Polityka przetwarzania i ochrony danych osobowych

WYDANIE 1.0

CHRZYPSKO WIELKIE, DNIA 9 KWIETNIA 2025 R.

Cel:

Ochrona osób fizycznych w związku z przetwarzaniem danych osobowych jest jednym z praw podstawowych. Art. 8 ust. 1 Karty praw podstawowych Unii Europejskiej oraz art. 16 ust. 1 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE) stanowią, że każda osoba ma prawo do ochrony danych osobowych jej dotyczących.

Podstawy prawne:

1. rozporządzenie Parlamentu Europejskiego i Rady Europy (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 (RODO) (4.5.2016, L 119);
2. ustawa z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. 2019 poz. 730);
3. ustawa z dnia 10 maja 2018r. o ochronie danych osobowych (t.j. Dz. U. z 2019 r. poz. 1781 z późn. zm.).

Przedmiot:

Przedmiotem Polityki przetwarzania i ochrony danych osobowych są zasady i tryb postępowania podczas przetwarzania danych osobowych w formie tradycyjnej i elektronicznej. Mając na względzie obowiązek stosowania odpowiednich zabezpieczeń przetwarzanych danych osobowych w odniesieniu do zakresu, kontekstu i celu, a także ryzyka naruszenia ochrony przetwarzanych danych, zgodnie z art. 32 RODO, wdraża się odpowiednie środki techniczne i organizacyjne.

Zakres stosowania:

Polityka przetwarzania i ochrony danych osobowych obowiązuje wszystkie istniejące, wdrażane obecnie lub w przyszłości systemy informacyjne, w których przetwarzane są dane osobowe. Politykę tę stosuje się we wszystkich lokalizacjach, w których przetwarzane są informacje podlegające ochronie, na wszystkich nośnikach informacji (tradycyjnych - papierowych, elektronicznych, optycznych, magnetycznych), które zawierają dane podlegające ochronie. Polityka obowiązuje wszystkich pracowników w rozumieniu przepisów Kodeksu Pracy, w tym stażystów i osób, z którymi podpisane są umowy cywilno-prawne wykonujących prace na rzecz Administratora oraz innych osób mających dostęp do danych.

ZATWIERDZAM I POLECAM STOSOWAĆ

……..

Kierownik Jednostki

SPIS TREŚCI

DEFINICJE

Ilekroć w niniejszej Polityce jest mowa o:

1) Administratorze Danych Osobowych – rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, które decydują o celach i środkach przetwarzania danych osobowych, a w niniejszej Polityce Klub Dziecięcy w Chrzypsku Wielkim (w skrócie: Klub dziecięcy) reprezentowany przez Dyrektora - Kierownika Jednostki zwanego „Administratorem";
2) Inspektorze Ochrony Danych Osobowych (lub IODO) – rozumie się przez to osobę wyznaczoną przez Administratora, która jest odpowiedzialna za zapewnienie przetwarzania danych zgodnie z odpowiednimi przepisami prawa;
3) Administratorze Systemów Informatycznych (lub ASI) – rozumie się przez to osobę wyznaczoną przez Administratora, która odpowiada za zapewnienie sprawności, należytej konserwacji i wdrażania technicznych zabezpieczeń systemów informatycznych oraz odpowiada za to, aby systemy informatyczne, w których przetwarzane są dane osobowe spełniały wymagania przewidziane przepisami prawa;
4) danych osobowych (lub danych) – rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
5) osobie upoważnionej – rozumie się przez to osobę, która otrzymała od Administratora pisemne upoważnienie do przetwarzania danych;
6) przetwarzaniu danych – rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te operacje, które wykonuje się w systemach informatycznych;
7) upoważnieniu – rozumie się przez to oświadczenie nadawane przez Administratora wskazujące z imienia i nazwiska oraz stanowiska osobę, która ma prawo przetwarzać dane w zakresie wskazanym w tym oświadczeniu;
8) RODO - 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), zwane w skrócie RODO;
9) PUDO lub Urząd Nadzoru – Prezes Urzędu Ochrony Danych Osobowych;
10) zbiorze danych – rozumie się przez to dane zebrane w postaci zbioru lub według kategorii:
    a) danych osobowych podopiecznych z podzbiorami,
    b) danych pracowniczych z podzbiorami,
    c) danych administracyjnych z podzbiorami,
    d) danych doraźnych,

przy czym każdy zbiór danych to zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

POSTANOWIENIA OGÓLNE
§ 1.

Przetwarzanie danych osobowych jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z poniższych warunków:

1. osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
2. przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
3. przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
4. przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
5. przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
6. przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem, co nie ma zastosowania do przetwarzania, którego dokonują organy publiczne w ramach realizacji swoich zadań.

INSPEKTOR DANYCH OSOBOWYCH I ADMINISTRATOR SYSTEMÓW INFORMATYCZNYCH
§ 2.

1. Administrator Danych Osobowych wyznacza i zgłasza do rejestru prowadzonego przez Urząd Ochrony Danych Osobowych Inspektora Ochrony Danych Osobowych (IODO), który jest odpowiedzialny za przetwarzanie danych.
2. Administrator Danych Osobowych wyznacza Administratora Systemów Informatycznych (ASI).
3. Administrator Danych Osobowych wyznacza osoby współdziałające z IODO w zakresie ochrony danych osobowych.

§ 3.

W przypadku niewyznaczenia IODO lub ASI za zapewnienie należytego przestrzegania zasad ochrony danych osobowych odpowiada Administrator.

§ 4.

1. W przypadku powzięcia jakichkolwiek wątpliwości co do ewentualnej zgodności z prawem planowanych działań w zakresie przetwarzania danych, należy zwrócić się do IODO z wnioskiem o rozstrzygnięcie wątpliwości.

2. Przed udzieleniem przez IODO odpowiedzi w przedmiocie istniejących wątpliwości niedozwolone jest zbieranie danych osobowych i ich utrwalanie, a w przypadku posiadania już danych osobowych których wątpliwość dotyczy należy, do czasu rozstrzygnięcia wątpliwości, wstrzymać wszystkie działania na danych osobowych, co do których istnieją wątpliwości czy są prawnie uzasadnione.

OSOBY UPOWAŻNIONE DO PRZETWARZANIA DANYCH OSOBOWYCH

§ 5.

Do przetwarzania danych osobowych w Klubie dziecięcym w Chrzypsku Wielkim są uprawnione wyłącznie osoby upoważnione przez Administratora.

§ 6.

1. Upoważnienia nadawane są indywidualnie, przed rozpoczęciem przez osobę upoważnianą przetwarzania danych osobowych. Wzór Upoważnienia do przetwarzania danych osobowych stanowi Załącznik Nr 1do niniejszej Polityki.
2. Upoważnienie do przetwarzania danych osobowych mogą uzyskać wyłącznie pracownicy oraz osoby fizyczne współpracujące z Administratorem, które uzyskują dostęp do danych osobowych w związku ze świadczeniem na jego rzecz usług na podstawie umów cywilnoprawnych lub jako osoby fizyczne wykonujące obowiązki na podstawie jednoosobowej działalności (zatrudnieni).
3. Upoważnienie nadawane jest niezwłocznie po przyjęciu do pracy lub po zawarciu umowy cywilnoprawnej, w sytuacjach gdy zakres wykonywanych obowiązków wiąże się z potrzebą uzyskania dostępu do danych osobowych.
4. Upoważnienie nadawane jest na czas zatrudnienia na danym stanowisku pracy lub na czas realizacji zleconych czynności.
5. Upoważnienie do przetwarzania danych osobowych nadawane jest przez Administratora.
6. Osoba posiadająca upoważnienie do przetwarzania danych jest uprawniona do ich przetwarzania w zakresie i czasie wskazanym w upoważnieniu.
7. Inspektor Ochrony Danych Osobowych na podstawie wydanych upoważnień prowadzi ewidencję (rejestr) osób upoważnionych do przetwarzania danych.
8. Każda osoba upoważniana do przetwarzania danych osobowych składa pisemne oświadczenie o zachowaniu w tajemnicy przetwarzanych danych osobowych oraz znanych jej informacji o stosowanych wobec danych środkach bezpieczeństwa. Wzór Oświadczenia stanowi Załącznik Nr 2 do niniejszej Polityki.

