**UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH**

Zawarta w dniu …………………………….................. w ………………………….......................... pomiędzy:

Województwem Małopolskim, ul. Basztowa 22, 31-156 Kraków, NIP 6762178337, REGON 351554287, w imieniu którego działa Małopolskie Centrum Doskonalenia Nauczycieli, ul. Lubelska 23, 30-003 Kraków, NIP 6772351458, REGON 121385785,

reprezentowane przez:

Łukasza Cieślika – Dyrektora,

zwanym dalej „Administratorem”,

a

……………………………..

reprezentowaną przez:

……………………………………..

zwanym dalej „Podmiotem Przetwarzającym”,

łącznie zwani „Stronami”.

**§ 1. Przedmiot umowy**

1. Przedmiotem umowy jest powierzenie przetwarzania danych osobowych, stosownie do art. 28 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz.Urz.UE.L Nr 119, str. 1), dalej „RODO”.

2. Podmiot Przetwarzający zobowiązuje się wykonywać w imieniu Administratora czynności przetwarzania danych osobowych wyłącznie w celu, zakresie i na zasadach określonych niniejszą umową.

**§ 2. Zakres powierzenia przetwarzania**

1. Administrator powierza Podmiotowi Przetwarzającemu przetwarzanie danych osobowych w następującym zakresie:

a) Dane pracowników działu IT i personelu uprawnionego do zgłaszania zleceń/praca lub odpowiedzialnych za realizację i obsługę zamówień i umów, które zawierają imię, nazwisko, adres e-mail, telefon, stanowisko pracownika.

b) Inne dane osobowe przetrzymywane w systemie IT Administratora, do których ma potencjalny dostęp Przetwarzający.

c) Dane kontaktowe kontrahentów i usługodawców Administratora.

2. Podmiot Przetwarzający jest upoważniony jedynie do wykonywania czynności przetwarzania danych osobowych niezbędnych do wykonania umów zawartych pomiędzy Stronami.

3. Administrator jest uprawniony do zmiany zakresu w jakim następuje powierzenie poprzez jego rozszerzenie lub zawężenie. Zmiana zakresu może nastąpić poprzez powiadomienie Podmiotu Przetwarzającego o nowym zakresie. W przypadku zawiadomienia o zawężeniu zakresu w jakim następuje powierzenie Administrator jest jednocześnie obowiązany zająć stanowisko czy dotychczas przetwarzane w ramach powierzenia dane mają zostać usunięte, zwrócone czy będą nadal przechowywane przez Podmiot Przetwarzający.

**§ 3. Przetwarzanie wyłącznie na udokumentowane polecenie administratora**

1. Przetwarzanie danych osobowych w zakresie przekraczającym § 2 wymaga zmiany niniejszej umowy w formie pisemnej pod rygorem nieważności.

2. Ust. 1 nie dotyczy sytuacji, gdy Podmiot Przetwarzający działa w celu realizacji obowiązku, który nakłada na niego prawo Unii Europejskiej lub prawo państwa członkowskiego któremu podlega Podmiot Przetwarzający, a realizacji tego obowiązku nie da się pogodzić z postanowieniami niniejszej umowy.

3. W sytuacji, o której mowa w ust. 2, przed rozpoczęciem przetwarzania Podmiot Przetwarzający informuje Administratora o tym obowiązku prawnym, o ile prawo nie zabrania udzielania takiej informacji.

4. Niniejsza umowa stanowi udokumentowane polecenie Administratora pozwalające na przetwarzania danych przez Podmiot Przetwarzający w zakresie niniejszą umową określonym.

**§ 4. Obowiązek zachowania tajemnicy**

1. Podmiot Przetwarzający upoważnia do przetwarzania powierzonych danych osobowych wyłącznie tych członków swojego personelu, którzy posiadają odpowiednie przeszkolenie z zakresu ochrony danych osobowych oraz zasad bezpieczeństwa i ich udział w przetwarzaniu danych jest niezbędny do realizacji niniejszej umowy.

2. Podmiot Przetwarzający zapewnia, aby osoby, o których mowa w ust. 1:

a) przetwarzały dane osobowe zgodnie z zasadą wiedzy koniecznej,

b) zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy,

c) posiadały nadane upoważnienia do przetwarzania danych.

