BURMISTRZ
Miasta i Gminy Kunów

Zarządzenie Nr 110.2018

Burmistrza Miasta i Gminy Kunów

z dnia 15.06.2018

w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji w Urzędzie Miasta i Gminy w Kunowie oraz w gminnych jednostkach organizacyjnych

Na podstawie art. 30 ust. 1 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz.U. z 2018 poz. 994 i 1000) oraz art. 24 ust. 2 oraz art. 32 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. UE L 1192 z dnia 04.05.2016) zarządza się, co następuje:

§ 1

Wprowadza się Politykę Bezpieczeństwa Informacji w Urzędzie Miasta i Gminy w Kunowie oraz w gminnych jednostkach organizacyjnych:

1. Miejsko Gminny Ośrodek Pomocy Społecznej w Kunowie,
2. Zakład Gospodarki Komunalno Mieszkaniowej w Kunowie,
3. Miejsko Gminna Biblioteka Publiczna w Kunowie,
4. Publiczne Przedszkole w Kunowie,
5. Publiczna Szkoła Podstawowa w Kunowie,
6. Zespół Szkolno Przedszkolny w Janiku,

w brzmieniu stanowiącym załącznik nr 1 do niniejszego zarządzenia.

§ 2

Polityka Bezpieczeństwa Informacji ma zastosowanie na wszystkich stanowiskach pracy, gdzie przetwarzane są dane osobowe lub praca odbywa się w systemach informatycznych Urzędu Miasta i Gminy w Kunowie oraz gminnych jednostek organizacyjnych wymienionych w § 1.

§ 3

1. Zobowiązuje się wszystkich pracowników Urzędu Miasta i Gminy w Kunowie oraz gminnych jednostek organizacyjnych do zapoznania się z treścią Polityki Bezpieczeństwa Informacji, w terminie dwóch tygodni od wejścia w życie zarządzenia oraz praktycznego wdrożenia określonych w niej zasad przetwarzania danych osobowych i bezpiecznej pracy w systemach informatycznych Urzędu Miasta i Gminy w Kunowie oraz gminnych jednostek organizacyjnych wymienionych w § 1.
2. Za wykonanie postanowień ust. 1 odpowiadają bezpośredni przełożeni poszczególnych pracowników.

§ 4

Wykonanie zarządzenia powierza się wspólnemu Inspektorowi Ochrony Danych.

§ 5

Traci moc Zarządzenie Nr 59/15 Burmistrza Miasta i Gminy Kunów z dnia 11.03.2015 w sprawie wdrożenia Instrukcji Zarządzania Systemem Informatycznym Urzędu Miasta i Gminy w Kunowie oraz Zarządzenie Nr 60/15 Burmistrza Miasta i Gminy Kunów z dnia 11.03.2015 w sprawie wdrożenia Polityki Bezpieczeństwa Przetwarzania Danych Osobowych w Urzędzie Miasta i Gminy w Kunowie.

§ 6

Zarządzenie wchodzi z dniem podpisania.

BURMISTRZ

mgr Lech Lodej

Monika Czekaj
RADCA PRAWNY
KL-K-631

Polityka Bezpieczeństwa Informacji

Urzędu Miasta i Gminy w Kunowie oraz gminnych jednostek organizacyjnych

Data opracowania: maj 2018

Spis treści

1 CEL, ZAKRES I POJĘCIA

1.1 WSTĘP

Niniejsza Polityka stanowi element Systemu Zarządzania Bezpieczeństwem Informacji i opracowana została w oparciu o dobre praktyki bazujące m.in. na normach ISO/IEC z serii 27000 oraz bibliotekach ITIL i literaturze fachowej poświęconej bezpieczeństwu informacji oraz bezpieczeństwu teleinformatycznemu. Zapisy niniejszej Polityki dostosowane są również do obowiązującego prawa, w tym Ogólnego Rozporządzenia o Ochronie Danych z dnia 27 kwietnia 2016 (Dz. Urz. UE L119 z 04.05.2016), ustawa z dnia 5 sierpnia 2010 r. o Ochronie Informacji Niejawnych, Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych).