§ 7.

1. Każdy kto przetwarza dane osobowe obowiązany jest zachować w tajemnicy dane osobowe do których posiada dostęp zarówno zamierzony jak i przypadkowy, sposoby zabezpieczania danych jak również wszelkie informacje, które powzięły w czasie przetwarzania danych. Obowiązek zachowania danych w tajemnicy jest bezterminowy.
2. Podczas przetwarzania danych należy zachować szczególną ostrożność i podjąć wszelkie możliwe środki umożliwiające zabezpieczenie oraz ochronę danych przed nieuprawnionym dostępem, modyfikacją, zniszczeniem lub ujawnieniem.

3. Należy dochować należytej staranności podczas przesyłania dokumentów zawierających dane za pomocą środków komunikacji elektronicznej, w szczególności należy upewnić się, czy przesyłane za pomocą poczty elektronicznej dokumenty trafiły do właściwego odbiorcy.
4. W przypadku przesyłania za pomocą środków komunikacji elektronicznej zestawień, spisów czy innych dokumentów zawierających dane osobowe, przesyłany dokument należy zaszyfrować, a hasło przesłać w innym środkiem komunikacji elektronicznej.

§ 8.

1. Administrator podejmuje odpowiednie środki, aby w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem – w szczególności gdy informacje są kierowane do osoby małoletniej – udzielić osobie, której dane dotyczą, wszelkich informacji, o których mowa w art. 13 i 14 RODO, oraz prowadzić z nią wszelką komunikację na mocy art. 15–22 i 34 w sprawie przetwarzania. Informacji udziela się na piśmie lub w inny sposób, w tym w stosownych przypadkach – elektronicznie. Jeżeli osoba, której dane dotyczą, tego zażąda, informacji można udzielić ustnie, o ile innymi sposobami potwierdzi się tożsamość osoby, której dane dotyczą.
2. W przypadku zbierania danych osobowych nie od osoby, której one dotyczą, Administrator jest obowiązany spełnić obowiązek informacyjny, wobec osoby, której dane uzyskano bezpośrednio po utrwaleniu zebranych danych.
3. Powyższy obowiązek Administrator nakłada na osoby zatrudnione przy przetwarzaniu danych osobowych, zobowiązując je do jego należytego wykonywania zgodnie z treścią dokumentów oraz klauzul informacyjnych stanowiących Załączniki od Nr 3 do Nr 8 do niniejszej Polityki (Klauzula ogólna (3), Klauzula do pracowników (4), Klauzula dla pracowników korzystających z ZFŚS (5), Klauzula dla stażystów, praktykantów i wolontariuszy (6), Klauzula dla kontrahentów w umowach cywilno-prawnych (7), Klauzula w związku z korzystaniem przez Administratora z mediów

§ 9

REALIZACJA PRAW PRZEZ OSOBY, KTÓRYCH DANE DOTYCZĄ

1. W przypadku otrzymania żądania w postaci pisemnego wniosku dotyczącego prawa dostępu przysługującego osobie, której dane dotyczą należy:
    a. wniosek należy przekazać do IODO,
    b. IODO przygotowuje projekt odpowiedzi na wniosek,
    c. odpowiedź na żądanie podpisuje Administrator lub osoba przez niego upoważniona,
    d. odpowiedź przekazywana jest adresatowi w formie listu poleconego za potwierdzeniem odbioru, jeżeli żądanie przyszło drogą elektroniczną i istnieje możliwość weryfikacji nadawcy, korespondencje można wysłać również drogą elektroniczną,
    e. IODO prowadzi rejestr wpływających wniosków.
2. W przypadku otrzymania żądania w postaci pisemnego wniosku dotyczącego prawa do sprostowania danych należy:

a. wniosek należy przekazać do IODO,
b. IODO zwraca się do ASI z prośbą o sprostowanie danych,
c. ASI jest zobowiązany do sprostowania danych, o które wnioskował IODO w ciągu 10 dni,
d. IODO przygotowuje projekt odpowiedzi na wniosek,
e. odpowiedź na żądanie podpisuje Administrator lub osoba przez niego upoważniona,
f. odpowiedź przekazywana jest adresatowi w formie listu poleconego za potwierdzeniem odbioru, jeżeli żądanie przyszło drogą elektroniczną i istnieje możliwość weryfikacji nadawcy, korespondencje można wysłać również drogą elektroniczną,
g. IODO prowadzi rejestr wpływających wniosków.

3. W przypadku otrzymania żądania w postaci pisemnego wniosku dotyczącego prawa do:
   a. usunięcia danych („prawo do bycia zapomnianym”),
   b. ograniczenia przetwarzania,
   c. przenoszenia danych,
   d. sprzeciwu,

   należy:
   1) wniosek należy przekazać do IODO,
   2) IODO ocenia zasadność wniosku:
   3) w przypadku, gdy żądanie nie jest zasadne:
      - IODO przygotowuje odpowiedź do akceptacji i podpisu Administratora lub osoby upoważnionej,
      - odpowiedź przekazywana jest adresatowi w formie listu poleconego za potwierdzeniem odbioru, jeżeli żądanie przyszło drogą elektroniczną i istnieje możliwość weryfikacji nadawcy, korespondencje można wysłać również drogą elektroniczną,
   4) w przypadku, gdy żądanie jest zasadne:
      - IODO zwraca się do ASI z prośbą o realizację żądań zawartych we wniosku,
      - ASI jest zobowiązany do realizacji wniosku IODO w ciągu 10 dni,
      - IODO przygotowuje projekt odpowiedzi na wniosek,
      - odpowiedź na wniosek podpisuje Administrator lub osoba upoważniona,
      - odpowiedź przekazywana jest adresatowi w formie listu poleconego za potwierdzeniem odbioru, jeżeli żądanie przyszło drogą elektroniczną i istnieje możliwość weryfikacji nadawcy, korespondencje można wysłać również drogą elektroniczną,
   5) IODO prowadzi rejestr wniosków.

4. Administrator Danych Osobowych udziela odpowiedzi na żądania osób, których dane dotyczą, bez zbędnej zwłoki, najpóźniej w terminie miesiąca, a jeżeli nie zamierza spełnić takiego żądania zobowiązany jest do podania przyczyny. Jeżeli żądanie ma skomplikowany charakter podmiot danych skierował dużą liczbę żądań, Administrator czas udzielenia odpowiedzi może wydłużyć o kolejne dwa miesiące**,** jednakże w takim wypadku jest zobowiązany do przekazania takiej informacji osobie fizycznej w terminie

pierwszego miesiąca licząc od momentu wpłynięcia żądania. Musi również w takim wypadku podać przyczyny wydłużenia terminu na udzielenie odpowiedzi.

5. W przypadku jakichkolwiek zmian w zbiorach danych wynikających z realizacji praw osób, których dane dotyczą, Administrator zobowiązany jest poinformować bez zbędnej zwłoki odbiorców, którym je udostępnił (przekazanie do wiadomości odpowiedzi kierowanej do adresata).

§ 10.

1. Dane osobowe mogą być udostępniane w następujących przypadkach:
   1) na podstawie wniosku od podmiotu uprawnionego do otrzymywania danych na podstawie przepisów prawa,
   2) na podstawie umowy powierzenia zawartej z innym podmiotem, w ramach której istnieje konieczność udostępnienia danych osobowych.
2. Dane osobowe udostępnia się na pisemny umotywowany wniosek, chyba że istnieją przepisy stanowiące inaczej.
3. Udostępniając dane osobowe należy zaznaczyć, że można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

OKREŚLENIE ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH, NIEZBĘDNNYCH DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH

§11.