**§ 5. Bezpieczeństwo przetwarzania**

Podmiot Przetwarzający zapewnia wdrożenie odpowiednich środków technicznych i organizacyjnych, aby zapewnić zgodność przetwarzania z RODO, w tym stopień bezpieczeństwa przetwarzania odpowiadający ryzyku naruszenia praw lub wolności osób, których dane dotyczą. Niezależnie od wyników analizy ryzyka Podmiot Przetwarzający obowiązany jest minimum do:

a) wprowadzenia procedur przyznawania indywidualnych loginów i haseł ze zróżnicowanym dostępem,

b) przechowywania nośników danych w bezpieczny sposób, tak aby nie były one dostępne dla osób trzecich,

c) zapewnienia, że budynki i systemy wykorzystywane do przetwarzania danych są bezpieczne oraz że stosowany jest wyłącznie wysokiej jakości sprzęt i oprogramowanie, które jest regularnie aktualizowane,

d) zapewnienia, że materiał testowy i odpadowy jest niszczony zgodnie z wymogami obowiązującymi w zakresie ochrony danych przez profesjonalną firmę zewnętrzną zajmującą się niszczeniem lub jeżeli niszczenie następuje w zakresie własnym Podmiotu Przetwarzającego – z wykorzystaniem sprzętu umożliwiającego niszczenie w sposób uniemożlwiający ponowne wykorzystanie danych.

**§ 6. Dalsze powierzenie przetwarzania**

1. W celu realizacji niniejszej umowy, Podmiot Przetwarzający może korzystać z usług innego podmiotu przetwarzającego, zwanego dalej Podpowierzającym, pod warunkiem uprzedniego uzyskania zgody Administratora, wyrażonej w formie pisemnej pod rygorem nieważności.

2. Administrator wyraża zgodę na przekazywanie przez Podmiot Przetwarzający danych określonych w §2, pkt 1, a) swoim kontrahentom, tj. dystrybucji i producentom sprzętu w celu realizacji zamówienia, szkolenia, użyczenia sprzętu lub oprogramowania oraz otrzymania potrzebnych symulacji cenowych.

3. Dokonując podpowierzenia Przetwarzający jest zobowiązany zobowiązać Podprzetwarzającego do realizacji wszystkich obowiązków wynikających z niniejszej umowy powierzenia danych, z wyjątkiem tych które nie mają zastosowania ze względu na naturę konkretnego powierzenia.

4. Jeżeli podmiot, na rzecz którego dokonano dalszego powierzenia przetwarzania danych nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec Administratora za wypełnienie obowiązków tego innego podmiotu przetwarzającego spoczywa na pierwotnym Podmiocie Przetwarzającym.

**§ 7. Przekazywanie danych osobowych poza obszar EOG**

Podmiot Przetwarzający może przekazywać lub autoryzować przekazywania powierzonych danych osobowych określonych w §2, pkt 1 poza Europejski Obszar Gospodarczy, w tym podmiotom działającym w Stanach Zjednoczonych w celu realizacji zamówienia, szkoleń, użyczenia sprzętu lub oprogramowania oraz otrzymania stosownej symulacji cenowej. Dane osobowe przekazywane będą jedynie podmiotom, które gwarantują odpowiednie standardy ich ochrony, posiadają certyfikację Privacy Shield, albo też w oparciu o inne odpowiednie zabezpieczenia, o których mowa w art. 46 RODO.

**§ 8. Odpowiadanie na żądania osoby, której dane dotyczą**

1. Na wniosek Administratora, Podmiot Przetwarzający stosuje środki organizacyjne i techniczne, umożliwiające Administratorowi wywiązanie się z obowiązku odpowiadania na żądania osoby, której dane dotyczą.

2. W razie wpływu do Podmiotu Przetwarzającego żądania w zakresie realizacji praw osób, których dotyczą powierzone dane, Podmiot Przetwarzający niezwłocznie informuje o tym Administratora. Udzielając informacji, Podmiot Przetwarzający przekazuje dane nadawcy i treść żądania oraz określa, w jakim zakresie jest w stanie przyczynić się do realizacji żądania. Na wniosek Administratora Podmiot Przetwarzający zobowiązany jest do udzielenia Administratorowi pomocy w rozpatrywaniu jak również udzielaniu odpowiedzi na wszelkie takie wnioski każdorazowo, gdy zażąda tego Administrator Danych.

