wpływ na realizację zadań organizacji, co wiąże się z konsekwencjami formalno-prawnymi oraz negatywnym wpływem na wizerunek organizacji;

   4) **Maksymalne** – negatywne zdarzenie powodujące brak możliwości realizacji zadań organizacji, zdarzenie negatywne powodujące również negatywny wpływ na wizerunek organizacji.

2. **Częstotliwość występowania naruszeń w zakresie bezpieczeństwa informacji:**

   1) **Sporadycznie** – naruszenie systemu bezpieczeństwa informacji występuje nie częściej, niż raz na rok;

   2) **Czasami** – naruszenie systemu bezpieczeństwa informacji występuje nie częściej, niż raz na kwartał;

   3) **Często** - naruszenie systemu bezpieczeństwa informacji występuje kilka razy w miesiącu.

§ 7

1. Administrator Danych szacuje wynik ryzyka. Poprzez określenie poziomu ryzyka akceptowalnego i kończy etap szacowania ryzyka.

2. Administrator Danych wyciąga wnioski oraz podejmuje działania naprawcze, mające na celu obniżenie wartości ryzyka akceptowalnego.

3. Tabela szacowania ryzyka stanowi **Załącznik nr 7 Jednolitej Analizy Kontrolnej Krajowych Ram Interoperacyjności stanowiącej załacznik do Zarządzenia Nr 0050.211.2018 Burmistrza Czarnego z dnia 21 grudnia 2018r .**

§ 8

1. Administrator Danych określa poziom ryzyka utraty bezpieczeństwa danych osobowych na poziomie **Średnie** w podmiocie o nazwie **Urząd Miasta i Gminy Czarne** przy uwzględnieniu ryzyka ogólnego przy wartości **2,48** o wartości procentowej ryzyka **49 %.**

   RYZYKO = wartość skutków x podatność zasobów systemu

   (max. = 4)

WARTOŚĆ	POZIOM RYZYKA
1	**NISKI** poziom ryzyka utraty bezpieczeństwa danych osobowych
<1 – 2,5≥	**ŚREDNI** poziom ryzyka utraty bezpieczeństwa danych osobowych
<2,5 - 4>	**WYSOKI** poziom ryzyka utraty bezpieczeństwa danych osobowych
4	**MAKSYMALNY** poziom ryzyka utraty bezpieczeństwa danych osobowych

2. **Poziomy ryzyka utraty bezpieczeństwa danych osobowych:**

   a) **NISKI** – niskie szkody w przypadku realizacji zagrożenia i niska możliwość jego wystąpienia;

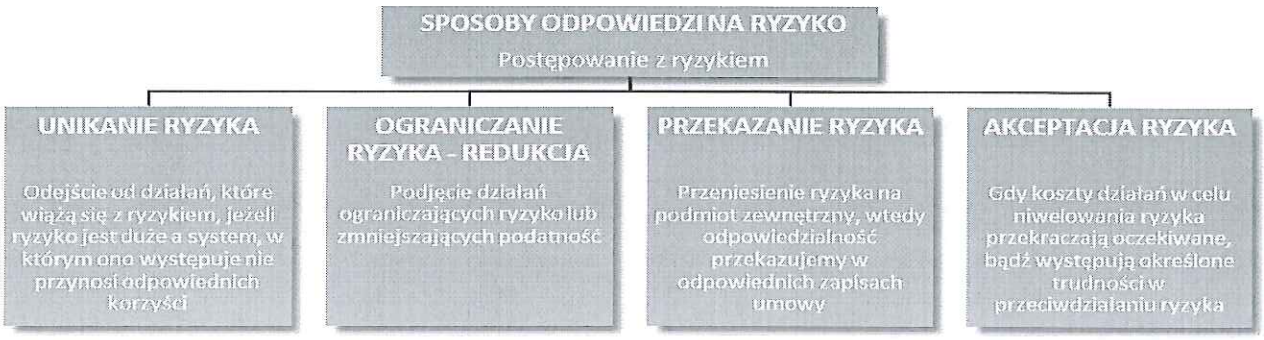
   b) **ŚREDNI** – wysokie szkody w przypadku realizacji zagrożenia i niska możliwość jego realizacji bądź niskie szkody w przypadku realizacji zagrożenia i wysoka możliwość jego realizacji;

   c) **WYSOKI** – wysokie szkody w przypadku realizacji zagrożenia i wysoka możliwość jego wystąpienia;

   d) **MAKSYMALNY** – wysokie szkody w przypadku realizacji zagrożenia oraz wysoka możliwość jego wystąpienia, skutkująca nie tylko na organizację, ale na podmioty trzecie.

