ANALIZA SKUTKÓW OPERACJI PRZETWARZANIA DANYCH OSOBOWYCH POD KĄTEM ZAGROŻEŃ I RYZYKA ORAZ OCENA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI SYSTEMÓW PRZETWARZANIA DANYCH OSOBOWYCH

zwana dalej:

ANALIZĄ ZAGROŻEŃ I RYZYKA
PRZY PRZETWARZANIU DANYCH OSOBOWYCH

Administrator Danych Osobowych: **Tomasz Kubera i Tomasz Kuśnierczak prowadzący działalność gospodarczą w formie spółki cywilnej „EMPRESSIA" (NIP: 7872084069)**

dnia: **30 marca 2018 roku**

zgodnie z:

ROZPORZĄDZENIEM PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/679 z dnia 27 kwietnia 2016 r.
w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE
(ogólne rozporządzenie o ochronie danych)

wprowadza dokument o nazwie:
„ANALIZA SKUTKÓW OPERACJI PRZETWARZANIA DANYCH OSOBOWYCH POD KĄTEM ZAGROŻEŃ I RYZYKA ORAZ OCENA POUFNOŚCI, INTEGRALNOŚCI I ROZŁĄCZALNOŚCI SYSTEMÓW PRZETWARZANIA DANYCH OSOBOWYCH"

zwanym dalej:
„ANALIZĄ ZAGROŻEŃ I RYZYKA
PRZY PRZETWARZANIU DANYCH OSOBOWYCH"

Zapisy tego dokumentu wchodzą w życie z dniem ogłoszenia.

§ 1

Administrator Danych ze względu na ciążące na nim obowiązki zobowiązany jest do:

1) wdrożenia środków technicznych i organizacyjnych, celem zapewnienia, że dane osobowe są przez niego przetwarzane zgodnie z obowiązującymi przepisami,
2) przetwarzania danych osobowych zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą,
3) zbierania danych osobowych wyłącznie w konkretnych, wyraźnych i prawnie uzasadnionych celach oraz nieprzetwarzania danych osobowych w sposób niezgodny z tymi celami,
4) przetwarzania danych adekwatnych, stosownych oraz niezbędnych do celów, w których dane są przetwarzane,
5) przetwarzania danych prawidłowych i uaktualnianych w razie bieżącej potrzeby,

6) przechowywania danych osobowych w sposób umożliwiający identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to konieczne dla realizacji celów, w jakich dane są przetwarzane,
7) przechowywania danych osobowych w sposób zapewniający odpowiednie zabezpieczenie tych danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów prawa, utratą, uszkodzeniem lub zniszczeniem.

§ 2

W związku z § 1 niniejszego dokumentu Administrator Danych wprowadza dokument „Analiza zagrożeń i ryzyka" w podmiocie o nazwie: **„EMPRESSIA" spółka cywilna** w celu badania i obserwowania istniejącego środowiska przetwarzania danych osobowych.

§ 3

Ilekroć w „Analizie zagrożeń i ryzyka przy przetwarzaniu danych osobowych" jest mowa o:

1. **ANALIZIE RYZYKA** – należy przez to rozumieć systematyczne wykorzystanie informacji do zidentyfikowania źródeł i oszacowania ryzyka w związku z przetwarzaniem danych osobowych;

2. **SZACOWANIU RYZYKA** – należy rozumieć przez to proces oceny i analizy ryzyka w związku z przetwarzaniem danych osobowych;

3. **OCENIE RYZYKA** – proces porównania oszacowanego ryzyka z określonymi kryteriami w celu określenia znaczenia ryzyka w procesie przetwarzania danych osobowych;

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, które stwarzają znaczne zakłócenia zadań biznesowych i zagrażają bezpieczeństwu informacji;

11. **AKTYWACH** – wszystko, co ma wartość dla organizacji;

12. **ZAGROŻENIACH SYSTEMU** – to wszystkie niekorzystne czynniki mogące przyczynić się w trakcie pracy z danymi osobowymi 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

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. Analiza zagrożeń i ryzyka, określa środki zastosowane dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych.

§ 5

Wymogi ogólne bezpieczeństwa przetwarzanych danych osobowych, wprowadzone przez Administratora Danych określa załącznik nr 1.

§ 6

Możliwe zagrożenia występujące w systemach informatycznych oraz poza systemami informatycznymi, określa załącznik nr 2.

§ 7

Podatność systemu na zagrożenia, określa załącznik nr 3.

§ 8

Analizę zagrożeń i ryzyka, określa załącznik nr 4.

§ 9

Analizę środków koniecznych do wdrożenia dla uzyskania legalności przetwarzania danych osobowych, określa załącznik nr 5

§ 10

Wnioski i działania naprawcze, określa załącznik nr 6.

§ 11

Przebieg przykładowej kontroli podatności systemu, określa załącznik nr 7.

§ 12

Tabela szacowania ryzyka została określona w załączniku nr 8.