3. W zakresie wskazanym w ust. 2 przez sformułowanie niezwłocznie rozumie się nie dłużej niż w ciągu 48 godzin od chwili wpływu wniosku.

**§ 9. Usunięcie lub zwrot danych osobowych**

1. Po zakończeniu świadczenia usług, o których mowa w § 2 ust. 2, zależnie od decyzji Administratora Podmiot Przetwarzający usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, o ile inne przepisy nie stanowią inaczej.

2. Podmiot Przetwarzający jest obowiązany wykonać decyzję Administratora, o której mowa w ust. 1, w terminie 7 dni od dnia jej doręczenia.

3. W przypadku decyzji Administratora o zwrocie danych, Administrator ma prawo zdecydować także na jakim nośniku dane mają zostać zwrócone.

**§ 10. Raportowanie**

1. Na wniosek Administratora, Podmiot Przetwarzający udostępnia wszelkie informacje niezbędne do realizacji lub wykazania spełnienia obowiązków wynikających z RODO.

2. Informacji, o których mowa w ust. 1, udziela się w terminie 14 dni od dnia doręczenia wniosku, z zastrzeżeniem ust. 3.

3. Jeżeli wniosek, o którym mowa w ust. 1, dotyczy realizacji obowiązku zgłoszenia naruszenia ochrony danych osobowych lub usunięcia jego skutków, Podmiot Przetwarzający udziela informacji w najbliższym możliwym terminie, nie później niż w ciągu 48 godzin od doręczenia wniosku.

4. Jeżeli Podmiot Przetwarzający wykryje podejrzenie naruszenie ochrony danych osobowych, zgłasza je Administratorowi w najbliższym możliwym terminie, nie później niż w ciągu 48 godzin od wykrycia podejrzenia naruszenia. Na wniosek Administratora, Podmiot Przetwarzający zobowiązany jest do pomocy Administratorowi w określeniu zakresu, w jakim bezpieczeństwo zostało naruszone, jak również w przygotowaniu wszelkich powiadomień dla Prezesa Urzędu Ochrony Danych Osobowych jak i dla osób, których dane te dotyczą (w tym także obowiązków wskazanych w art. 32-36 RODO uwzględniając charakter przetwarzania i dostępne informacje).

5. Podmiot przetwarzający niezwłocznie informuje Administratora o:

a) jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania powierzonych danych osobowych,

b) o wydaniu jakiegokolwiek orzeczenia dotyczącego przetwarzania powierzonych danych osobowych,

c) o wszelkich planowanych lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania powierzonych danych osobowych.

6. Na wniosek Administratora, Podmiot Przetwarzający zobowiązany jest do stwierdzenia lub udokumentowania, że spełnia on wymogi przewidziane przepisami RODO, włączając w to dokumentację dotyczącą przepływu danych w Podmiocie Przetwarzającym oraz procedurę lub politykę przetwarzania danych osobowych. Ponadto, na żądanie, Podmiot Przetwarzający zobowiązany jest do przedstawienia Administratorowi kopii umów dotyczących powierzenia przetwarzania danych zawartych z podmiotami przetwarzającymi dane w ramach dalszego powierzenia przetwarzania danych.

**§ 11. Audyty**

1. W celu weryfikacji spełniania obowiązków wynikających z niniejszej umowy, Administrator ma prawo przeprowadzenia audytu Podmiotu przetwarzającego. Audyt może zostać przeprowadzony przez wskazany przez Administratora niezależny podmiot zewnętrzny.

2. Prawo przeprowadzenia audytu obejmuje:

a) wstęp do pomieszczeń, w których znajdują się zasoby uczestniczące w operacjach przetwarzania powierzonych danych osobowych,

b) żądanie złożenia pisemnych lub ustnych wyjaśnień od osób upoważnionych do przetwarzania powierzonych danych osobowych,

c) wgląd do wszelkich dokumentów i wszelkich danych mających bezpośredni związek z celem audytu,

d) przeprowadzanie oględzin urządzeń, nośników oraz systemów informatycznych służących do przetwarzania powierzonych danych.