§ 9

Administrator Danych po oszacowaniu ryzyka przystępuje do etapu postępowania z ryzykiem. Koniecznym jest podjęcie działania, które będzie odpowiedzią podmiotu na oszacowany poziom występującego ryzyka. W ramach postępowania z ryzykiem możemy podjąć cztery różne działania.



§ 10

Proces zarządzania ryzykiem związany z bezpieczeństwem informacji zapewnia:

1. identyfikowanie zagrożeń dla przetwarzanych informacji;
2. oszacowanie ryzyka w kategoriach konsekwencji dla funkcjonowania biznesowego oraz prawdopodobieństwa wystąpienia zagrożeń;
3. odpowiednie przedstawienie oraz zrozumienie prawdopodobieństwa oraz konsekwencji materializacji ryzyka;
4. ustanowienie priorytetów dotyczących postępowania z ryzykiem;
5. wprowadzanie priorytetowych działań mających na celu redukcję ryzyka;
6. zaangażowanie kierownictwa podczas podejmowania decyzji związanych z zarządzaniem ryzykiem oraz bieżące informowanie go o postępach realizowanych działań minimalizujących;
7. monitorowanie i regularne przeglądanie ryzyka oraz procesu zarządzania nimi;
8. kształcenie pracowników w zakresie ryzyka oraz działań mających na celu obniżenie poziomu prawdopodobieństwa ich wystąpienia.

BURMISTRZ
mgr Piotr Zabrocki

.....
(Podpis Administratora Danych)

Załącznik Nr 5 Jednolitej Analizy Kontrolnej Krajowych Ram Interoperacyjności stanowiącej zalacznik do Zarządzenia Nr 0050.211.2018 Burmistrza Czarnego z dnia 21 grudnia 2018 r.

Wnioski i działania naprawcze w związku z przeprowadzoną jednolitą analizą kontrolną krajowych ram interoperacyjności przy przetwarzaniu danych osobowych

§ 1

1. Administrator Danych: **Burmistrz Czarnego,** przeprowadził jednolitą analizę kontrolną dla wszystkich chronionych zasobów oraz wszystkich możliwych zagrożeń.
2. Administrator Danych jest zobowiązany dostosować środki bezpieczeństwa, zarówno techniczne, jak i fizyczne oraz organizacyjne, do wyników, jakie oddała przeprowadzona jednolita analiza kontrolna.

§ 2

W wyniku przeprowadzonej analizy w jednostce o nazwie: **Urząd Miasta i Gminy w Czarnem**, Administrator Danych wyróżnił potencjalnie najniebezpieczniejsze zagrożenia, a w szczególności są to:

1) pożar,
2) zalanie wodą

§ 3

W celu zmniejszenia zagrożeń, wymienionych w § 2 przez Administratora Danych, należy zwrócić uwagę w szczególności na:

1) czujki dymu,
2) aktualizacje gaśnic,
3) sprawność sprzętu sanitarnego

§ 4

Administrator Danych w celu wyeliminowania zagrożeń, wynikłych w toku przeprowadzonej analizy, podejmuje działania naprawcze, polegające w szczególności na:

1) wykonaniu ekspertyzy całego budynku,
2) rozważenia możliwości założenia czujek dymu,

BURMISTRZ
mgr Piotr Zabrocki

.....
(Podpis Administratora Danych)

Załącznik Nr 6 Jednolitej Analizy Kontrolnej Krajowych Ram Interoperacyjności stanowiącej zalacznik do Zarządzenia Nr 0050.211.2018 Burmistrza Czarnego z dnia 21 grudnia 2018 r.

Plan postępowania z ryzykiem w związku z przeprowadzoną Jednolitą Analizą Kontrolną Krajowych Ram Interoperacyjności przy przetwarzaniu danych osobowych

§ 1

Plan postępowania z ryzykiem określa działania naprawcze mające na celu zminimalizowanie poziomu ryzyka. W planie postępowania z ryzykiem należy określić osoby odpowiedzialne za realizację działań naprawczych oraz terminy, w ramach których osoby te będą realizować zadania określone w planie. Plan postępowania z ryzykiem stanowi podstawę wdrożenia stosownych mechanizmów, zarówno o charakterze technicznym jak i organizacyjnym, które będą minimalizować potencjalną utratę poufności, rozliczalności i integralności danych osobowych.