ZAŁĄCZNIK NR 1

WYMOGI OGÓLNE BEZPIECZEŃSTWA PRZETWARZANYCH DANYCH OSOBOWYCH, WPROWADZONE PRZEZ ADMINISTRATORA DANYCH W:

„EMPRESSIA" spółka cywilna

§ 1

W czasie przetwarzania danych osobowych informacje mogą występować w postaci:

1. plików lub informacji przechowywanych na dysku twardym komputera;
2. plików lub informacji zapisanych na nośnikach komputerowych;
3. wersji roboczych lub gotowych dokumentów wydrukowanych na papierze.

§ 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 komputerowego, w tym określenia zasad postępowania z nimi przed nieuprawnionym dostępem;
3. zapewnienie fizycznej ochrony miejsc, gdzie przechowywane są dane osobowe w postaci wydruków i zabezpieczenia tych miejsc przed nieuprawnionym dostępem osób trzecich, jak również przed zniszczeniem tych danych na skutek działania sił przyrody;
4. zagwarantowania należytej archiwizacji danych przechowywanych w formie wydruków komputerowych, w tym uwzględniając konieczność ich zniszczenia po zakończeniu przechowywania danych osobowych;
5. zabezpieczenia przed nieupoważnionym dostępem do danych osobowych znajdujących się w zasobach systemu informatycznego;
6. zapewnienia dostępności do danych osobowych znajdujących się na technicznych nośnikach informacji oraz w pamięci systemu informatycznego dla upoważnionych użytkowników;
7. zapewnienia możliwości kontroli dostępu do zasobów systemu informatycznego oraz wykonywanych na nim czynności;
8. zapewnienia możliwości kontroli nośników, na których przetwarzano lub przechowywano dane osobowe.

ZAŁĄCZNIK NR 2

ZAGROŻENIA WYSTĘPUJĄCE W SYSTEMACH INFORMATYCZNYCH

I POZA NIMI

§ 1

Każdy Administrator Danych Osobowych powinien zapewnić takie warunki pracy w systemie informatycznym, aby przetwarzanie cechowało się poufnością, integralnością i rozliczalnością.

§ 2

Każde zauważone zagrożenie związane z poufnością, integralnością lub rozliczalnością, powinno być niezwłocznie zgłoszone Administratorowi Danych Osobowych.

§ 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 Osobowych zadań wraz z wszelkimi konsekwencjami organizacyjnymi i prawnymi.
3. Strategiczną częścią zabezpieczania danych w systemach informatycznych oraz w systemach tradycyjnych przed utratą poufności jest odpowiednio prowadzony system szkoleń dla pracowników merytorycznych mających dostęp do informacji. Administrator Danych Osobowych zapozna osoby upoważnione do przetwarzania danych z przepisami o ochronie danych osobowych oraz konsekwencjami prawnymi z nich wynikającymi.

§ 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 nieuprawnioną;
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. stosowanie korupcji oraz szantażu w celu wydobycia określonych informacji od wybranych pracowników firmy;
17. zagubienie dokumentów lub utrata przetwarzanych informacji.

§ 5

Skala identyfikacji skutków utraty zasobów dla atrybutu poufności danych osobowych.

WARTOŚĆ	SKUTKI
< 0 >	Brak skutków utraty poufności
< 1 – 3 >	Niski skutek utraty poufności
< 4 – 7 >	Średni skutek utraty poufności
< 8 – 9 >	Wysoki skutek utraty poufności
< 9 – 10 >	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. 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
< 0 >	Utrata integralności nie występuje
< 1 – 3 >	Niski skutek utraty integralności
< 4 – 7 >	Średni skutek utraty integralności
< 8 – 9 >	Wysoki skutek utraty integralności
< 10 >	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

Skala identyfikacji skutków utraty zasobów dla atrybutu rozliczalności danych osobowych.

WARTOŚĆ	SKUTKI
< 0 >	Utrata rozliczalności nie występuje
< 1 – 3 >	Niski skutek utraty rozliczalności
< 4 – 6 >	Średni skutek utraty rozliczalności
< 7 – 8 >	Wysoki skutek utraty rozliczalności
< 9 >	Ekstremalny skutek utraty rozliczalności
< 10 >	Absolutny skutek utraty rozliczalności

§ 12

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

1. **SIŁY NATURY** (to zdarzenia niewynikające z działalności człowieka), mogą to być:

   a) uderzenie pioruna;
   b) pożar będący konsekwencją ww. uderzenia pioruna;
   c) starzenie się sprzętu;
   d) starzenie się nośników pamięci;
   e) smog, kurz;
   f) katastrofy budowlane;
   g) ulewny deszcz;
   h) huragan;
   i) ekstremalne temperatury, wilgotność;
   j) epidemia.