1. Wszelkie dokumenty zwierające dane osobowe przechowywane są w szafach i pomieszczeniach zamykanych na klucz.
2. Osoba będąca dysponentem kluczy jest zobowiązana nie przekazywać kluczy do budynków i pomieszczeń, w których przetwarzane są dane, osobom nieuprawnionym, a ponadto obowiązana jest przedsięwziąć działania celem wykluczenia ryzyka ich utraty.
3. Osoba która utraciła posiadane klucze do pomieszczeń Administratora, w których przetwarzane są dane, niezwłocznie zgłasza tę okoliczność IODO i Administratorowi.
4. IODO i Administrator podejmują wszelkie niezbędne środki techniczne organizacyjne w celu zabezpieczenia pomieszczenia, do którego klucze utracono.

ŚRODKI BEZPIECZEŃSTWA STOSOWANE PODCZAS PRACY Z DANYMI

§ 12.

1. Osoba przetwarzająca dane po zakończeniu pracy porządkuje swoje stanowisko zabezpieczając dokumenty i nośniki elektroniczne z danymi w specjalnie do tego przeznaczonych szafach lub pomieszczeniach.
2. Niszczenie dokumentów zawierających dane odbywa się jedynie za pomocą niszczarki lub za pośrednictwem firmy zajmującej się niszczeniem dokumentów, po zawarciu umowy o powierzeniu przetwarzania danych osobowych.
3. Każdy dokument zawierający dane, a nieużyteczny niszczy się niezwłocznie.

4. Podczas korzystania z urządzeń wielofunkcyjnych należy zachować szczególną ostrożność. Dokumenty kopiowane bądź skanowane wyjmowane są z urządzenia wielofunkcyjnego niezwłocznie po ich użyciu. Dotyczy to również dokumentów powstałych na skutek kopiowania bądź skanowania.
5. Przebywanie osób trzecich w obszarze, w którym przetwarzane są dane jest dopuszczalne za zgodą Administratora lub w obecności osoby upoważnionej.

POSTĘPOWANIE W RAZIE ZAISTNIENIA ZAGROŻENIA DLA BEZPIECZEŃSTWA PRZETWARZANYCH DANYCH OSOBOWYCH LUB NARUSZENIA ZASAD PRZETWARZANIA DANYCH OSOBOWYCH
§ 13.

1. Incydentem w zakresie danych osobowych jest sytuacja powodująca utratę poufności, integralności lub dostępności przetwarzanych danych.
2. Naruszeniem danych osobowych jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia jakiegokolwiek elementu systemu informatycznego, 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.
3. Każdy pracownik, który stwierdzi fakt naruszenia danych osobowych lub podejrzewa, że taka sytuacja miała miejsce, ma obowiązek podjąć czynności niezbędne do powstrzymania skutków naruszenia ochrony oraz zabezpieczyć dowody umożliwiające ustalenie przyczyn oraz skutków naruszenia.
4. W przypadku podejrzenia lub stwierdzenia naruszenia bezpieczeństwa danych należy zaniechać wszelkich działań mogących utrudnić analizę wystąpienia naruszenia i udokumentowanie zdarzenia oraz nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Inspektora Ochrony Danych Osobowych lub innej osób upoważnionych przez Administratora.
5. Wobec osoby, która naruszyła zasady ochrony danych osobowych lub w przypadku stwierdzonego naruszenia danych osobowych nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby, zgodnie z określonymi zasadami wszczyna się postępowanie dyscyplinarne, porządkowe lub karne. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych. Kara dyscyplinarna, wobec osoby dokonującej naruszenia lub uchylającej się od powiadomienia o naruszeniu danych osobowych nie wyklucza odpowiedzialności karnej z aktualnie obowiązującym przepisami oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

6. W przypadku podejrzenia lub stwierdzenia naruszenia zasad bezpieczeństwa danych osobowych lub naruszenia zabezpieczeń stosowanych przez Administratora dla ochrony przetwarzanych danych osobowych należy niezwłocznie zawiadomić IODO i Administratora.
7. W przypadku opisanym w ust. 1 przeprowadza się sprawdzenie doraźne. Sprawdzenie jest dokonywane niezwłocznie.
8. Przy dokonywaniu sprawdzenia IODO oraz osobom wyznaczonym do współpracy z nim przez Administratora przysługują uprawnienia wskazane w rozporządzeniu ministra administracji i cyfryzacji w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych, w szczególności prawo do:
   a) utrwalenia danych z systemu informatycznego służącego do przetwarzania lub zabezpieczania na informatycznym nośniku danych lub dokonania wydruku tych danych;
   b) odebrania wyjaśnień osoby, której czynności objęto sprawdzeniem;
   c) sporządzeniu kopii otrzymanego dokumentu;
   d) sporządzeniu kopii obrazu wyświetlonego na ekranie urządzenia stanowiącego część systemu informatycznego służącego do przetwarzania lub zabezpieczania danych osobowych.
9. Inspektor Ochrony Danych dokumentuje zaistniały przypadek naruszenia bezpieczeństwa danych sporządzając Raport według wzoru(Załącznik Nr 9).
10. Inspektor Ochrony Danych zasięga potrzebnych mu opinii i proponuje działania naprawcze, w tym także ustosunkowuje się do kwestii ewentualnego odtworzenia danych oraz terminu wznowienia przetwarzania danych osobowych i prowadzi Wykaz naruszeń według wzoru (Załącznik Nr 10).
11. Jeżeli IODO jest długotrwale nieobecny Administrator w przypadku, o którym mowa w ust. 1 obowiązany jest przeprowadzić postępowanie wyjaśniające i ustalające skutki oraz przyczyny naruszenia lub narażenia na naruszenie zasad bezpieczeństwa i sposobów zabezpieczenia, w sposób odpowiadający czynnościom podejmowanym przez IODO w przypadku sprawdzenia doraźnego.

§ 14
POSTĘPOWANIE W SYTUACJI NARUSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

1. IODO podejmuje decyzje o wprowadzeniu zmian w środkach zabezpieczeń fizycznych oraz w systemie organizacji pracy, stosownie do mogących ponownie wystąpić naruszeń bezpieczeństwa danych osobowych.
2. ASI podejmuje decyzje odnośnie zmian w sposobie zabezpieczenia systemu informatycznego.
3. Administrator podejmuje decyzje o wyciągnięciu konsekwencji wobec osoby odpowiedzialnej za naruszenie zasad bezpieczeństwa.
4. IODO przekazuje do PUODO w terminie do 72 godzin, zgłoszenie zawierające informacje o stwierdzeniu naruszenia, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych:

1) w przypadku przekroczenia 72 godzinnego terminu dodatkowo do zgłoszenia dołącza wyjaśnienia,
2) w przypadku gdy informacji nie może udzielić w tym samym czasie, udziela ją sukcesywnie bez zbędnej zwłoki.

5. IODO dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze.
6. Poinformowanie bez zbędnej zwłoki osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby, tak aby umożliwić tej sobie podjęcie niezbędnych działań zapobiegawczych. Należy przekazywać informację osobom, których dane dotyczą, tak szybko, jak jest to rozsądnie możliwe, w ścisłej współpracy z PUODO, z poszanowaniem wskazówek przekazanych przez PUODO lub inne odpowiednie organy, takie jak organy ścigania. Zawiadomienie powinno przekazywać informację w jasnym i prostym języku i zawierać:
    1) opis charakteru naruszenia ochrony danych osobowych,
    2) zalecenia dla danej osoby fizycznej co do minimalizacji potencjalnych niekorzystnych skutków.
7. Poinformowanie, o którym mowa w pkt. 6 nie jest wymagane jeśli PUODO stwierdzi, że spełniony został jeden z poniższych warunków:
    1) Administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych,
    2) Administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą,
    3) wymagałoby ono niewspółmiernie dużego wysiłku - w takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

PROCEDURY NADAWANIA UPRAWNIEŃ DO PRZETWARZANIA DANYCH I REJESTROWANIA TYCH UPRWANIEŃ W SYSTEMIE INFORMATYCZNYM
§ 15.