§ 2

Poziom ryzyka powinien podlegać cyklicznemu monitorowaniu. Z uwagi na techniczne i organizacyjne czynniki występujące w organizacji, poziom ryzyka może ulegać zmianom w czasie. Może się okazać, iż mechanizm zastosowany w czasie rzeczywistym w celu minimalizacji poziomu ryzyka, nie będzie wystarczający w przyszłości i trzeba będzie wprowadzać dodatkowe mechanizmy w postaci na przykład dodatkowych zabezpieczeń.

§ 3

Proces zarządzania ryzykiem w organizacji wymaga udziału wielu pracowników, których sklasyfikować pod względem kompetencji można w następujący sposób:

1) **Kadra kierownicza organizacji** – zaangażowanie tej grupy osób jest szczególnie istotne, ponieważ to właśnie ta kadra powinna dokładać szczególnych starań, by proces zarządzania ryzykiem przebiegał bez zakłóceń;
2) **Koordynator procesu** – w zakresie bezpieczeństwa informacji koordynatorem procesu będzie Administrator Danych lub osoba przez niego wyznaczona;
3) **Eksperci techniczni** – w tej grupie osób znajdzie się między innymi Administrator Systemów Informatycznych czy Audytor Zewnętrzny w zakresie bezpieczeństwa informacji.

§ 4

Wzór planu postępowania z ryzykiem:

Obszar bezpieczeństwa informacji	Zakres podejmowanych działań naprawczych	Osoby odpowiedzialne za realizację planu postępowania z ryzykiem	Terminy planowanego rozpoczęcia i zakończenia działań naprawczych

BURMISTRZ

.....mgr Piotr Zabrocki.....

(Podpis Administratora Danych)

Załącznik nr 7 do Jednolitej Analizy Kontrolnej Krajowych Ram Interoperatywności stanowiącej załącznik do Zarządzenia Nr 0050.211.2018 Burmistrza Czarnego z dnia 21 grudnia 2018 r.

* **UWAGA:** Pusta kratka ☐ oznacza odpowiedź "NIE". Zaznaczona kratka ☑ oznacza odpowiedź "TAK"

LP	PYTANIE	Odpowiedź A*	Odpowiedź B*
1	A) Czy jakiekolwiek stanowisko komputerowe uległo awarii sprzętowej (mowa o osprzęcie fizycznym -np. brak możliwości uruchomienia stanowiska komputerowego)? B) Czy w okresie 24 godzin usterka może być naprawiona przez informatyka / firmę zewnętrzną?	☐	☑
2	A) Czy na terenie podmiotu występują urządzenia typu UPS / generator prądu? B) Czy w ostatnim kwartale wystąpiła utrata zasilania minimum 2 razy?	☐	☐
3	A) Czy na terenie placówki znajduje się ilość gaśnic, zgodna z zasadami PPOŻ? B) Czy występuje ryzyko związane z przekroczeniem właściwych terminów wykonania legalizacji gaśnic (okresowa kontrola gaśnic)?	☑	☐
4	A) Czy podmiot posiada Pendrive'y do celów służbowych dla pracowników przetwarzających dane? B) Czy pracownicy używają prywatnych Pendrive'ów?	☐	☐
5	A) Czy podmiot posiada komputery przenośne? B) Czy w przypadku, gdy pracownicy korzystają z komputerów przenośnych, są one wynoszone poza obręb podmiotu?	☑	☑
6	A) Czy sprzęt komputerowy zawierający dane osobowe jest zabezpieczony hasłem głównym ograniczającym jego uruchomienie? (np. hasło BIOS; WINDOWS) B) Czy doszło do sytuacji, podczas której osoba postronna uruchomiła sprzęt komputerowy zawierający dane osobowe bez użycia hasła głównego? (np. hasło BIOS; WINDOWS)	☐	☐
7	A) Czy wszystkie urządzenia elektroniczne uczestniczące w procesie elektronicznego przetwarzania danych osobowych są ze sobą kompatybilne wg opinii osoby/ób zajmującej/ych się infrastrukturą informatyczną?	☑	
8	A) Czy osoba/y zajmująca/e się infrastrukturą informatyczną we współpracy z osobą/ami zajmują/cymi się sprzętem spoza w/w infrastruktury może/gą kompleksowo zapewnić kalkulację wydatków w ciągu 30 dni kalendarzowych celem planowania budżetu związanego z modernizacją sprzętu?	☑	
9	A) Czy zakupiony sprzęt komputerowy jest nabyty od producentów godnych zaufania? Składa się na to: marka, rozpoznawalność, referencje, częstotliwość występowania w innych placówkach o podobnym profilu działania.	☑	
10	A) Czy w okresie ostatniego roku pracownicy byli przeszkoleni w zakresie używania sprzętu komputerowego? B) Czy z powodu niewłaściwego użytkowania sprzętu doszło w ostatnim półroczu do awarii?	☐	☐
11	A) Czy po zakończeniu pracy przy stanowisku komputerowym wyłączana jest listwa zasilająca? B) Czy pracownicy są uczuleni w kwestii niewykonywania tzw. "twardego resetu"?	☑	☑