2. **LUDZI** (mogą to być pracownicy lub osoby z zewnątrz, które działają w sposób celowy lub przypadkowy), mogą to być:

   a) błędy i pomyłki użytkowników;
   b) błędy i pomyłki administratorów;
   c) błędy utrzymania systemu w poufności, integralności i rozliczalności;
   d) zaniedbania użytkowników przy przesyłaniu, udostępnianiu i kopiowaniu;
   e) zagubienie nośnika zawierającego dane osobowe;
   f) niewłaściwe zniszczenie nośnika;
   g) nielegalne użycie oprogramowania;
   h) choroba ważnych osób i nieuprawnione zastępstwo;
   i) epidemia kadry i brak osób upoważnionych do dostępu;
   j) podpalenie obiektu;
   k) zalanie wodą;
   l) katastrofa budowlana będąca konsekwencją przypadkowego działania człowieka;
   m) zakłócenia elektromagnetyczne, radiotechniczne;
   n) podłożenie i wybuch bomby, ładunku wybuchowego;
   o) użycie broni;
   p) zmiany napięcia w sieci;
   q) utrata prądu;
   r) zbieranie się ładunków elektrostatycznych;
   s) utrata kluczowych pracowników;
   t) niedobór pracowników;
   u) defekty oprogramowania;
   v) szpiegostwo;
   w) terroryzm;
   x) wandalizm;
   y) destrukcja zbiorów i programów impulsem elektromagnetycznym;
   z) kradzież;

aa) włamanie do systemu;
bb) wyłudzenie, fałszowanie dokumentów;
cc) podszycie się pod uprawnionego użytkownika;
dd) podsłuch;
ee) użycie złośliwego oprogramowania;
ff) wykorzystanie promieniowania ujawniającego.

ZAŁĄCZNIK NR 3

PODATNOŚĆ SYSTEMU NA ZAGROŻENIA

§ 1

Podatność systemu na zagrożenia stanowi pewnego rodzaju słabość. Obecnie, szczególnie trudno jest obronić się przed zagrożeniami w zakresie teleinformatycznym, co związane jest z coraz to bardziej wyrafinowaną cyberprzestępczością. Wraz z coraz to większą ilością dostępnych w środowisku internetowym usług, nasilają się działania przestępcze. Chroniąc Przedsiębiorstwo przed takowym działaniem, należy wdrożyć odpowiednie procedury.

§ 2

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 zapewnienia prawidłowości przetwarzania danych osobowych.

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

   System informatyczny w Przedsiębiorstwie 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.

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

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

§ 3

1. Podatność systemu na zagrożenia w podmiocie **„EMPRESSIA" spółka cywilna** została ograniczona poprzez:
   - **a)** zapewnienie ochrony fizycznej budynku, w którym znajduje się siedziba Przedsiębiorstwa,
   - **b)** ograniczenie osób zaangażowanych w przetwarzanie danych osobowych (w tym zakresie w jakim jest to możliwe, tj. w zakresie danych osobowych Współpracowników),
   - **c)** częściową ochronę fizyczną stanowisk komputerowych;
   - **d)** kontrolę dostępu do pomieszczeń, gdzie przetwarzane są dane osobowe;
   - **e)** zawieranie umów o obowiązku zachowania poufności z Kontrahentami (nie zawsze) i Współpracownikami,
   - **f)** przeglądy okresowe nośników;
   - **g)** testowanie oprogramowania;
   - **h)** audyt;
   - **i)** zabezpieczanie haseł – częściowy (dostęp do poczty elektronicznej nie jest zabezpieczony hasłem);
   - **j)** użycie oprogramowania antywirusowego.
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. przede wszystkim środowisko komputerowe. Warunkiem wyeliminowania działań cyberprzestępców, jest pełne współdziałanie wszystkich obszarów przetwarzania danych osobowych:
   - **a)** prowadzenie odpowiedniej dokumentacji;
   - **b)** fizyczna ochrona danych osobowych;
   - **c)** środowisko komputerowe;
   - **d)** „politykę ochrony danych osobowych" wdrożony przez Administratora Danych Osobowych.

   Przebieg przykładowej kontroli tych obszarów stanowi załącznik nr 9.

§ 4

W celu wdrażania systemu ochrony danych osobowych w taki sposób, by uniemożliwić działanie nieuprawnione na danych osobowych, Administrator Danych Osobowych zobowiązuje pracowników podmiotu o nazwie **„EMPRESSIA" spółka cywilna** do stosownego zachowania w trakcie przetwarzania danych osobowych.

§ 5

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

§ 6

Identyfikacja podatności systemu informatycznego na określone zagrożenia.