3. Administrator może korzystać z prawa przeprowadzenia audytu w godzinach pracy Podmiotu Przetwarzającego, o ile zawiadomi Podmiot Przetwarzający o takim zamiarze przynajmniej na 14 dni roboczych przed audytem.

4. Podmiot Przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas audytu przez Administratora.

**§ 12. Odpowiedzialność Podmiotu Przetwarzającego**

1. Podmiot Przetwarzający jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią umowy, a w szczególności za udostępnienie powierzonych do przetwarzania danych osobowych osobom nieupoważnionym.

2. W razie udostępnienia danych osobowych osobom nieupoważnionym lub przetwarzania powierzonych danych osobowych niezgodnie z § 2, Podmiot Przetwarzający będzie obowiązany do zapłaty na rzecz Administratora kary umownej, przy czym wysokość kary umownej ograniczona jest do wartości wynagrodzenia uzyskanego przez Podmiot Przetwarzający z tytułu umowy, w ramach której dane te zostały powierzone, za okres nie dłuższy niż ostatnie 12 miesięcy, a jeśli okres był krótszy, za ten okres. Administratorowi nie przysługuje prawo dochodzenia odszkodowania w wysokości przewyższającej zastrzeżoną karę umowną.

3. Administrator powinien wykazać, iż Podmiot Przetwarzający uzyskał dostęp (skopiował, wyświetlił zawartość, otrzymał na jakimś nośniku) do danych określone w §2, pkt 1. b). Do wykazania tego w systemie IT służą usługi audytowania dostępu systemów Microsoft Windows lub GNU/Linux. Do wskazania tego na innym nośniku powinny zostać zastosowane odpowiednie protokoły potwierdzające otrzymanie takich danych. Brak możliwości wykazania, iż Podmiot Przetwarzający uzyskał dostęp do powierzonych danych (skopiował, wyświetlił zawartość, otrzymał na jakimś nośniku), wyklucza odpowiedzialność Podmiotu Przetwarzającego.

4. Jeżeli wskutek naruszenia postanowień niniejszej umowy przez Podmiot Przetwarzający, Administrator będzie obowiązany do zapłaty odszkodowania lub zostanie w inny sposób pociągnięty do odpowiedzialności za naruszenie przepisów o ochronie danych osobowych, Administrator może żądać od Podmiotu Przetwarzającego naprawy wynikłej stąd szkody, przy czym odpowiedzialność Podmiotu Przetwarzającego ograniczona jest do wartości wynagrodzenia uzyskanego przez Podmiot Przetwarzający z tytułu umowy, w ramach której dane te zostały powierzone, za okres nie dłuższy niż ostatnie 12 miesięcy, a jeśli okres był krótszy, za ten okres.

5. Podmiot Przetwarzający wyklucza się z całkowitej odpowiedzialności za wyciek danych z systemu IT Administratora, nawet jeżeli posiadał do niego pełny dostęp, jeżeli Administrator nie zastosował odpowiednich form zabezpieczeń, które definiuje załącznik numer 1 do umowy.

**§ 13. Postanowienia końcowe**

1. Niniejsza umowa zostaje zawarta na czas trwania Umowy Głównej.

2. Każda ze stron może wypowiedzieć niniejszą umowę z zachowaniem terminów wypowiedzenia przewidzianych w umowie o świadczenie usług o której mowa w § 2 ust. 2, przy czym wypowiedzenie niemniejszej umowy stanowi jednoczesne wypowiedzenie umowy, o której mowa w § 2 ust. 2.

3. Administrator może rozwiązać niniejszą umowę ze skutkiem natychmiastowym, gdy Podmiot Przetwarzający:

a) pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas audytu nie usunie ich w wyznaczonym terminie,

b) przetwarza dane osobowe w sposób niezgodny z umową,

c) powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody Administratora.