12	A) Czy w przeciągu ostatniego roku wystąpił alarm przeciwpożarowy? B) Czy w przypadku zmiany zagospodarowania przestrzennego budynku podmiotu, pracownicy zostali poinformowani o naniesionych zmianach (np. punkt zbiórki, o ile się zmienił)?	☐	☑
13	A) Czy pracownicy korzystając z internetu w podmiocie spowodowali atak wirusa komputerowego? B) Czy pracownicy przechodzili w okresie ostatniego roku szkolenia informatyczne (ogólne)?	☐	☑
14	A) Czy w przeciągu ostatniego roku doszło do kradzieży danych osobowych na terenie podmiotu? B) Czy prowadzona jest ewidencja wejść i wyjść pracowników administracyjnych?	☐	☑
15	A) Czy w przeciągu ostatniego roku odbyła się kontrola zewnętrzna z powodu nieprawidłowego przepływu danych osobowych w podmiocie? B) Czy osoby z innych działów/referatów/stanowisk mają dostęp do szaf zamykanych z innych działów?	☐	☐
16	A) Czy istnieje wewnętrzny regulamin określający przepływ informacji pomiędzy działami/referatami lub stanowiskami?	☐	
17	A) Czy w podmiocie została sporządzona dokumentacja dot. ochrony danych osobowych względem Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 (RODO)	☑	
18	A) Czy wszyscy pracownicy w podmiocie są upoważnieni do przetwarzania danych osobowych?	☐	
19	A) Czy w okresie ostatniego kwartału wystąpiła awaria systemu WINDOWS z powodu awarii płyty głównej w komputerze? B) Czy na komputerach przenośnych (o ile występują) zainstalowany jest fabrycznie system WINDOWS? (dot. komputerów bez płyty instalacyjnej systemu WINDOWS)	☑	☑
20	A) Czy w okresie ostatniego kwartału doszło do awarii systemu WINDOWS z powodu utraty zasilania? B) Czy pomiędzy urządzeniem UPS (jeśli jest) a komputerem występuje komunikacja elektroniczna (celem awaryjnego wyłączenia zasilania)?	☐	☐
21	A) Czy w przypadku wystąpienia alarmu przeciwpożarowego kierownik podmiotu został poinformowany drogą elektroniczną (np. SMS) lub telefoniczną? B) Czy na wypadek wystąpienia alarmu przeciwpożarowego zastosowano system powiadamiania drogą elektroniczną (np. SMS) lub telefoniczną?	☐	☐
22	A) Czy z powodu wirusa komputerowego doszło do utraty danych osobowych? B) Czy w podmiocie występuje "serwer aktualizacji"?	☐	☐
23	A) Jeśli występuje sieć VPN, czy doszło do kradzieży w jej obrębie lub poprzez zdalny pulpit? B) Jeśli występuje sieć Wi-Fi, to czy jest ona zabezpieczona kluczem WPA-PSK 2?	☐	☐
24	A) Czy poza AD, IOD i ASI ma ktoś dostęp do ewidencji loginów i haseł w systemach informatycznych? B) Czy pracownicy administracyjni w systemach informatycznych mają własne loginy do programów specjalistycznych?	☐	☐