Użytkownikowi systemu informatycznego zostaje nadany dostęp na podstawie „Karty dostępu (zmiany) do przetwarzania danych w systemie informatycznym", stanowiącej Załącznik Nr 11 do niniejszej Polityki, która to karta może mieć formę elektronicznego zapisu w systemach ASI, po uprzednim:

1. Zapoznaniu z przepisami dotyczącymi ochrony danych osobowych.
2. Podpisaniu oświadczenia o zapoznaniu się z niniejszą dokumentacją przetwarzania danych osobowych.
3. Podpisaniu oświadczenia o zachowaniu informacji (w tym danych osobowych), do których użytkownik będzie miał dostęp podczas wykonywania obowiązków służbowych lub

zobowiązań umownych oraz środków ich zabezpieczania w tajemnicy (również po ustaniu łączącej strony umowy), w tym powstrzymanie się od wykorzystywania ich w celach pozasłużbowych.
4. Otrzymaniu upoważnienia do przetwarzania danych osobowych.

POLITYKA HASEŁ
§ 16.

1. Każdy użytkownik systemu informatycznego musi posiadać unikalny identyfikator i wprowadzone przez siebie hasło autoryzujące jego osobę w systemie informatycznym.
2. Hasła użytkowników lub inne dane uwierzytelniające podlegają szczególnej ochronie.
3. Użytkownik ponosi pełną odpowiedzialność za utworzenie hasła (prócz pierwszego hasła do systemu nadawanego przez Administratora Systemu Informatycznego) i jego przechowywanie.
4. Każdy użytkownik posiadający dostęp do systemów informatycznego Administratora jest obowiązany do:
   1) zachowania w poufności wszystkich swoich haseł lub innych danych uwierzytelniających wykorzystanych do pracy w systemie informatycznym;
   2) niezwłocznej zmiany haseł w przypadkach zaistnienia podejrzenia lub rzeczywistego ujawnienia;
   3) niezwłocznej zmiany hasła tymczasowego, przekazanego przez Administratora Systemu Informatycznego;
   4) poinformowania Administratora Systemu Informatycznego oraz Inspektora Danych Osobowych o podejrzeniu lub rzeczywistym ujawnieniu hasła;
   5) stosowania haseł o minimalnej długości 8 znaków, zawierających kombinację małych i dużych liter oraz cyfr lub znaków specjalnych;
   6) stosowania haseł nie posiadających w swojej strukturze części loginu;
   7) stosowania haseł nie będących zbliżonych do poprzednich (np.Tomasz$2013 - Tomasz$2014);
   8) zmiany wykorzystywanych haseł nie rzadziej niż raz na 30 dni.
5. Hasła zachowują swoją poufność również po ustaniu ich użyteczności.
6. Zabronione jest:
   1) zapisywanie haseł w sposób jawny i umieszczania ich w miejscach dostępnych dla innych osób;
   2) stosowanie haseł opartych na skojarzeniach, łatwych do odgadnięcia lub wywnioskowania z informacji dotyczących danej osoby, np. imiona, numery telefonów, daty urodzenia itp.;
   3) używanie tych samych haseł w różnych systemach operacyjnych i aplikacjach;
   4) udostępnianie haseł innym użytkownikom;
   5) przeprowadzanie prób łamania haseł;
   6) wpisywanie haseł „na stałe” (np. w skryptach logowania) oraz wykorzystywania opcji autozapamiętywania haseł (np. w przeglądarkach internetowych);

7) po trzykrotnym, błędnym wprowadzeniu hasła użytkownik jest zobowiązany zgłosić ten fakt do Administratora Systemu Informatycznego, w celu zresetowania hasła dostępowego.

ZASADY POSTĘPOWANIA Z KLUCZAMI KRYPTOGRAFICZNYMI
§ 17.

1. W systemach obsługujących transmisję danych osobowych wrażliwych lub informacji poufnych Administratora powinny być wykorzystywane klucze kryptograficzne służące do zabezpieczenia danych.
2. Przekazywanie kluczy użytkownikom powinno odbywać się w sposób protokolarny, o ile nie następuje w drodze teletransmisji.
3. Obowiązkiem użytkownika jest zabezpieczenie kluczy (prywatnych) przed dostępem osób nieupoważnionych.
4. W przypadku stwierdzenia ujawnienia klucza osobie nieupoważnionej lub podejrzenia o jego ujawnienie należy bezzwłocznie powiadomić Administratora Systemu Informatycznego oraz Inspektora Danych Osobowych.
5. Dane osobowe wrażliwe lub informacje poufne Administratora, do których nie stosuje się kluczy kryptograficznych, można przesyłać wyłącznie pocztą elektroniczną po uaktywnieniu funkcji podpisywania i szyfrowania pliku.
6. Każdy użytkownik korzystający z kluczy kryptograficznych jest zobowiązany do ich użytkowania i przechowywania w sposób uniemożliwiający utratę lub dostęp osób niepowołanych.
7. W przypadku podejrzenia lub rzeczywistego naruszenia bezpieczeństwa klucza fakt ten należy niezwłocznie zgłosić Administratorowi Systemu Informatycznego oraz Inspektorowi Ochrony Danych.

PROCEDURA ROZPOCZĘCIA, ZAWIESZENIA, PROWADZENIA I ZAKOŃCZENIA PRACY W SYSTEMIE INFORMATYCZNYM
§ 18.

1. Rozpoczęcie pracy w systemie informatycznym następuje po wprowadzeniu unikalnego identyfikatora i hasła.
2. Zawieszenie pracy w systemie informatycznym tj. brak wykonywania jakichkolwiek czynności przez okres 5 minut w systemie informatycznym powoduje automatycznie uruchomienie systemowego wygaszacza ekranu blokowanego hasłem. Zastosowanie powyższego mechanizmu nie zwalnia użytkownika z obowiązku każdorazowego blokowania ekranu wygaszaczem chronionym hasłem po odejściu od stanowiska.
3. W sytuacji gdy wgląd w wyświetlane na monitorze dane może mieć nieuprawniona osoba należy tymczasowo zmienić widok wyświetlany na monitorze lub obrócić monitor (przymknąć ekran laptopa) w sposób uniemożliwiający wgląd w wyświetlaną treść.
4. Przed zakończeniem pracy należy upewnić się czy dane zostały zapisane, aby uniknąć ich utraty danych.

5. Po zakończeniu pracy, użytkownik obowiązany jest wylogować się z systemu informatycznego przetwarzającego dane osobowe i z systemu operacyjnego, zabezpieczyć nośniki informacji (elektroniczne i papierowe) oraz wyłączyć komputer.
6. Użytkownik systemu informatycznego przetwarzającego dane osobowe niezwłocznie powiadamia administratora systemu w przypadku, gdy:
   1) Wygląd systemu, sposób jego działania, zakres danych lub sposób ich przedstawienia przez system informatyczny odbiega od standardowego stanu uznawanego za typowy dla danego systemu informatycznego;
   2) Niektóre opcje, dostępne użytkownikowi w normalnej sytuacji, przestały być dostępne lub też opcje niedostępne użytkownikowi w normalnej sytuacji, stały się dostępne.

ZASADY KORZYSTANIA ZE SŁUŻBOWEJ POCZTY ELEKTRONICZNEJ
§ 19.