1.2 DEKLARACJA STOSOWANIA

Opracowanie Polityki Bezpieczeństwa Informacji i stosowanie się do zapisów w niej zawartych ma na celu rozpoznanie i minimalizację ryzyka związanego z zagrożeniami, które mogą prowadzić do naruszenia bezpieczeństwa krytycznych aktywów, a zwłaszcza danych osobowych. Niniejsza Polityka Bezpieczeństwa Informacji opracowana została z inicjatywy i przy wsparciu władz Urzędu Miasta i Gminy w Kunowie. Do stosowania zapisów zawartych w Polityce zobowiązuje się zatem wszystkich pracowników urzędu oraz następujących gminnych jednostek organizacyjnych:

- Publicznej Szkoły Podstawowej w Kunowie, razem z odziałem Gimnazjum
- Publicznego Przedszkola w Kunowie
- Zespołu Szkolno - Przedszkolnego w Janiku
- Miejsko - Gminnego Ośrodka Pomocy Społecznej w Kunowie
- Miejsko - Gminnej Biblioteki Publicznej w Kunowie
- Zakładu Gospodarki Komunalno-Mieszkaniowej w Kunowie

1.3 PODSTAWOWE DEFINICJE I ROLE

Do celów realizacji zadań zawartych w Polityce Bezpieczeństwa Informacji definiuje się poniższe pojęcia oraz role użytkowników.

1.3.1 POJĘCIA

Aktywa
wszystkie urządzenia, wyposażenie, systemy, dane ze szczególnym uwzględnieniem danych osobowych, a także informacje i osoby z nich korzystające, które stanowią wartość dla organizacji.
Instrukcja Analizy Ryzyka (IAR)
dokument opisujący zasady przeprowadzania okresowej analizy ryzyka będący częścią Systemu Zarządzania Bezpieczeństwem Informacji.
Dane osobowe
Wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osoba możliwa do zidentyfikowania to taka, której tożsamość da się określić bezpośrednio lub pośrednio, wskazując jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne.

Szczególne kategorie danych (tzw. dane wrażliwe)
Dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dotyczące zdrowia, seksualności lub orientacji seksualnej, a także informacje o wyrokach skazujących i naruszeniach prawa.
Incydent bezpieczeństwa
Zdarzenie naruszające lub mogące naruszyć bezpieczeństwo aktywów chronionych przez Politykę Bezpieczeństwa Informacji
Informacja niejawna
w rozumieniu ustawy o ochronie informacji niejawnych - taka, której nieuprawnione ujawnienie może spowodować szkody dla państwa (osłabia jego bezpieczeństwo lub narusza interesy jego obywateli). Dotyczy bezpieczeństwa, obronności, polityki, nauki, gospodarki.
Instrukcja Ochrony Danych Osobowych (IODO)
Dokument określający zasady bezpieczeństwa danych osobowych w myśl Ogólnego Rozporządzenia o Ochronie Danych (RODO).
Naruszenie ochrony danych osobowych
Incydent bezpieczeństwa skutkujący lub mogący skutkować naruszeniem integralności, poufności lub dostępności danych osobowych (przykłady naruszeń i metody postępowania z nimi zawarte zostały w Instrukcji Ochrony Danych Osobowych (załącznik Z2).
Podatność
Cecha aktywów sprzyjająca pojawieniu się określonych zagrożeń
Przetwarzanie danych
Każde uporządkowane wykonywanie operacji na tychże danych, w tym m.in. wgląd, edycja, modyfikacja, usuwanie, kopiowanie, przenoszenie, archiwizacja, odtwarzania, udostępnianie, powierzanie
Umowa SLA (Service Level Agreement)
Umowa pomiędzy usługodawcą a klientem zawierająca zapisy dotyczące gwarantowanego poziomu jakości świadczonej usługi.
System Zarządzania Bezpieczeństwem Informacji (SZBI)
Zbiór polityk, instrukcji, regulaminów, szablonów dokumentów, procedur oraz rozwiązań organizacyjnych mających na celu zapewnienie bezpieczeństwa informacji w organizacji.
Zagrożenie
Stan lub zdarzenie mogące prowadzić do wystąpienia incydentu naruszenia bezpieczeństwa