25	A) Czy na terenie placówki występuje oprogramowanie jednego producenta działające na wspólnej bazie danych (systemy ERP)?	☐	
26	A) Czy osoba zajmująca się systemami informatycznymi ma możliwość grupowego oraz zdalnego zarządzania oprogramowaniem na terenie podmiotu (aktualizacje, licencje, prawa użytkownika, czynności serwisowe)?	☐	
27	A) Czy kopie zapasowe (elektroniczne) programów specjalistycznych są przechowywane w zamykanym pomieszczeniu z zamykaną szafą (szafką, szafą serwerową, szufladzie)?	☐	
28	A) Czy w przeciągu ostatniego roku doszło do awarii sprzętu komputerowego z powodu nadmiernego okablowania tj. kable łączące stanowisko komputerowe w całość są za długie, leżą na ziemi i podatne są na zerwanie przez użytkownika? B) Czy planowana jest w przeciągu najbliższego roku modernizacja sprzętu komputerowego pod kątem urządzeń typu All-In-One? (np. komputery zamknięte w jednej jednolitej obudowie wraz z monitorem)	☐	☐
29	A) Czy podmiot posiada rozdzieloną sieć elektryczną na gniazdka dla urządzeń elektrycznych, oraz osobno dla urządzeń komputerowych? B) Czy podmiot posiada opisaną infrastrukturę elektryczną tj. opisane na obudowie gniazdka elektryczne na/w ścianach?	☐	☐
30	A) Czy w pomieszczeniach zainstalowane są czujki przeciwpożarowe? B) Czy wobec czujek przeciwpożarowych podejmowane są czynności konserwacyjne minimum raz na rok?	☐	☐
31	A) Czy w ostatnim kwartale wystąpiło zainfekowanie stanowiska komputerowego wirusem przez petenta? (podanie i podłączenie urządzenia przenośnego wraz ze szkodliwym oprogramowaniem) B) Czy pracownicy administracyjny są uświadomieni by przeciwdziałać sytuacjom pozyskiwania/podłączania urządzeń przenośnych do komputerów?	☐	☐
32	A) Czy w ostatnim roku doszło do sytuacji utraty danych po godzinach pracy? (mowa o konkretnych pomieszczeniach, oraz utracie danych w wersji papierowej) B) Czy pomieszczenia w których przetwarzane są dane osobowe zabezpieczone są zamkami?	☐	☐
33	A) Czy poza AD, IOD i ASI inny pracownik administracyjny ma dostęp do pomieszczenia serwerowni? B) Czy po godzinach pracy (oraz w trakcie jeśli zajdzie taka potrzeba) klucze do pomieszczeń składowane są w wyznaczonym pomieszczeniu, celem ograniczenia nieautoryzowanego dostępu fizycznego?	☐	☐
34	A) Czy kierownik działu/referatu itp. nadzoruje jedno pomieszczenie? (jeśli nie, sytuacja dotyczy pracowników podległych osobie kierującej, rozmieszczonych w wielu pomieszczeniach)	☐	
35	A) Czy kierownik działu/referatu nadzorując pomieszczenie/a tworzy pisemny raport minimum raz na pół roku w zakresie zapotrzebowania sprzętowego oraz oprogramowania?	☐	
36	A) Czy informacje nt. incydentów takich jak: awaria sprzętu, odcięcie zasilania, atak wirusa, kradzież, nieuprawniony dostęp - przekazywane są najpierw do AD i IOD (jeśli występuje)?	☑	
37	A) Czy w okresie ostatniego roku doszło do awarii serwera backup? (lub urządzenia do kopii zapasowych) B) Czy w okresie ostatniego roku doszło do awarii serwera głównego?	☐	☐

38	A) Czy w okresie ostatniego roku doszło do awarii zasilania z powodu warunków pogodowych? B) Czy na terenie podmiotu jest awaryjny UPS podtrzymujący wszystkie komputery (lub generator prądu)?	☐	☐
39	A) Czy w podmiocie jest system automatycznego gaszenia pożaru? B) Czy w podmiocie występują drzwi przeciwpożarowe?	☐	☐
40	A) Czy wystąpiły sytuacje włamania/ataku informatycznego wobec podmiotu? B) Czy pracownicy korzystają na terenie podmiotów z poczt prywatnych?	☐	☐
41	A) Czy wystąpiły sytuacje, podczas których pracownik podmiotu nieautoryzowanie wyniósł dokumentację z podmiotu? B) Czy podmiot posiada służbę ochrony?	☐	☐
42	A) Czy wystąpiło zagrożenie utraty danych (kradzież) z sieci wewnętrznej poprzez sieć publiczną (ogólnodostępne Wi-Fi)? B) Czy sieć publiczna (ogólnodostępna poprzez Wi-Fi) jest oddzielona od sieci wewnętrznej?	☐	☐
43	A) Czy placówka posiada archiwistę?	☐	
44	A) Czy w przypadku potrzeby pozyskania dokumentu z archiwum czas realizacji jest mniejszy niż 3 dni?	☐	
45	A) Czy archiwum na terenie placówki spełnia wymogi zgodnie z ustawą o narodowych zasobach archiwalnych?	☐	