1. Użytkownikowi zostaje nadany dedykowany adres skrzynki poczty elektronicznej działający w domenie Administratora.
2. Informacja o służbowym adresie skrzynki pocztowej jest jawna i dostępna powszechnie, w tym może być dostępna na łamach witryny internetowej Administratora w postaci książki adresowej.
3. Nadany użytkownikowi adres skrzynki poczty elektronicznej służy wyłącznie do realizacji celów służbowych lub umownych. Korespondencja realizowana drogą elektroniczną z wykorzystaniem systemów informatycznych Administratora podlega rejestrowaniu i może być monitorowana. Informacje przesyłane za pośrednictwem sieci Administratora (w tym do i z Internetu) nie stanowią własności prywatnej użytkownika.
4. Wszelka korespondencja elektroniczna prowadzona przez pracownika, a niezwiązana z działalnością Administratora, powinna być prowadzona przez prywatną skrzynkę poczty elektronicznej użytkownika.
5. Użytkownicy mają prawo korzystać z systemu poczty elektronicznej dla celów prywatnych wyłącznie okazjonalnie i powinno być to ograniczone do niezbędnego minimum.
6. Korzystanie z systemu poczty elektronicznej dla celów prywatnych nie może wpływać na jakość i ilość świadczonej przez użytkownika pracy oraz na prawidłowe i rzetelne wykonywanie przez niego obowiązków służbowych lub umownych, a także na wydajność systemu poczty elektronicznej.
7. Zabronione jest:
   1) wysyłanie bez zgody Administratora materiałów służbowych zawierających chronione dane na konta prywatne (np. celem pracy nad dokumentami poza miejscem pracy);
   2) wykorzystywanie systemu poczty elektronicznej do działań mogących zaszkodzić wizerunkowi Administratora;
   3) odbieranie przesyłek z nieznanych źródeł;
   4) otwieranie załączników z plikami samorozpakowującymi się bądź wykonalnymi typu exe, com, itp.;
   5) przesyłanie pocztą elektroniczną plików wykonywalnych typu: bat, com, exe, plików multimedialnych oraz plików graficznych bez zgody Administratora;
   6) ukrywanie lub dokonywanie zmian tożsamości nadawcy;

7) czytanie, usuwanie, kopiowanie lub zmiana zawartości skrzynek pocztowych innego użytkownika;
8) odpowiadanie na niezamówione wiadomości reklamowe lub wysyłane łańcuszki oraz na inne formy wymiany danych określanych spamem; w przypadku otrzymania takiej wiadomości należy przesłać ją administratorowi systemu informatycznego;
9) posługiwanie się adresem służbowym e-mail w celu rejestrowania się na stronach handlowych, informacyjnych, chat'ach lub forach dyskusyjnych, które nie dotyczą zakresu wykonywanej pracy lub obowiązków umownych;
10) wykorzystywanie poczty elektronicznej do reklamy prywatnych towarów lub usług, działalności handlowo-usługowej innej niż wynikającej z potrzeb Administratora lub do poszukiwania dodatkowego zatrudnienia.

ZASADY KORZYSTANIA Z SIECI PUBLICZNEJ (INTERNET)
§ 20.

1. Zdalne korzystanie z systemów informatycznych poprzez sieć publiczną może mieć miejsce po zastosowaniu systemu uwierzytelniania użytkownika i szyfrowanego kanału transmisji.
2. Zdalny dostęp do serwerów w celach administracyjnych może mieć miejsce po zastosowaniu systemu uwierzytelniania użytkownika i szyfrowanego kanału transmisji.
3. Dostęp użytkowników do sieci publiczne (Internet) powinien być ograniczony do niezbędnego minimum na danym stanowisku pracy.
4. Wprowadza się całkowity zakaz w dostępie do treści niezgodnych z prawem lub niestosownych, a w szczególności pornograficznych, rasistowskich, traktujących o przemocy, przestępstwach, jak również do protokołów umożliwiających wymianę plików w sieciach z naruszeniem przepisów prawa.

ZASADY POSTĘPOWANIA Z NOŚNIKAMI ELEKTRONICZNYMI ORAZ VPN PODCZAS PRACY POZA OBSZAREM PRZETWARZANIA DANYCH
§ 21.

Każdy użytkownik wymiennych nośników elektronicznych oraz użytkownicy zdalnych dostępów do sieci służbowej Administratora (VPN) oraz użytkownicy elektronicznych kart dostępu ponoszą całkowitą odpowiedzialność za powierzony do użytkowania sprzęt oraz są obowiązani do stosowania się do poniższych zasad:

1) Zabrania się pozostawiania bez opieki w miejscach publicznych nośników wymiennych przetwarzających informacje Administratora;
2) Komputery przenośne należy przewozić jako bagaż podręczny i w miarę możliwości maskować je;
3) Użytkownik wykonując czynności zawodowe lub umowne poza stałym miejscem wykonywania obowiązków powinien zadbać o należyte zabezpieczenie powierzonego sprzętu oraz dostępu do informacji przed nieautoryzowanym dostępem osób trzecich;
4) Zabrania się spożywania posiłków i picia podczas pracy z powierzonym sprzętem;

5) Zabrania się udostępniania osobom trzecim nośników elektronicznych informacji oraz powierzonego sprzętu będącego własnością Klubu dziecięcego w Chrzypsku Wielkim.
6) W przypadku utraty nośnika elektronicznego lub sprzętu komputerowego należy ten fakt bezzwłocznie zgłosić do bezpośredniego przełożonego lub administratora systemu informatycznego. Bezpośredni przełożony lub administrator systemu informatycznego bezzwłocznie zgłaszają taki fakt do Inspektora Danych Osobowych, ponieważ zagubienie nośnika przetwarzającego dane może wiązać się z utratą poufności informacji chronionych przez Administratora;
7) Problemy wynikające z nieprawidłowego funkcjonowania sprzętu komputerowego należy zgłaszać administratorowi systemu informatycznego.

UŻYTKOWANIE SPRZĘTU KOMPUTEROWEGO, OPROGRAMOWANIA, NOŚNIKÓW DANYCH
§ 22.

1. Do sprzętu komputerowego zalicza się między innymi:
   1) komputery stacjonarne,
   2) komputery przenośne,
   3) tablety,
   4) smartphony,
   5) drukarki,
   6) modemy,
   7) monitory,
   8) routery,
   9) osprzęt dostarczony razem z wyżej wymienionym sprzętem lub zakupiony oddzielnie, a w szczególności: zasilacze, torby, klawiatury, myszki komputerowe.
2. Administrator udziela pomocy użytkownikowi w obsłudze sprzętu i oprogramowania.
3. W przypadku niepoprawnego i niezgodnego z przeznaczeniem użytkowania przez użytkownika sprzętu komputerowego, administrator systemu informatycznego informuje o powyższym Inspektora Ochrony Danych Osobowych.
4. Użytkownik jest zobowiązany do dbałości o sprzęt oraz oprogramowanie, a także odpowiedzialny za zabezpieczenie go przed używaniem przez osoby nieuprawnione oraz do ochrony przed kradzieżą lub zagubieniem.
5. Użytkownik nie może samodzielnie zmieniać konfiguracji przekazanego sprzętu komputerowego oraz instalować, usuwać oprogramowania, w tym nie może używać na przekazanym sprzęcie prywatnego oprogramowania.

KORZYSTANIE Z URZĄDZEŃ KOMUNIKACJI GŁOSOWEJ I WIZYJNEJ
§ 23.

1. Każdy użytkownik zobowiązany jest do przestrzegania zakazu prowadzenia rozmów, podczas których może dochodzić do wymiany informacji danych osobowych lub informacji

poufnych Administratora, jeśli rozmowy te odbywają się w miejscach publicznych, otwartych pomieszczeniach biurowych lub takich, które nie gwarantują zachowania poufności rozmów.
2. Odczytanie wiadomości z faksów, automatycznych sekretarek lub systemów poczty głosowej powinno być możliwe wyłącznie po wprowadzeniu indywidualnego hasła. W przypadku braku takiej możliwości urządzenia należy zabezpieczyć przed dostępem osób nieuprawnionych.
3. Zabronione jest wykorzystywanie domyślnych („fabrycznych") haseł dla ww. urządzeń.
4. Przekazywanie za pomocą urządzeń faksowych dokumentów zawierających dane osobowe wrażliwe lub informacje poufne Administratora jest zabronione.
5. Drukarki nie mogą być pozostawione bez kontroli, jeśli są wykorzystywane (lub wkrótce będą) do drukowania dokumentów zawierających informacje wrażliwe.

OCHRONA PRZED SZKODLIWYM OPROGRAMOWANIEM
§ 24.

1. Zidentyfikowanymi obszarami systemu informatycznego Administratora narażonymi na ingerencję wirusów oraz innego szkodliwego oprogramowania są dyski twarde lub karty pamięci urządzeń, pamięć RAM oraz elektroniczne nośniki informacji.
2. Drogą przedostania się wirusów lub szkodliwego oprogramowania może być sieć publiczna, wewnętrzna sieć teleinformatyczna lub elektroniczne nośniki informacji.
3. Użytkownicy systemu mają obowiązek skanowania każdego zewnętrznego elektronicznego nośnika informacji, który chcą wykorzystać.
4. W przypadku stwierdzenia pojawienia się wirusa i braku możliwości usunięcia go przez program antywirusowy, użytkownik powinien skontaktować się z administratorem systemu informatycznego.