4. W okresie trzech miesięcy od wygaśnięcia, upływu okresu wypowiedzenia lub rozwiązania ze skutkiem natychmiastowym umowy, o której mowa w § 2 ust. 2, Administrator zachowuje prawo przeprowadzenia audytu, o którym mowa w § 11, w zakresie weryfikacji wykonania obowiązku zwrotu lub usunięcia danych osobowych, o którym mowa w § 9.

5. Podmiot Przetwarzający niezwłocznie informuje Administratora, jeśli jego zdaniem wydane mu polecenie stanowi naruszenie przepisów z zakresu ochrony danych osobowych w tym RODO.

6. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

7. W sprawach nieuregulowanych zastosowanie będą miały przepisy Kodeksu cywilnego oraz RODO.

8. Sądem właściwym do rozstrzygania spraw z zakresu niniejszej umowy jest sąd polski według właściwości ogólnej.

…………………………………. ………………………………….....

 Administrator Podmiot Przetwarzający

**ZAŁĄCZNIK NR 1**

Obie strony wspólnie przyjmują, iż w przypadku otrzymania w którejś z kategorii 5 punktów lub sumarycznie 21 punktów, Administrator nie zastosował odpowiednich form zabezpieczenia. Co za tym idzie, Przetwarzający zwolniony jest z jakichkolwiek zarzutów w przypadku stwierdzenia wycieku danych z elementów systemów IT, do których Przetwarzający miał dostęp.

**Dostęp do serwerowni i punktów dystrybucyjnych:**

1 - Wydzielona zamykana przestrzeń. Opracowana polityka dostępu do przestrzeni. Dostęp monitorowany.

2 - Wydzielona zamykana przestrzeń. Opracowana polityka dostępu do przestrzeni.

3 - Wydzielona zamykana przestrzeń.

4 - Urządzenia w przestrzeni współużytkowanej. Zamykana szafa. Dostęp monitorowany.

5 - Urządzenia w przestrzeni współużytkowanej. Brak mechanizmów bezpieczeństwa fizycznego.

**Segmentacja sieci wewnętrznej (VLAN lub SGT/EPG):**

1 - Segmentacja obejmuje pracowników, telefony, serwery udostępniające usługi wewnętrznie, serwery udostępniające usługi dla świata, gości, interfejsy zarządzania i inne.

2 - Oddzielne segmenty min. dla serwerów wewnętrznych, zewnętrznych, pracowników i gości.

3 - Oddzielne segmenty min. dla serwerów, pracowników i gości.

4 - Oddzielne segmenty min. dla pracowników i gości.

5 - Wszystko w jednym segmencie.

**Ochrona poczty elektronicznej E-Mail:**

1 - Wykorzystywanie S/MIME lub GPG. SPF, DKIM i DMARC. Ochrony antywirusowa i antyspamowa. Komercyjne rozwiązania ochrony z aktywną subskrypcją.

2 - SPF, DKIM i DMARC. Ochrony antywirusowa i antyspamowa. Komercyjne rozwiązania ochrony z aktywną subskrypcją.

3 - SPF, DKIM i DMARC. Ochrona antywirusowa i antyspamowa. Brak komercyjnych rozwiązań ochrony.

4 - SPF, DKIM. Ochrona antywirusowa i antyspamowa. Brak komercyjnych rozwiązań ochrony.

5 - Brak mechanizmów ochrony poczty elektronicznej.

**Dostęp do sieci wewnętrznej:**

1 - Tymczasowe dostępy do sieci gościnnej. IEEE 802.1X do sieci przewodowej i bezprzewodowej. Aktywne mechanizmy L2/L3 Security. Sprawdzanie stanu stacji.

2 - Tymczasowe dostępy do sieci gościnnej. IEEE 802.1X do sieci przewodowej i bezprzewodowej. Aktywne mechanizmy L2/L3 Security.

3 - Tymczasowe dostępy do sieci gościnnej. IEEE 802.1X do sieci bezprzewodowej. Aktywne mechanizmy L2/L3 Security.

4 - Klucz współdzielony dla gości. Klucz współdzielony do sieci bezprzewodowej. Aktywne mechanizmy L2/L3 Security.

5 - Brak mechanizmów bezpieczeństwa dostępu do sieci.