WARTOŚĆ	SKUTKI
< 0 >	Brak podatności
< 1 – 4 >	Niski poziom
< 5 – 7 >	Średni poziom
< 8 – 9 >	Wysoki poziom
< 10 >	Ekstremalny poziom

ZAŁĄCZNIK NR 4

ANALIZA ZAGROŻEŃ I SZACOWANIE RYZYKA

§ 1

Administrator Danych Osobowych, aby poprawnie przeprowadzić analizę ryzyka, powinien określić:

1. **ZASOBY** - które będzie chronić:
   - **a)** sprzęt komputerowy przechowujący dane - dysk twardy,
   - **b)** dane osobowe przetwarzane w formie papierowej i elektronicznej,
   - **c)** aplikacje, w których przetwarzane są dane osobowe,
   - **d)** pomieszczenia, w których pracują osoby przetwarzające dane osobowe;
2. **ZAGROŻENIA** - czynnik, który może 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

Administrator Danych Osobowych, aby dokonać skutecznego zarządzania bezpieczeństwem informacji w Przedsiębiorstwie, dokonuje dokładnej analizy zagrożeń w związku z reagowaniem na zmieniające się warunki otoczenia mające wpływ na ryzyko w organizacji. Tak stworzony efektywny system zarządzania daje możliwość podjęcia działań redukujących wartość ryzyka do akceptowanego poziomu.

§ 3

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

§ 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

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

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

3. Tabela szacowania ryzyka stanowi załącznik nr 10.

§ 6

1. Administrator Danych Osobowych określa poziom ryzyka utraty bezpieczeństwa danych osobowych na poziomie średnim w podmiocie o nazwie **„EMPRESSIA" spółka cywilna** przy uwzględnieniu ryzyka ogólnego przy wartości **31,2**

   RYZYKO = wartość skutków x podatność zasobów systemu

   (max. = 100)

WARTOŚĆ	POZIOM RYZYKA
<1-20>	**NISKI** poziom ryzyka utraty bezpieczeństwa danych osobowych
<21-60>	**ŚREDNI** poziom ryzyka utraty bezpieczeństwa danych osobowych
<61-80>	**WYSOKI** poziom ryzyka utraty bezpieczeństwa danych osobowych
<81-100>	**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;

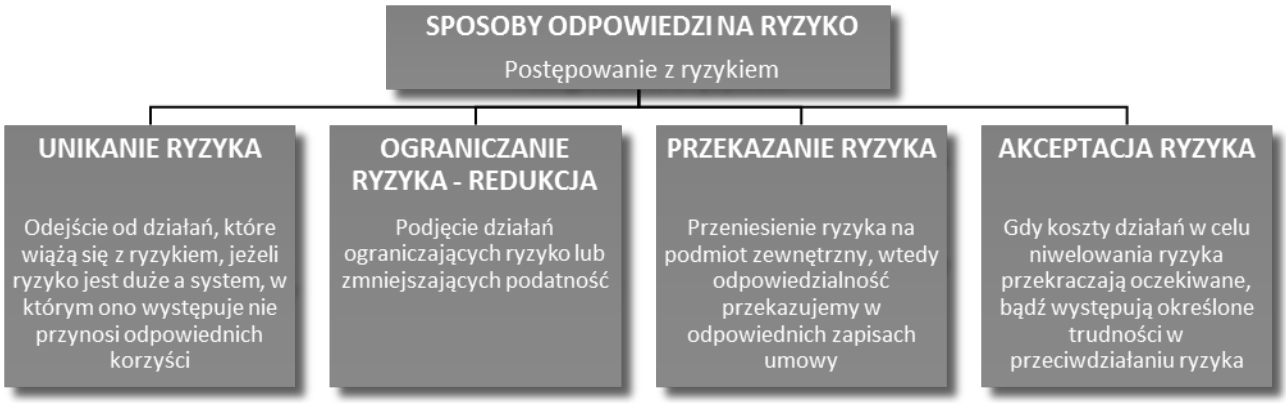
   b) **ŚREDNI** – wysokie szkody w przypadku realizacji zagrożenia i niska możliwość jego realizacji bądź niskie szkody w przypadku realizacji zagrożenia i wysoka możliwość jego realizacji;

   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.

§ 7

Administrator Danych Osobowych 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.



§ 8

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.

ZAŁĄCZNIK NR 5

ANALIZA ŚRODKÓW KONIECZNYCH DO WDROŻENIA DLA UZYSKANIA LEGALNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH W:

„EMPRESSIA" spółka cywilna

§ 1 Kategorie przetwarzanych danych osobowych i podstawa ich przetwarzania

Administrator Danych Osobowych przetwarza dane osobowe następujące dane osobowe:

1) dane osobowe kandydatów do nawiązania współpracy są przetwarzane w oparciu o art. 6 ust. 1 lit. a RODO, tj. na podstawie zgody kandydata na przetwarzanie jego danych osobowych na potrzeby bieżącej lub przyszłych rekrutacji,
2) dane osobowe Współpracowników przetwarzane są w oparciu o art. 6 ust. 1 lit. b RODO, tj. w związku z zawartą umową o współpracy,
3) dane osobowe Reprezentantów Kontrahentów są przetwarzane w oparciu o art. 6 ust. 1 lit. f RODO, tj. przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora. W zakresie, w jakim to Reprezentant Kontrahenta nawiązuje kontakt z „EMPRESSIA" spółka cywilna powinno to się odbywać w oparciu o art. 6 ust. 1 lit. a RODO, czyli w oparciu o zgodę osoby nawiązującej kontakt,
4) dane osobowe osób fizycznych – Konsumentów „EMPRESSIA" spółka cywilna przetwarza jedynie jako procesor, tj. podmiot, któremu powierzono dane osobowe, w związku z usługami świadczonymi na rzecz Kontrahentów. „EMPRESSIA" spółka cywilna, odnośnie tych danych osobowych, nie jest administratorem, tj. nie decyduje o celach i sposobach przetwarzania tych danych osobowych. Przesłanką legalizującą przetwarzanie danych osobowych powinny być, co do zasady, umowy o powierzeniu przetwarzania danych osobowych.