1.3.2 ROLE ZWIĄZANE Z REALIZACJĄ ZAPISÓW POLITYKI BEZPIECZEŃSTWA

ASI
Administrator Systemów Informatycznych – jedna lub więcej osób odpowiedzialnych za realizację zadań związanych z utrzymaniem i zarządzaniem systemami teleinformatycznymi wg zapisów Polityki Bezpieczeństwa Informacji.
IOD
Inspektor Ochrony Danych - w rozumieniu Ogólnego Rozporządzenia o Ochronie Danych (RODO) – osoba odpowiedzialna m.in. za nadzór nad realizacją zapisów Polityki Bezpieczeństwa oraz ochronę danych osobowych i analizę ryzyka.
Pełnomocnik d/s Informacji Niejawnych

Osoba odpowiedzialna za nadzór nad przetwarzaniem informacji niejawnych w myśl Ustawy o Ochronie Informacji Niejawnych.

1.4 CEL STOSOWANIA POLITYKI BEZPIECZEŃSTWA INFORMACJI

Główne cele stosowania Polityki Bezpieczeństwa Informacji to:

- Ochrona krytycznych aktywów urzędu i jednostek pomocniczych
- Analiza, szacowanie i ocena ryzyka związanego z zagrożeniami
- Minimalizacja negatywnych skutków naruszeń bezpieczeństwa
- Zapewnienie ciągłości procesów realizowanych przez urząd i jednostki pomocnicze
- Zapewnienie zgodności z obowiązującymi przepisami prawa
- Ochrona dobrego wizerunku urzędu i jednostek pomocniczych
- Ograniczenie uchybień organizacyjnych i błędów ludzkich

1.5 ZAKRES I GRANICE OBOWIĄZYWANIA

Polityka Bezpieczeństwa Informacji obejmuje swoim zakresem wszystkie procesy i komórki organizacyjne Urzędu Miasta i Gminy w Kunowie oraz gminnych jednostek organizacyjnych, biorące udział w przetwarzaniu informacji oraz mające dostęp do aktywów objętych ochroną, które zdefiniowane zostały w punkcie następnym. W zakres obszaru objętego ochroną niniejszej Polityki wchodzą:

- Publiczna Szkoła Podstawowa w Kunowie, ul. Szkolna 1, 27-415 Kunów razem z odziałem Gimnazjum, ul. Fabryczna 1, 27-415 Kunów
- Publiczne Przedszkole w Kunowie os. E. Dziewulskiego 5, 27-415 Kunów
- Zespół Szkolno - Przedszkolny w Janiku, ul. Szkolna 27, 27-415 Kunów
- Miejsko - Gminny Ośrodek Pomocy Społecznej w Kunowie, ul. Warszawska 45B, 27-415 Kunów wraz ze świetlicą przy ul. Warszawskiej 56 oraz budynkiem „Senior +" przy ul. Fabrycznej 1, 27-415 Kunów
- Miejsko - Gminna Biblioteka Publiczna w Kunowie, ul. Warszawska 48, 27-415 Kunów
- Zakład Gospodarki Komunalno-Mieszkaniowej w Kunowie, ul. Partyzantów 47, 27-415 Kunów.

1.6 WYKAZ AKTYWÓW OBJĘTYCH OCHRONĄ

Przez aktywa objęte Polityką Bezpieczeństwa Informacji rozumie się wszystkie urządzenia, wyposażenie, systemy, dane oraz informacje, które stanowią szczególną wartość dla Urzędu Miasta i Gminy w Kunowie oraz gminnych jednostek organizacyjnych ze względu na ich udział w zadaniach realizowanych przez urząd i jego jednostki lub ochronę, której podlegają na mocy przepisów prawa. Szczegółowy wykaz tych aktywów zawarty został poniżej.