JEDNOLITA ANALIZA KONTROLNA KRAJOWYCH RAM INTEROPERACYJNOŚCI - TABELA SZACOWANIA RYZYKA

SZACOWANIE RYZYKA DLA BEZPIECZEŃSTWA INFORMACJI																				
RYZYKO ŚREDNIE :					2,25			1,72			3,00			3,00			2,42	2,48
ZAGROŻENIA																		RYZYKO OGÓLNE :
	INTEGRALNOŚĆ	AWARIA SPRZĘTU	1	1	1,00	2	1	2,50	2	2	4,00	1	2	2,50	1	1	1,50	
		ODCIĘCIE ZASILANIA	2	1	2,50	2	1	2,50	1	2	2,50	2	2	4,00	1	2	2,50	
		POŻAR	1	1	1,00	1	1	1,50	2	2	4,00	2	2	4,00	2	2	4,00	
		ATAK WIRUSA	2	1	2,50	1	1	1,50	1	2	2,50	1	2	2,50	1	1	1,50	
		KRADZIEŻ	2	2	4,00	1	1	1,50	1	2	2,50	1	2	2,50	1	2	2,50	
		NIEUPRAWNIONY DOSTĘP	2	1	2,50	1	1	1,50	1	2	2,50	1	2	2,50	1	2	2,50	
	ROZLICZALNOŚĆ	AWARIA SPRZĘTU	1	1	1,00	2	1	2,50	2	2	4,00	1	2	2,50	1	1	1,50	
		ODCIĘCIE ZASILANIA	2	1	2,50	2	1	2,50	1	2	2,50	2	2	4,00	1	2	2,50	
		POŻAR	1	1	1,00	1	1	1,00	2	2	4,00	2	2	4,00	2	2	4,00	
		ATAK WIRUSA	2	1	2,50	1	1	1,00	1	2	2,50	1	2	2,50	1	1	1,50	
		KRADZIEŻ	2	2	4,00	1	1	1,00	1	2	2,50	1	2	2,50	1	2	2,50	
		NIEUPRAWNIONY DOSTĘP	2	1	2,50	1	1	1,00	1	2	2,50	1	2	2,50	1	2	2,50	
	POUFNOŚĆ	AWARIA SPRZĘTU	1	1	1,00	2	1	2,50	2	2	4,00	1	2	2,50	1	1	1,50	
		ODCIĘCIE ZASILANIA	2	1	2,50	2	1	2,50	1	2	2,50	2	2	4,00	1	2	2,50	
		POŻAR	1	1	1,00	1	1	1,50	2	2	4,00	2	2	4,00	2	2	4,00	
		ATAK WIRUSA	2	1	2,50	1	1	1,50	1	2	2,50	1	2	2,50	1	1	1,50	
		KRADZIEŻ	2	2	4,00	1	1	1,50	1	2	2,50	1	2	2,50	1	2	2,50	
		NIEUPRAWNIONY DOSTĘP	2	1	2,50	1	1	1,50	1	2	2,50	1	2	2,50	1	2	2,50	
SZACOWANIE			SKUTKI	PODATNOŚĆ	RYZYKO	SKUTKI	PODATNOŚĆ	RYZYKO	SKUTKI	PODATNOŚĆ	RYZYKO	SKUTKI	PODATNOŚĆ	RYZYKO	SKUTKI	PODATNOŚĆ	RYZYKO	
ZASOBY SZACOWANE			SPRZĘT			LUDZIE			APLIKACJA			POMIESZCZENIA			DODATKOWE ZABEZPIECZENIA			

PODSUMOWANIE

Po przeprowadzeniu analizy poufności, integralności i rozliczalności systemów informatycznych pod kątem zagrożeń i ryzyka, zwanej dalej: **Jednolitą Analizą Kontrolną Krajowych Ram Interoperacyjności** przy przetwarzaniu danych osobowych wartość i poziom ryzyka przedstawia się następująco:

RYZYKO OGÓLNE: **49 %**

Powyższa wartość ryzyka określa: **ŚREDNIE** ryzyko utraty bezpieczeństwa danych osobowych.

BURMISTRZ
mgr Piotr Zabrocki