§ 2 Obowiązek informacyjny

1. „EMPRESSIA" spółka cywilna powinna wypełniać obowiązek informacyjny wobec osób, których dane osobowe przetwarza. Wypełnienie tego obowiązku powinno nastąpić:
   a) odnośnie danych osobowych kandydatów do podjęcia współpracy – przy pierwszym kontakcie z kandydatem (np. w formie przesłanej wiadomości e-mail),
   b) odnośnie danych osobowych Współpracowników – w treści zawieranej umowy o współpracy,
   c) odnośnie danych osobowych Reprezentantów Kontrahentów – przy pierwszym kontakcie z tą osobą, o ile jest to możliwe (tzn. zostanie nawiązany kontakt mailowy).
2. „EMPRESSIA" spółka cywilna powinna ustalić reguły odnoszące się do okresu przechowywania danych osobowych, jak również procedury związane z ich niszczeniem.
3. W zakresie korzystania przez osoby trzecie z formularza kontaktowego na stronie internetowej „EMPRESSIA" spółka cywilna, konieczne jest uzależnienie przesłania zapytania od wyrażenia zgody na przetwarzanie danych osobowych tej osoby.

§ 3 Umowy o powierzeniu danych osobowych

1. W zakresie, w jakim „EMPRESSIA" spółka cywilna jest procesorem, przetwarzającym dane osobowe Klientów swoich kontrahentów, konieczne jest zawarcie umów o powierzeniu przetwarzania danych osobowych.
2. W zakresie, w jakim to „EMPRESSIA" spółka cywilna powierza przetwarzanie danych osobowych, których jest Administratorem, z uwagi na okoliczność, iż są to duże podmioty, przetwarzające dane osobowe na masową skalę, zasadne jest oczekiwanie na propozycję zmiany umów (w tym regulaminów) ze strony tych podmiotów.
3. Przetwarzanie danych osobowych, o którym mowa w § 3 ust. 1, odbywać się będzie na podstawie umowy o powierzeniu przetwarzania danych osobowych, określającej jej przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, jak również obowiązki i prawa administratora. Umowa będzie ponadto określać:
    a) prawo do przetwarzania danych osobowych wyłącznie na udokumentowane polecenie administratora,
    b) gwarancje, że osoby upoważnione do przetwarzania danych osobowych zobowiążą się do zachowania tajemnicy,
    c) obowiązek zapewnienia środków technicznych i organizacyjnych, zapewniających bezpieczeństwo danych osobowych odpowiednie do ryzyka związanego z ich przetwarzaniem,
    d) warunki korzystania z usług innego podmiotu przetwarzającego,
    e) obowiązek wywiązania się z odpowiedzi na żądania osoby, które dane dotyczą,
    f) obowiązek usunięcia danych osobowych lub zwrotu tych danych Administratorowi, po zakończeniu świadczenia usług związanych z przetwarzaniem danych, chyba, że powszechnie obowiązujące przepisy prawa nakazują przechowywanie danych osobowych,
    g) prawa Administratora do przeprowadzenia audytów zgodności przetwarzania danych z przepisami prawa oraz możliwości korzystania przez Administratora z dostępu do informacji niezbędnych do wykazania spełnienia obowiązków.

§ 4 Wprowadzenie polityki ochrony danych osobowych

Celem zagwarantowania przetwarzania danych osobowych zgodnie z obowiązującymi przepisami prawa, w tym przede wszystkim zgodnie z zasadą rzetelności, przejrzystości, ograniczenia celu, minimalizacji danych, prawidłowości, ograniczenia przechowywania oraz integralności i poufności, Administrator Danych Osobowych powinien wprowadzić politykę ochrony danych osobowych, w której określi:

1) zakres oraz zasady przetwarzania danych osobowych,
2) wykaz zbiorów danych osobowych,
3) zasady udzielania osobom, których dane dotyczą, wglądu do danych, w tym ich poprawienia i aktualizacji,
4) szczegółowe obowiązki Administratora Danych Osobowych,
5) organizacyjne i techniczne środki zabezpieczenia danych osobowych przed niedozwolonym lub niezgodnym z prawem przetwarzaniem danych osobowych oraz przypadkową utratą, zniszczeniem oraz uszkodzeniem,
6) obowiązki użytkowników przetwarzających dane osobowe w systemie informatycznym i tradycyjnym,

7) zasady kontroli nad prawidłowością przetwarzania danych osobowych,
8) zasady postępowania w przypadku naruszenia ochrony danych osobowych.