1.6.1 INFRASTRUKTURA TELEINFORMATYCZNA

- Urządzenia sieciowe i telekomunikacyjne
- Urządzenia serwerowe (serwery, systemy pamięci masowych)
- Urządzenia i systemy do backupu i archiwizacji
- Urządzenia wspomagające prace serwerowni (klimatyzatory, UPS-y, systemy monitoringu środowiskowego)
- Systemy i oprogramowanie serwerowe służące do pełnienia obowiązków służbowych we wszystkich komórkach organizacyjnych
- Systemy baz danych

- Urządzenia komputerowe i telefoniczne wykorzystywane przez pracowników urzędu i jednostek pomocniczych do pełnienia swoich obowiązków służbowych

1.6.2 ZBIORY DANYCH SZCZEGÓLNIE CHRONIONYCH

- Zbiory danych osobowych według Rejestru Czynności Przetwarzania prowadzonego przez Inspektora Ochrony Danych (IOD) wg wzoru z załącznika „W6 – Rejestr Czynności Przetwarzania"
- Informacje niejawne przetwarzane wg instrukcji dotyczącej sposobu i trybu przetwarzania informacji niejawnych o klauzuli „zastrzeżone", nad którymi nadzór sprawuje Pełnomocnik ds. Ochrony Informacji Niejawnych

1.6.3 INFRASTRUKTURA WYKORZYSTYWANA DO ZABEZPIECZENIA FIZYCZNEGO

- Systemy alarmowe
- Systemy kontroli dostępu
- Klucze do pomieszczeń, w których przetwarzane są dane szczególnie chronione lub w których znajdują się wymienione w punktach poprzednich aktywa

1.6.4 DOKUMENTACJA W FORMIE PAPIEROWEJ

- Wszelka dokumentacja zgromadzona przez poszczególne komórki organizacyjne w ramach prowadzonych przez nie zadań
- Licencje pozwalające na użytkowanie zakupionego oprogramowania
- Dokumentacja przekazana do archiwum
- Dokumentacja wewnętrzna regulująca pracę urzędu, w tym niniejsza Polityka

1.7 DEFINICJA BEZPIECZEŃSTWA

Na potrzeby Polityki Bezpieczeństwa Informacji przyjmuje się następującą definicję bezpieczeństwa: przez bezpieczeństwo aktywów rozumiemy zapewnienie ochrony następujących ich cech:

- **Poufności** – właściwości zapewniającej, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom albo procesom.

- **Integralności danych** – właściwości zapewniającej, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany.

- **Integralności systemu** – właściwości polegającej na tym, że system realizuje swoją zamierzoną funkcję w sposób nienaruszony, wolny od nieautoryzowanej manipulacji, celowej lub przypadkowej.

- **Dostępności** – właściwości bycia dostępnym i możliwym do wykorzystania na żądanie, w założonym czasie, przez autoryzowanych użytkowników.

- **Rozliczalności** - właściwości zapewniającej, że określone działania dowolnego podmiotu mogą być jednoznacznie przypisane temu podmiotowi

1.8 WARTOŚĆ CHRONIONYCH INFORMACJI I KONSEKWENCJA ICH UTRATY.

Zagrożenia, na które narażone są aktywa chronione przez Politykę Bezpieczeństwa Informacji pociągają za sobą określone straty materialne związane z przestojami w pracy, utratą danych, kosztami odzyskania danych i kosztami przywrócenia systemów do stanu początkowego. Pozbawienie urzędu właściwej ochrony aktywów może również pociągać za sobą szereg konsekwencji takich jak:

- Brak możliwości realizowania ustawowych zadań
- Utrata zaufania ze strony klientów
- Utrata dobrego wizerunku
- Konsekwencje prawne

2 KLASYFIKACJA AKTYWÓW I ICH WPŁYW NA PROCESY

W celu realizacji podstawowych założeń Polityki Bezpieczeństwa Informacji konieczne jest dokonanie klasyfikacji objętych nią aktywów pod względem ich niezbędności, oczekiwanego poziomu bezpieczeństwa oraz możliwego wpływu na działanie urzędu lub jednostek pomocniczych.