**Aktualne oprogramowanie urządzenia/systemu:**

1 - Zawiera stabilne oprogramowanie z wszystkimi poprawkami bezpieczeństwa.

2 - Zawiera rozwojowe oprogramowanie z wszystkimi poprawkami bezpieczeństwa.

3 - Nie był aktualizowany przez okres 2-mc.

4 - Nie był aktualizowany przez okres 4-mc.

5 - Nie był aktualizowany przez okres 6-mc i dłużej.

**Dostęp do aplikacji i stron www:**

1 - Logowanie tylko po HTTPS. Ochrona za pomocą WAF i weryfikacja integralności plików strony. Strona jest aktualizowana co minimum 3-mc. Strona zamknięta w kontenerze lub oddzielnej VM.

2 - Logowanie tylko po HTTPS. Ochrona za pomocą WAF i weryfikacja integralności plików strony. Brak aktualizacji od ponad 4-mc. Strona zamknięta w kontenerze lub oddzielnej VM.

3 - Logowanie tylko po HTTPS. Ochrona za pomocą WAF i weryfikacja integralności plików strony. Brak aktualizacji od ponad 12-mc. Strona zamknięta w kontenerze lub oddzielnej VM.

4 - Logowanie tylko po HTTPS. Weryfikacja integralności plików strony. Brak WAF. Brak aktualizacji od ponad 12-mc.

5 - Logowanie bez HTTPS. Brak WAF i weryfikacji integralności plików strony. Brak aktualizacji od ponad 12-mc.

**Dostęp do aktualizacji bezpieczeństwa i zaleceń:**

1 - Producent oprogramowania gwarantuje aktualizacje bezpieczeństwa i zalecenia po pojawiających się podatnościach stosowną umową/serwisem/subskrypcją.

2 - Producent oprogramowania gwarantuje aktualizacje bezpieczeństwa stosowną umową/serwisem/subskrypcją.

3 - Producent oprogramowania udostępnia bez żadnych zobowiązań aktualizacje bezpieczeństwa i zalecenia po pojawiających się podatnościach.

4 - Producent oprogramowania udostępnia bez żadnych zobowiązań aktualizacje bezpieczeństwa.

5 - Brak aktualizacji bezpieczeństwa przez producenta oprogramowania.

**Bezpieczeństwo danych na serwerze z zewnątrz:**

1 - Dostęp zabezpieczony przez system komercyjny system IPS z aktywną subskrypcją, wykorzystanie szyfrowanych połączeń i system serwera zawierający wszystkie aktualizacje bezpieczeństwa.

2 - Dostęp zabezpieczony przez system komercyjny system IPS z aktywną subskrypcją, wykorzystanie szyfrowanych połączeń i system serwera był nieaktualizowany do 1-mc.

3 - Dostęp zabezpieczony przez system komercyjny system IPS z aktywną subskrypcją, wykorzystanie szyfrowanych połączeń i system serwera nieaktualizowany do 3-mc.

4 - Wykorzystanie szyfrowanych połączeń do usług i aktualny system.

5 - Brak systemu IPS z aktywną subskrypcją i nieaktualny system lub brak szyfrowanych połączeń.

**Bezpieczeństwo danych na stacji końcowej:**

1 - Lokalny system antywirusowy i Firewall, system AMP i IPS na brzegu sieci i system z wszystkimi łatkami bez dostępu bezpośredniego z sieci Internet.

2 - Lokalny system antywirusowy i Firewall, system AMP na brzegu sieci i system z wszystkimi łatkami bez dostępu bezpośredniego z sieci Internet.

3 - Lokalny system antywirusowy i Firewall, system z wszystkimi łatkami bez dostępu bezpośredniego z sieci Internet.

4 - Lokalny system antywirusowy i Firewall, system AMP i IPS na brzegu sieci i system z wszystkimi łatkami. System dostępny z sieci Internet.

5 - Brak antywirusa lub nieaktualny system operacyjny.

Należy pamiętać, iż wiele usług systemu IT jest ze sobą powiązanych i prosty wyciek loginu lub hasła może mieć wpływ na lawinowy wyciek dużo większej ilości danych.

…………………………………. ………………………………….....

 Administrator Podmiot przetwarzający