§ 5 Rejestrowanie czynności przetwarzania danych osobowych

Administrator Danych Osobowych nie jest zobowiązany do prowadzenia rejestru czynności przetwarzania danych osobowych. „EMPRESSIA" spółka cywilna jest przedsiębiorcą zatrudniającym mniej niż 250 osób, a przetwarzanie danych osobowych nie powoduje ryzyka naruszenia praw lub wolności osób, których dane dotyczą. „EMPRESSIA" spółka cywilna nie przetwarza szczególnych kategorii danych (np. w związku z brakiem zatrudnienia pracowników, nie przetwarza danych osobowych o ich stanie zdrowia).

§ 6 Inspektor Ochrony Danych Osobowych

Biorąc pod uwagę charakter przetwarzanych danych osobowych oraz możliwe ryzyko związane z czynnościami przetwarzania danych osobowych, Administrator Danych Osobowych nie zobligowany do powołania inspektora ochrony danych. „EMPRESSIA" spółka cywilna nie jest organem, ani podmiotem publicznym. Główna działalność przedsiębiorstwa „EMPRESSIA" spółka cywilna nie jest związana z wykonywaniem operacji na danych osobowych, w szczególności nie wiąże się z systematycznym monitorowaniem osób, których dane dotyczą. Główną działalnością przedsiębiorstwa „EMPRESSIA" spółka cywilna nie jest przetwarzanie na dużą skalę szczególnych kategorii danych osobowych – takie dane w ogóle nie są przetwarzane.

§ 7 Rejestr osób przetwarzających dane osobowe w imieniu Administratora i klauzule poufności

1. Administrator Danych osobowych powinien wprowadzić system nadawania uprawnień do przetwarzania danych osobowych oraz prowadzić rejestr wydanych uprawnień.
2. Każda osoba, która przetwarza dane osobowe w imieniu Administratora powinna zostać zobligowana do zachowania poufności powierzonych danych osobowych oraz znajomości postanowień polityki ochrony danych osobowych.
3. Administrator powinien przeprowadzać okresowe szkolenia określające zasady przetwarzania danych osobowych. Administrator powinien ponadto podejmować działania celem zwiększenia świadomości potrzeby ochrony danych osobowych przez osoby uczestniczące w procesie ich przetwarzania.

§ 8 Naruszenia ochrony danych osobowych

1. Administrator danych osobowych jest zobligowany do wprowadzenia rejestru naruszeń ochrony danych osobowych, jak również raportowania naruszeń organowi nadzorczemu.
2. Jeśli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator jest ponadto zobowiązany do zawiadomienia, bez zbędnej zwłoki o naruszeniu ochrony jej danych.
3. Zawiadomienie, o którym mowa w § 8 ust. 2 nie jest wymagane, w następujących przypadkach:
   a) 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;

b) administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane osobowe zostały naruszone;
c) zawiadomienie wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku Administrator powinien wydać publiczny komunikat, za pomocą którego osoby, których dane zostały naruszone, będą poinformowane o tym naruszeniu w równie skuteczny sposób.

ZAŁĄCZNIK NR 6

WNIOSKI I DZIAŁANIA NAPRAWCZE

W ZWIĄZKU Z PRZEPROWADZONĄ „ANALIZĄ RYZYKA I ZAGROŻEŃ

PRZY PRZETWARZANIU DANYCH OSOBOWYCH"

§ 1

1. Administrator Danych Osobowych w Przedsiębiorstwie o nazwie: **„EMPRESSIA" spółka cywilna**, przeprowadził analizę dla wszystkich chronionych zasobów oraz wszystkich możliwych zagrożeń.
2. Administrator Danych Osobowych jest zobowiązany dostosować środki bezpieczeństwa, zarówno techniczne, jak i fizyczne oraz organizacyjne, do wyników, jakie wykazała przeprowadzona analiza.
3. Zmiany zostaną wprowadzone do polityki ochrony danych osobowych.

§ 2

W wyniku przeprowadzonej analizy w Przedsiębiorstwie o nazwie: **„EMPRESSIA" spółka cywilna**, Administrator Danych Osobowych wyróżnił potencjalnie najniebezpieczniejsze zagrożenia, a w szczególności są to:

- **niedyskrecja współpracowników,**
- **awaria sprzętu,**
- **uszkodzenia systemu informatycznego, w którym przetwarzane są dane osobowe,**
- **niekontrolowane przetwarzanie danych osobowych przez podmioty, którym powierzono dane osobowe,**
- **działanie złośliwego oprogramowania,**
- **niekontrolowany dostęp osób trzecich do miejsc przetwarzania danych osobowych.**