2.1 KLASYFIKACJA AKTYWÓW OBJĘTYCH OCHRONĄ

W celu skutecznego stosowania procedury analizy ryzyka zapewniającej ochronę aktywów stosowną do ich wartości przyjęto następującą ich klasyfikację:

a) Jako **aktywa krytyczne**, bez których niemożliwe jest funkcjonowanie urzędu i jednostek pomocniczych, lub których utrata grozi poważnymi konsekwencjami sklasyfikowano:

- Urządzenia serwerowe (serwery, systemy pamięci masowych)
- Systemy i oprogramowanie serwerowe służące do pełnienia obowiązków służbowych we wszystkich komórkach organizacyjnych
- Systemy baz danych
- Zbiory danych osobowych według Rejestru Czynności Przetwarzania prowadzonego przez Inspektora Ochrony Danych wg wzoru z załącznika „W6 - Rejestr Czynności Przetwarzania"
- Informacje niejawne przetwarzane wg instrukcji dotyczącej sposobu i trybu przetwarzania informacji niejawnych o klauzuli „zastrzeżone", nad którymi nadzór sprawuje Pełnomocnik ds. Ochrony Informacji Niejawnych

b) Jako **aktywa ważne**, których zadania mogą być wykonane innymi środkami ale przy dodatkowym nakładzie sił i kosztów, lub których krótkotrwała niedostępność nie powoduje poważnych konsekwencji sklasyfikowano:

- Urządzenia sieciowe i telekomunikacyjne
- Urządzenia i systemy do backupu i archiwizacji
- Urządzenia wspomagające prace serwerowni (klimatyzatory, UPS-y, systemy monitoringu środowiskowego)
- Systemy alarmowe
- Systemy kontroli dostępu

c) Jako **aktywa zasadnicze**, których zadania przy małym nakładzie dodatkowych sił i środków mogą być wykonywane np. ręcznie, lub przy użyciu innych narzędzi sklasyfikowano:

- Urządzenia komputerowe i telefoniczne wykorzystywane przez pracowników do pełnienia swoich obowiązków służbowych

2.2 OCENA SKUTKÓW UTRATY AKTYWÓW

W celu zapewnienia odpowiedniej ochrony sklasyfikowanym w punkcie poprzednim aktywom konieczne jest zdefiniowanie i przypisanie im określonych poziomów bezpieczeństwa w zależności od wpływu, który mogą one mieć na funkcjonowanie urzędu. W odniesieniu do przeprowadzonej w punkcie poprzednim klasyfikacji zdefiniowano następujące poziomy wpływu, które będą miały zastosowanie w procesie analizy ryzyka:

a) **Krytyczny wpływ** - dotyczy aktywów sklasyfikowanych w punkcie poprzednim jako krytyczne, ich utrata lub uszkodzenie mogą spowodować załamanie w funkcjonowaniu urzędu lub jednostek pomocniczych oraz wywrzeć niekorzystne skutki społeczne.

b) **Znaczący wpływ** – dotyczy aktywów sklasyfikowanych w punkcie poprzednim jako ważne, ich utrata lub uszkodzenie mogą spowodować znaczne trudności w normalnym funkcjonowaniu urzędu lub jednostek pomocniczych, nie pociągając za sobą niekorzystnych skutków społecznych.

c) **Niski wpływ** – dotyczy aktywów sklasyfikowanych w punkcie poprzednim jako zasadnicze, ich utrata lub uszkodzenie wpłyną nieznacznie na funkcjonowanie urzędu lub jednostek pomocniczych

3 ANALIZA RYZYKA

Analiza, szacowanie i ocena ryzyka zagrożeń mogących wpłynąć na bezpieczeństwo aktywów objętych Polityką Bezpieczeństwa Informacji jest jednym z zadań koniecznych do zapewnienia ciągłości działania urzędu i jednostek pomocniczych. Ma też na celu eliminację lub minimalizację negatywnych skutków incydentów naruszenia bezpieczeństwa. Za realizację zadań związanych z analizą ryzyka odpowiedzialny jest Inspektor Ochrony Danych. W zadaniach tych wspierać go powinni Administratorzy Systemów Informatycznych.