ZARZĄDZANIE RYZYKIEM BEZPIECZEŃSTWA INFORMACJI I CIĄGŁOŚCI DZIAŁANIA
§ 25.

1. Proces zarządzania ryzykiem jest procesem stałym natomiast, podprocesy szacowania i oceny ryzyka przeprowadza się nie rzadziej niż raz na 12 miesięcy oraz każdorazowo w przypadku:
    a. wprowadzenia nowego procesu, istotnego z punktu widzenia zachowania ciągłości działania lub zapewnienia bezpieczeństwa przetwarzanych informacji,
    b. modyfikacji istniejącego procesu istotnego z punktu widzenia zachowania ciągłości działania lub zapewnienia bezpieczeństwa przetwarzanych informacji;
    c. istotnej zmiany w kontekście funkcjonowania Jednostki.
2. Proces zarządzania ryzykiem składa się z następujących podprocesów:
    a. identyfikacji ryzyka,
    b. szacowania (analiza) ryzyka,
    c. cceny ryzyka.

3. Identyfikacja ryzyka ma za zadanie dostarczyć informacji w jakich obszarach działań znajdują się ryzyka, mogące wpływać na działalność Jednostki. Do identyfikacji ryzyka wykorzystywany jest katalog wskzany poniżej.

Lp.	Kategoria ryzyka	Zagrożenie
1	Zagrożenia fizyczne	Ogień
2	Zagrożenia fizyczne	Woda
3	Zagrożenia fizyczne	Zanieczyszczenia, szkodliwe promieniowanie
4	Zagrożenia fizyczne	Poważny wypadek
5	Zagrożenia fizyczne	Eksplozja
6	Zagrożenia fizyczne	Pył, korozja, zamarzanie
7	Zagrożenia naturalne	Zjawisko klimatyczne
10	Zagrożenia naturalne	Zjawisko meteorologiczne
11	Zagrożenia naturalne	Powódź
12	Zagrożenia naturalne	Zjawisko pandemii / epidemii
13	Awarie infrastruktury	Awaria systemu zasilania
14	Awarie infrastruktury	Awaria chłodzenia lub wentylacji
15	Awarie infrastruktury	Utrata zasilania
16	Awarie infrastruktury	Awaria sieci telekomunikacyjnej
17	Awarie infrastruktury	Awaria sprzętu telekomunikacyjnego
18	Awarie infrastruktury	Promieniowanie elektromagnetyczne
19	Awarie infrastruktury	Promieniowanie cieplne
20	Awarie infrastruktury	Impulsy elektromagnetyczne
21	Awarie techniczne	Uszkodzenie urządzenia lub systemu
22	Awarie techniczne	Przeciążenie systemu informacyjnego
23	Awarie techniczne	Naruszenie możliwości utrzymania systemu inform.
24		
25	Działania ludzkie	Atak terrorystyczny, sabotaż
26	Działania ludzkie	Inżynieria społeczna
27	Działania ludzkie	Przechwytywanie promieniowania urządzenia
28	Działania ludzkie	Zdalne szpiegowanie
29	Działania ludzkie	Podsłuch
30	Działania ludzkie	Kradzież nośników lub dokumentów
31	Działania ludzkie	Kradzież sprzętu
32	Działania ludzkie	Kradzież tożsamości cyfrowej lub danych uwierzytelniających
33	Działania ludzkie	Odzyskiwanie nośników poddanych recyklingowi lub wyrzuconych.
34	Działania ludzkie	Ujawnianie informacji
35	Działania ludzkie	Dane wprowadzane z niewiarygodnych źródeł
36	Działania ludzkie	Manipulowanie przy urządzeniach
37	Działania ludzkie	Ingerencja w oprogramowanie
38	Działania ludzkie	Eksploity typu drive-by-exploits wykorzystujące komunikację internetową
39	Działania ludzkie	Atak typu replay, atak typu man-in-the-middle
40	Działania ludzkie	Nieuprawnione przetwarzanie danych osobowych

41	Działania ludzkie	Nieuprawnione wejście do obiektów
42	Działania ludzkie	Nieuprawnione użycie urządzeń
43	Działania ludzkie	Niewłaściwe użycie urządzeń
44	Działania ludzkie	Uszkodzenie urządzeń lub nośników
45	Działania ludzkie	Nielegalne kopiowanie oprogramowania
46	Działania ludzkie	Używanie podrobionego lub skopiowanego oprogramowania
47	Działania ludzkie	Uszkodzenie danych
48	Działania ludzkie	Nielegalne przetwarzanie danych
49	Działania ludzkie	Wysyłanie lub rozpowszechnianie złośliwego oprogramowania
50	Działania ludzkie	Wykrywanie położenia
51	Kompromitacja funkcji lub usług	Błąd w użyciu
52	Kompromitacja funkcji lub usług	Nadużywanie praw lub uprawnień
53	Kompromitacja funkcji lub usług	Fałszowanie praw lub uprawnień
54	Kompromitacja funkcji lub usług	Zaprzeczanie działaniom
55	Zagrożenia organizacyjne	Brak personelu
56	Zagrożenia organizacyjne	Brak zasobów
57	Zagrożenia organizacyjne	Niewydolność dostawców usług
58	Zagrożenia organizacyjne	Naruszenie prawa lub przepisów

4. W procesie identyfikacji ryzyka należy uwzględniać także zdarzenia historyczne, które miały miejsce w lokalizacji Jednostki, ale także w innych podobnych podmiotach, jeżeli dostęp do takich informacji jest ogólnodostępny lub udostępniony przez inne podmioty:
    a. krokiem pierwszym jest identyfikacja ryzyka związanego z bezpieczeństwem informacji i ciągłością działania dla aktywów informacyjnych / zasobów;
    b. identyfikowane ryzyko może mieć negatywny wpływ i wtedy jest nazywane zagrożeniem lub pozytywny wpływ i wtedy nazywane jest szansą; zidentyfikowane ryzyko opisywane jest w modelu trzyelementowym: przyczyna – ryzyko – skutek;
    c. krokiem drugim jest określenie aktualnie wdrożonych zabezpieczeń, które ograniczają zidentyfikowane ryzyko.
5. Szacowanie (analiza) ryzyka polega na wskazaniu zagrożeń, które mogą się zmaterializować w danym procesie lub w komórce organizacyjnej.
6. Ocenę prawdopodobieństwa wystąpienia zagrożenia dla każdego z obszarów przedstawia się w sposób ogólny zgodnie ze skalą przedstawioną w tabeli poniżej:

Poziom	**Wartość**	**Opis**
5 (Bardzo wysokie)	0,85	Jesteśmy absolutnie przekonani, że jeżeli nic nie zrobimy to tak się stanie. Istnieją racjonalne przesłanki by ocenić, że zagrożenie raczej się zmaterializuje.