§ 3

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

- **szkolenia z zakresu ochrony danych osobowych, zobligowanie osób przetwarzających dane osobowe w imieniu Administratora do zachowania poufności,**
- **okresowe przeglądy stanu sprzętu,**
- **okresowe przeglądy systemu informatycznego,**
- **dbałość o powierzanie danych osobowych zaufanym podmiotom oferującym należyte zasady przetwarzania danych osobowych w imieniu Administratora,**
- **przeglądy oprogramowania antywirusowego oraz zabezpieczanie wszystkich gromadzonych danych osobowych, za pomocą tego oprogramowania,**
- **stosowanie środków organizacyjnych celem zapewnienia zabezpieczenia danych osobowych.**

§ 4

Administrator Danych Osobowych w celu wyeliminowania zagrożeń, wynikłych w toku przeprowadzonej analizy, podejmuje określone działania wskazane w załączniku nr 5.

ZAŁĄCZNIK NR 7

PRZEBIEG PRZYKŁADOWEJ KONTROLI PODATNOŚCI SYSTEMU

LP.	ZAKRES KONTROLI	PODEJMOWANE CZYNNOŚCI
1.	DOKUMENTACJA	Sprawdzenie, czy Polityka Ochrony Danych Osobowych jest aktualna względem obowiązującego stanu prawnego oraz faktycznego.
2.	DOKUMENTACJA	Sprawdzenie, czy osoba ma upoważnienie do przetwarzania danych osobowych – upoważnienie powinno odzwierciedlać zakres obowiązków.
3.	DOKUMENTACJA	Sprawdzenie, czy osoby, które mają dostęp do danych osobowych, ale nie przetwarzają tych danych, posiadają zezwolenie na przebywanie w obszarze przetwarzania.
4.	DOKUMENTACJA	Sprawdzenie, czy prowadzona jest aktualna ewidencja osób przetwarzających dane osobowe.
5.	FIZYCZNA OCHRONA DANYCH OSOBOWYCH	Kontrolowanie osób przetwarzających dane osobowe - czy stosują się do „zasady czystego biurka”.
6.	FIZYCZNA OCHRONA DANYCH OSOBOWYCH	Sprawdzenie, czy w pomieszczeniu znajdują się szafy zamykane na klucz, w których przechowuje się dokumentację zawierającą dane osobowe podlegające ochronie (jeśli tak - można sporządzić dokumentację fotograficzną pomieszczeń, która stanowić będzie załącznik do poniższego sprawdzenia).
7.	FIZYCZNA OCHRONA DANYCH OSOBOWYCH	Sprawdzenie, czy w pomieszczeniu znajduje się niszczarka dokumentów. Szczególnie powinno się zwrócić uwagę, czy niepotrzebne dokumenty nie są wyrzucane do kosza na śmieci – dokumenty powinny być niszczone w sposób mechaniczny, a ewentualnie manualny, tak, by uniemożliwić ich odczytanie osobom postronnym.
8.	OCHRONA ŚRODOWISKA KOMPUTEROWEGO	Kontrolowanie, mające na celu sprawdzenie, czy komputer jest zabezpieczony hasłem.
9.	OCHRONA ŚRODOWISKA KOMPUTEROWEGO	Sprawdzenie, czy systemy komputerowe służące do przetwarzania danych osobowych zapamiętują wszelakie czynności, jakich dokonuje się przy przetwarzaniu danych osobowych.
10.	OCHRONA ŚRODOWISKA KOMPUTEROWEGO	Monitorowanie, czy osoby przetwarzające dane osobowe w programie komputerowym bazodanowym logują się za pomocą własnego identyfikatora i hasła.
11.	OCHRONA ŚRODOWISKA KOMPUTEROWEGO	Kontrolowanie aktywności systemu antywirusowego, na komputerach, które m.in. służą do obsługi systemów przetwarzających dane osobowe.
12.	OCHRONA ŚRODOWISKA KOMPUTEROWEGO	Kontrolowanie, czy pracownik korzysta z wygaszacza ekranu.

LP.	ZAKRES KONTROLI	PODEJMOWANE CZYNNOŚCI
13.	OCHRONA ŚRODOWISKA KOMPUTEROWEGO	Sprawdzenie, czy monitor komputera został usytuowany w sposób uniemożliwiający wgląd do danych osobom postronnym.
14.	KONTROLA PRAKTYKI	Przeprowadzenie analizy pod kątem pracowników - jakie obecnie mają problemy w zakresie przetwarzania danych osobowych oraz czy ostatnio miały miejsce zdarzenia typu: • próby nieuprawnionego dostępu do danych osobowych; • działanie zewnętrznych aplikacji, wirusów czy złośliwego oprogramowania; • nieuprawniony dostęp do otwartych aplikacji w systemie informatycznym; • próba nieuprawnionej interwencji przy sprzęcie komputerowym; • wynoszenie niezabezpieczonych pamięci z miejsca pracy; • udzielanie informacji osobom postronnym, pomijając formalny tryb administracyjny.