3.1 ZASADY PRZEPROWADZANIA

Analiza ryzyka przeprowadzana jest minimum raz w roku na zasadach opisanych w Instrukcji Analizy Ryzyka stanowiącej **załącznik Z1.** do niniejszej Polityki. Wyniki szacowania ryzyk po zakończeniu procedury analizy ryzyka powinny być zachowane do wglądu. Na podstawie otrzymanych w wyniku szacowania ryzyka danych podjęte powinny być odpowiednie kroki mające na celu eliminację, minimalizację lub przeniesienie ryzyk, których poziom jest wyższy niż akceptowalny.

3.2 ZASADY POSTĘPOWANIA Z RYZYKIEM

Końcowym etapem analizy ryzyka jest podjęcie decyzji o jego akceptacji lub przeciwdziałaniu jego skutkom w zależności od otrzymanej wartości ryzyka. Poniższa tabela prezentuje wartości graniczne poziomów ryzyka, w zależności od których konieczne jest podjęcie odpowiednich działań. Informacje na temat zasad postępowania z ryzykiem nieakceptowalnym zawarte zostały w Instrukcji Analizy Ryzyka.

Wartość ryzyka	Poziom akceptowalności ryzyka
1	Akceptowalne
2	Akceptowalne
3 - 4	Warunkowe
6	Nieakceptowalne

4 ZABEZPIECZENIE GRUP INFORMACJI SZCZEGÓLNIE CHRONIONYCH

W celu spełnienia wymogów prawnych dotyczących przetwarzania poszczególnych grup informacji szczególnie chronionych, zdefiniowane zostały dedykowane tym wymogom odrębne instrukcje definiujące zasady przetwarzania. Podejście takie umożliwia wydzielenie z Polityki Bezpieczeństwa Informacji wymogów specyficznych dla danych grup informacji.

4.1 OCHRONA DANYCH OSOBOWYCH

W celu ochrony danych osobowych ustanowiona została dedykowana im Instrukcja Ochrony Danych Osobowych stanowiąca **załącznik Z2.** do niniejszej Polityki. Instrukcja ta reguluje wszelkie kwestie związane m.in. z przetwarzaniem danych osobowych, nadawaniem i odbieraniem uprawnień, upoważnieniami do przetwarzania oraz umowami powierzenia danych osobowych, a także dokumentowaniem i zgłaszaniem naruszeń bezpieczeństwa danych osobowych.
Osobą odpowiedzialną za nadzór nad przestrzeganiem zapisów Instrukcji Bezpieczeństwa Danych Osobowych oraz rozstrzyganie kwestii z nią związanych jest Inspektor Ochrony Danych.

4.2 OCHRONA INFORMACJI NIEJAWNYCH

W celu ochrony informacji niejawnych zdefiniowana została instrukcja dotycząca sposobu i trybu przetwarzania informacji niejawnych o klauzuli „zastrzeżone". Instrukcja ta reguluje wszelkie kwestie związane m.in. z wytwarzaniem, przyjmowaniem oraz przetwarzaniem informacji niejawnych oraz pracą Kancelarii Informacji Niejawnych.
Osobą odpowiedzialną za nadzór nad przestrzeganiem zapisów powyższej instrukcji oraz rozstrzyganie kwestii z nią związanych jest Pełnomocnik ds. Informacji Niejawnych.