		Zagrożenie jest realne. Prawdopodobieństwo: 85-100%
4 **(Wysokie)**	0,65	Jesteśmy przekonani, że jeżeli nic nie zrobimy to tak się stanie. Mieliśmy już z tym zagrożeniem problemy (występowało w przeszłości), nie zabezpieczyliśmy się przed tym zagrożeniem, stanowi ono dla nas ważny problem. Wysoce prawdopodobne że zagrożenie wystąpi. Prawdopodobieństwo: 65-84%
3 **(Średnie)**	0,50	Wystąpienie zagrożenia jest realne. Materializacja zagrożenia oceniamy na okolice 50% Materializowało się sporadycznie w przeszłości w ciągu ostatnich 2 - 3 lat Prawdopodobieństwo: 36-64%
2 **(Niskie)**	0,35	Zagrożenie materializowało się sporadycznie w przeciągu ostatnich 5 lat. Zagrożenie jest niskie ale ciągle występuje. Prawdopodobieństwo: 16 – 35%
1 **(Bardzo niskie)**	0,15	Bardzo małe prawdopodobieństwo że zagrożenie wystąpi nie mniej jednak jest realne. Prawdopodobieństwo: 0 – 15%

7. Ocenę skutków materializacji zagrożenia przedstawia się w pięciostopniowej skali, zgodnie z poniższą tabelą:

Poziom	**Wartość**	**Opis**
5 **(Bardzo wysokie)**	10	Katastrofalne skutki finansowe, konsekwencje prawne, przerwanie procesów biznesowych oraz ciągłości działania i usług wpływające na Klientów/Petentów i tym samym na wizerunek jak i funkcjonowanie Jednostki. Praktycznie brak możliwości zachowania pełnej ciągłości działania
4 **(Wysokie)**	8	Poważne skutki finansowe, konsekwencje prawne, przerwanie procesów biznesowych wpływające na Klientów/Petentów i tym samym na wizerunek Jednostki. Poważne problemy z zachowaniem ciągłości działania i usług.
3 **(Średnie)**	5	Przeciętne skutki finansowe, konsekwencje prawne, przerwanie procesów biznesowych wpływające na Klientów/Petentów Urzędu i tym samym na wizerunek Jednostki. Niewielkie trudności w zachowaniu ciągłości działania.
2 **(Średnie)**	2	Małe skutki finansowe (kilka-kilkanaście tysięcy zł, zakłócenia procesów biznesowych, które nie wpływają na Klientów/Petentów. Ciągłość działania zachowana.
1 **(Niskie)**	1	Drobne wewnętrzne zakłócenie procesu/działania Jednostki - brak konsekwencji finansowych / prawnych. Ciągłość działania zachowana.

8. Ocenę ryzyka przedstawia się w sposób ogólny za pomocą poniższego wzoru:

R=P x S
R-Ryzyko
S-Skutek materializacji zagrożenia

P-Prawdopodobieństwo materializacji zagrożenia

9. Wyznaczony podczas analizy poziom ryzyka jest porównywany z określonym progiem akceptowalności, w celu określenia sposobu postępowania z ryzykiem

Poziom ryzyka - R	**Skutki – S (1-5)**				
Prawdopodobieństwo - P (1-5)	**1 (1)**	**2 (2)**	**3 (5)**	**4 (8)**	**5 (10)**
1 (0,15)	0,15	0,3	0,75	1,2	1,5
2 (0,35)	0,35	0,7	1,75	2,8	3,5
3 (0,50)	0,5	1,0	2,5	4	5
4 (0,65)	0.65	1,3	3,25	5,2	6,5
5 (0,85)	0,85	1,7	4,25	5,2	8,5

10. Macierz do oceny ryzyka pozwala na określenie poziomu ryzyka. Zidentyfikowane zostały trzy poziomy ryzyka: niskie, średnie i wysokie. Zależność ryzyka od parametrów „prawdopodobieństwo" i „skutki" obrazuje poniższa tabela:

Poziom	**Wartość**
Wysokie	Większe lub równe 4,25
Średnie	Większe lub równe 1,2
Niskie	Większe lub równe 0

11. Przyjmuje się następujące podejście do akceptowania ryzyka:

Poziom ryzyka	
Wysokie	Ryzyko nieakceptowalne. Akceptacja możliwa jest decyzją Kierownika Jednostki. Wymaga natychmiastowego zaplanowania i podjęcia działania.
średnie	Ryzyko nieakceptowalne. Akceptacja możliwa jest decyzją Właściciela ryzyka. Wymaga zaplanowania działania.
Niskie	Ryzyko akceptowalne. Nie wymaga planowania i podejmowania działania.

12. Zaplanowanie działań związanych z analizowanym ryzykiem jest konieczne w przypadku, kiedy ryzyko nie jest akceptowalne. Należy wtedy stworzyć Plan

postępowania z ryzykiem określając jakie działania zostaną podjęte, kto będzie odpowiedzialny za ich realizację i do kiedy mają zostać zrealizowane.

13. Następnie zalecane jest ocena ryzyka rezydualnego, czyli poziomu ryzyka po realizacji planu postępowania z ryzykiem i wprowadzeniu zabezpieczeń. Aby tego dokonać należy oszacować rezydualne prawdopodobieństwo i rezydualny skutek. Jeżeli ryzyko rezydualne nie jest akceptowalne, należy dokonać modyfikacji planu postępowania z ryzykiem i ponowić ocenę ryzyka rezydualnego.
14. Ostatnim krokiem jest opracowanie raportu z analizy ryzyka, który przedstawia się organowi założycielskiemu/prowadzącemu/nadzorczemu.

ZASADY BEZPIECZEŃSTWA
§ 27.

a. Zasady bezpieczeństwa fizycznego, technicznego i środowiskowego

1) Zabezpieczenia zewnętrzne w danej lokalizacji powinny obejmować m.in. takie obszary jak zewnętrzne ciągi komunikacyjne – ciągi piesze, podjazdy dla karetek, drogi dojazdowe, parkingi, poczekalnie. Wdrażając środki zabezpieczeń należy w szczególności uwzględnić:
    a) odpowiednią jakość oświetlenia – co oznacza zapewnienie możliwości identyfikacji poszczególnych osób, zapewnienie światła o właściwym natężeniu tak, aby zapewnić odpowiedni rozkład luminancji, zapobiegając zjawiskom olśnienia i kontrastu;
    b) stan i architekturę zabezpieczeń budowlano-mechanicznych budynków, ścian, drzwi, okien, bram, włazów dachowych;
    c) podniesione krawężniki, ciężkie gazony lub ciągi słupków zabezpieczających lub inne elementy ograniczające, w przypadku gdy wprowadzenie wskazanych zabezpieczeń jest konieczne po oszacowaniu ryzyka.
2) Parkowanie samochodów prywatnych, służbowych na obszarze przynależącym do lokalizacji powinno odbywać się zgodnie z powszechnie obowiązującymi przepisami prawa.
3) Pomieszczenia, w których przetwarzane są informacje powinny być wyposażone w odpowiednie miejsca służące przechowywaniu nośników tych informacji – adekwatne do klasy informacji w nich przechowywanych.
4) Należy sprawować stały nadzór nad punktami dostępu, w szczególności takimi, jak obszary dostaw, wejścia, recepcje oraz innymi punktami, przez które nieuprawnione osoby mogą wejść do pomieszczeń (w szczególności znajdujących się w strefie chronionej i administracyjnej). Jeżeli jest to możliwe, wskazane punkty dostępu należy odizolować od miejsc przetwarzania i/lub przechowywania informacji stanowiących tajemnicę Urzędu /informacji wrażliwych lub prawnie chronionych, aby zapobiec nieuprawnionemu dostępowi do wymienionych wyżej informacji.