ZAŁĄCZNIK NR 8

TABELA SZACOWANIA RYZYKA

SZACOWANIE RYZYKA DLA BEZPIECZEŃSTWA INFORMACJI																			
RYZYKO ŚREDNIE [1]:					27			35			33			29			32		31,2
ZAGROŻENIA	**INTEGRALNOŚĆ**	**NIEDYSKRECJA WSPÓŁPRACOWNI-**	5	5	25	8	5	40	8	5	40	8	4	32	8	5	40		
		AWARIA SPRZĘTU	6	5	30	6	5	30	8	6	48	7	6	42	7	5	35		
		USZKODZENIE SYSTEMU INF.	5	2	10	7	6	42	7	5	35	8	4	32	6	6	36		
		NIEKONTROLOWANE POWIERZENIE	6	3	18	7	5	30	8	5	40	5	5	25	5	4	20		
		ATAK WIRUSA	7	4	28	8	6	48	6	5	30	7	4	28	6	4	24		
		NIEKONTROLOWANY DOSTĘP	7	5	35	5	4	20	7	6	42	7	5	35	6	5	30		
	ROZLICZALNOŚĆ	**NIEDYSKRECJA WSPÓŁPRACOWNI-**	8	5	40	7	5	35	5	5	25	6	5	30	6	5	30		
		AWARIA SPRZĘTU	7	5	35	6	6	36	7	5	35	8	6	48	9	5	45		
		USZKODZENIE SYSTEMU INF.	7	4	28	7	4	28	5	4	20	7	4	28	6	5	30		
		NIEKONTROLOWANE POWIERZENIE	6	4	24	6	5	30	5	5	25	5	4	20	5	5	25		
		ATAK WIRUSA	7	4	28	7	3	21	6	5	30	6	4	24	6	5	30		
		NIEKONTROLOWANY DOSTĘP	6	4	24	8	3	24	7	5	35	8	3	18	8	5	40		
	POUFNOŚĆ	**NIEDYSKRECJA WSPÓŁPRACOWNI-**	5	3	15	8	5	40	4	4	16	5	4	20	7	6	42		
		AWARIA SPRZĘTU	4	4	16	7	5	35	6	6	36	7	5	35	5	5	25		
		USZKODZENIE SYSTEMU INF.	7	3	21	7	6	42	7	6	42	8	3	24	6	5	30		
		NIEKONTROLOWANE POWIERZENIE	5	5	20	7	5	35	7	5	35	5	4	20	6	5	30		
		ATAK WIRUSA	8	6	48	8	5	40	7	4	28	8	4	32	5	5	25		
		NIEKONTROLOWANY DOSTĘP	7	5	35	8	6	48	7	5	35	7	4	28	7	4	28		
SZACOWANIE			**SKUTKI**	**PODATNOŚĆ**	**RYZYKO [3]**	**SKUTKI**	**PODATNOŚĆ**	**RYZYKO [3]**	**SKUTKI**	**PODATNOŚĆ**	**RYZYKO [3]**	**SKUTKI**	**PODATNOŚĆ**	**RYZYKO [3]**	**SKUTKI**	**PODATNOŚĆ**	**RYZYKO [3]**		
ZASOBY SZACOWANE			**SPRZĘT**			**LUDZIE**			**APLIKACJA**			**POMIESZCZENIA**			**DODATKOWE ZABEZPIECZENIA**			**RYZYKO OGÓLNE [2]:**	

Skala poziomu ryzyka:

1 **RYZYKO ŚREDNIE** = suma ryzyka każdego z sześciu zakresów poufności, rozliczalności i integralności dzielona przez 18

2 **RYZYKO OGÓLNE** = suma ryzyka średniego z zasobów: sprzęt, ludzie, aplikacja, pomieszczenia, zabezpieczenia dodatkowe, dzielona przez 5

3 **RYZYKO** = wartość skutków x podatność zasobów systemu (max. = 100)

WARTOŚĆ	POZIOM RYZYKA
1-20	**NISKI** poziom ryzyka utraty bezpieczeństwa danych osobowych
21-60	**ŚREDNI** poziom ryzyka utraty bezpieczeństwa danych osobowych
61-80	**WYSOKI** poziom ryzyka utraty bezpieczeństwa danych osobowych
81-100	**MAKSYMALNY** poziom ryzyka utraty bezpieczeństwa danych osobowych

PODSUMOWANIE

W podmiocie o nazwie: **„EMPRESSIA" spółka cywilna** po przeprowadzeniu analizy poufności, integralności i rozliczalności systemów informatycznych pod kątem zagrożeń i ryzyka, zwanej dalej: analizą zagrożeń i ryzyka przy przetwarzaniu danych osobowych wartość i poziom ryzyka przedstawia się następująco:

Ryzyko ogólne wynosi: 31,2 / 100.

Powyższa wartość ryzyka określa Średnie ryzyko utraty bezpieczeństwa danych osobowych.