b. Wytyczne dla bezpieczeństwa okablowania strukturalnego

1) Okablowanie zasilające oraz telekomunikacyjne lub wspomagające usługi informacyjne powinno być chronione przed przechwyceniem, nieautoryzowanym wpięciem, zakłóceniem lub uszkodzeniem.
2) W skład systemów okablowania w zakresie konstrukcyjno-mechanicznym wchodzą w szczególności:
    a. trakty kablowe (listwy PCV, szyny, rury, przepusty);
    b. szafy dystrybucyjne;
    c. tablice;
    d. krosownice.
3) Okablowanie powinno być poprowadzone w miejscach bezpiecznych (jeżeli jest to możliwe, linie zasilające oraz telekomunikacyjne powinny być prowadzone pod ziemią), tj. z dala od korytarzy, przejść i ciągów komunikacyjnych. Jeżeli zachodzi konieczność poprowadzenia okablowania w miejscach użyteczności, to muszą być one poprowadzone w rynnach zabezpieczających.
4) Kable powinny być odpowiednio zorganizowane, zapewniając bezpieczeństwo oraz dostępność tj.:
    a. okablowanie prowadzące do tego samego urządzenia powinno być zabezpieczone specjalną tubą osłonową;
    b. grupy kabli biegnących obok siebie powinny być powiązane za pomocą pasków uciskowych (np. w serwerowni);
    c. kable powinny być odpowiednio podwieszone, przy stanowiskach ze sprzętem, w sposób który zapobiega ich prowadzeniu po podłodze.
5) Dla systemów krytycznych należy:
    a. instalować zbrojone rury kablowe i w zamykanych pomieszczeniach lub szafkach w punktach kontrolnych i zakończeń,
    b. korzystać z ekranów elektromagnetycznych w celu ochrony kabli,
    c. kontrolować dostęp do paneli połączeniowych i pomieszczeń z okablowaniem.
6) Wszystkie systemy okablowania powinny podlegać okresowym przeglądom.
7) Należy wyznaczyć osobę/osoby odpowiedzialne za przeprowadzanie przeglądu.
8) Zakres przeglądu powinien w szczególności zawierać:
    a. sprawdzenie stanu technicznego (konstrukcyjno-mechanicznego) elementów systemu okablowania;
    b. sprawdzenie zabezpieczeń elektronicznych dla systemów okablowania polegające na sprawdzeniu poprawności funkcjonowania np. elektronicznych systemów kontroli dostępu zastosowanych do zabezpieczenia szaf dystrybucyjnych, krosownic lub innych urządzeń.
9) Przeglądy powinny zostać przeprowadzane w szczególności poprzez:
    a. sprawdzenie mocowania listew traktów kablowych, w miejscach ogólnie dostępnych, np. narażonych na uszkodzenia mechaniczne, spowodowane przez przenoszenie przedmiotów o dużych gabarytach (biurko, szafa) lub ruch osobowy;
    b. sprawdzenie zamknięcia szaf, tablic, osłon włazów i studzienek zlokalizowanych zarówno wewnątrz jak i poza budynkiem;

c. sprawdzenie czy występują ślady po próbach ingerencji osób nieuprawnionych, itp.;
d. sprawdzenie poszczególnych elementów konstrukcyjno-mechanicznych systemów okablowania powinno opierać się na porównaniu stanu faktycznego (rzeczywistego) z opisem w dokumentacji technicznej;
e. przestrzegania zasad ochrony okablowania oraz punktów połączeń okablowania pod kątem zidentyfikowania podłączonych nieautoryzowanych urządzeń przechwytujących, rejestrujących, transmitujących i zniekształcających sygnał transmisyjny;
f. stanu technicznego instalacji poprzez wykonanie pomiarów okablowania.

10) W przypadku rozbieżności pomiędzy stanem rzeczywistym, a dokumentacją techniczną należy niezwłocznie dokonać aktualizacji dokumentacji technicznej lub przywrócić instalację do stanu opisanego w dokumentacji technicznej.
11) W przypadku stwierdzenia nieautoryzowanej ingerencji w okablowanie lub próby ingerencji poprzez zniszczenie, przechwycenie, wpięcie i inne należy niezwłocznie poinformować właściwe organy śledcze.

c. Wytyczne bezpieczeństwa dla systemów alarmowych

1) Podmiot zajmujący się instalacją systemów, z chwilą przekazania systemów do eksploatacji, powinien dostarczyć poświadczenie zgodności stwierdzające, że systemy zostały zainstalowane zgodnie z dokumentacją powykonawczą.
2) Po zakończeniu instalacji systemów zabezpieczeń należy je uruchomić i sprawdzić zgodność ze specyfikacją i poziomami funkcjonalności określonymi na etapie projektowania.
3) W przypadku systemów połączonych z wykorzystaniem łącz WiFi (innych bezprzewodowych) należy dbać o wprowadzenie silnych haseł oraz innych zabezpieczeń minimalizujących / uniemożliwiających dostęp do tych urządzeń osobom trzecim.
4) Każde włamanie do elektronicznych systemów bezpieczeństwa fizycznego należy traktować jako incydent krytyczny / bardzo poważny i niezwłocznie informować odpowiednie służby / organy.
5) Po przekazaniu danego systemu do eksploatacji powinien być on poddany testowaniu.
6) Należy wyznaczyć Administratora/Administratorów systemów alarmowych.
7) Administratorzy poszczególnych systemów i – jeżeli to właściwe - ich użytkownicy przed oddaniem systemu do użytkowania powinni uczestniczyć w demonstracji działania danego systemu, łącznie z obsługą urządzeń do sygnalizacji napadu, kontroli dostępu i wizji, z pokazaniem sposobów ich testowania i objaśnieniem procedur komunikacji.
8) Wszystkie systemy powinny zawierać przejrzystą i zwięzłą instrukcję obsługi, zawierającą opis właściwych procedur włączania i wyłączania poszczególnego systemu. Dostęp do instrukcji powinny posiadać wszystkie osoby odpowiedzialne za obsługę danego systemu.
9) Dokumentacja systemów alarmowych powinna zawierać informacje dotyczące:
    a. firmy instalacyjnej: nazwa, adres i numer telefonu firmy bądź dane konkretnego instalatora;

   b. firmy serwisowej odpowiedzialnej za konserwację i naprawy: nazwa, adres i numer telefonu firmy bądź dane osoby odpowiedzialnej za konserwację i/lub naprawy, włącznie ze szczegółową informacją, jak można skontaktować się z tą firmą lub jej dyżurnym przedstawicielem przez całą dobę;
   c. firmy prowadzącej centrum monitoringu: nazwa, adres i numer telefonu centrum monitoringu odpowiedzialnego za reakcję na sygnały alarmowe;
   d. zasad weryfikacji przez centrum monitoringu zgłaszanych sygnałów: szczegóły wszelkich procedur związanych z weryfikacją stanu alarmu;
   e. firmy podejmującej interwencje: nazwa, adres i numer telefonu organizacji odpowiedzialnej za interwencję w miejscu chronionym w przypadku wystąpienia stanu alarmu.
10) Użytkownikom należy przeprowadzić szkolenia w zakresie obsługi, proporcjonalnie do stopnia złożoności systemów.
11) W przypadku wystąpienia działań niepożądanych należy udokumentować wszystkie działania podjęte wskutek wystąpienia stanów niepożądanych np. alarmów oraz wszelkie naprawy i modyfikacje z tym związane.
12) Należy dokumentować zapisy z systemów – co oznacza, że należy zapisywać:
   a. daty i godziny zgłoszenia stanów alarmowych;
   b. inne dane, np. z którego czujnika doszło do zgłoszenia alarmu.
13) Wszystkie systemy zabezpieczeń podlegają minimum raz na 12 miesięcy (chyba, że producent zaleca częstsze przeglądy) regularnym przeglądom technicznym dokonywanym przez osoby posiadające odpowiednie uprawnienia.
14) Wszystkie systemy zabezpieczeń muszą być systematycznie konserwowane – w tym poddawane przeglądom i serwisowaniu), zaraz po przekazaniu ich do eksploatacji, zgodnie z harmonogramem uzgodnionym z firmą instalacyjną.
15) Przeglądy systemów zabezpieczeń przeprowadzane są każdorazowo w przypadku wystąpienia incydentów zagrażających lub mogących powodować zagrożenie dla bezpieczeństwa osób i mienia.
16) Należy poinformować osoby odpowiedzialne za konserwację systemów zabezpieczeń o ich odpowiedzialności za:
   a. dopuszczenie do obsługi systemów jedynie osób wyszkolonych w tym zakresie oraz zadbanie o to, aby były obsługiwane zgodnie z instrukcjami producentów i po odbyciu stosownych szkoleń;
   b. bezzwłoczne zgłaszanie wszelkich usterek do właściwej firmy serwisowej;
   c. zgłaszanie planów wszelkich zmian aranżacyjnych w poszczególnych strefach bezpieczeństwa lub planowanych zmian w sposobie ich użytkowania.

POSTANOWIENIA KOŃCOWE
§ 28.

1. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszej Polityki potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych lub niewykonanie zobowiązania w przypadku stosunku prawnego innego niż stosunek pracy.
2. W sprawach nieuregulowanych w Polityce mają zastosowanie przepisy powszechnie obowiązującego prawa, w tym w szczególności przepisy ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych oraz Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych, zwane w skrócie RODO).
3. Polityka przetwarzania i ochrony danych osobowych jest dostępna w siedzibie Administratora.