5 ZARZĄDZANIE BEZPIECZEŃSTWEM INFORMACJI

5.1 ZARZĄDZANIE INCYDENTAMI BEZPIECZEŃSTWA

Identyfikacja, zgłaszanie, inwentaryzacja i analiza incydentów bezpieczeństwa są czynnościami niezbędnymi do zapewnienia bezpieczeństwa aktywów chronionych przez niniejszą Politykę. Mają one też na celu eliminację podatności, które mogą zostać wykorzystane przez zagrożenia i w efekcie prowadzić do naruszenia bezpieczeństwa. Dlatego też, w celu realizacji zadań związanych z zarządzaniem incydentami bezpieczeństwa ustanawia się Instrukcję Zarządzania Incydentami Bezpieczeństwa i Przeciwdziałania Ich Występowaniu, stanowiącą **załącznik Z3.** do niniejszej Polityki. Za realizację zadań wynikających z powyższej instrukcji odpowiedzialni są: Administrator Systemów Informatycznych oraz Inspektor Ochrony Danych.

5.2 SZKOLENIA I AKTUALIZACJA INFORMACJI O ZAGROŻENIACH

Utrzymanie stale wysokiego poziomu bezpieczeństwa wymaga okresowego szkolenia pracowników, informowania ich o nowych zagrożeniach i sposobach ochrony przed nimi oraz przypominania o konieczności stosowania się do zapisów niniejszej Polityki Bezpieczeństwa Informacji. W celu realizacji powyższych zadań w Instrukcji Zarządzania Incydentami Bezpieczeństwa i Przeciwdziałania Ich Występowaniu (**załącznik Z3**) ustanawia się zasady szkoleń, podnoszenia świadomości pracowników oraz informowania o nowych zagrożeniach i zmianach w Polityce Bezpieczeństwa Informacji. Za realizację zadań wynikających z powyższych zapisów odpowiedzialni są: Administrator Systemów Informatycznych oraz Inspektor Ochrony Danych.

5.3 AUDYT BEZPIECZEŃSTWA

W celu weryfikacji skuteczności procedur bezpieczeństwa zdefiniowanych w Polityce Bezpieczeństwa Informacji oraz sprawdzenia stopnia jej znajomości i stosowania się do jej zapisów przez pracowników, konieczne jest okresowe badanie bezpieczeństwa aktywów objętych Polityką. W tym celu minimum raz w roku (wymóg m.in. rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności) konieczne jest przeprowadzenie audytu bezpieczeństwa. Za jego realizację odpowiada Administrator Systemów Informatycznych. Nie powinien on jednak prowadzić prac audytowych we własnym zakresie, ze względu na fakt, iż sam jest odpowiedzialny za realizację części procesów zdefiniowanych w Polityce Bezpieczeństwa Informacji. Powinien natomiast zapoznać się z wynikami audytu w celu przeanalizowania zaleceń poaudytowych oraz wprowadzenia ewentualnych usprawnień.

5.4 PLAN CIĄGŁOŚCI DZIAŁANIA

W celu zapewnienia ciągłości działania wszystkich krytycznych procesów w Urzędzie Miasta i Gminy w Kunowie oraz jednostkach pomocniczych wprowadza się Plan Ciągłości Działania. Jego zadaniem jest przygotowanie reguł postępowania w sytuacjach awaryjnych, gdy niedostępny stanie się jeden z zasobów, systemów lub pracowników pełniących krytyczną rolę w organizacji. Wchodzące w skład Planu Ciągłości Działania procedury zdefiniowane zostały w **załączniku Z5** Polityki Bezpieczeństwa Informacji.

6 PROCEDURY I ZALECENIA DLA POSZCZEGÓLNYCH GRUP PRACOWNIKÓW

Poza obowiązkami i zaleceniami wynikającymi z głównych zapisów Polityki, każdy z pracowników urzędu zobowiązany jest do zapoznania się ze szczegółowymi wytycznymi zdefiniowanymi dla poszczególnych grup pracowników.. W zależności od pełnionych obowiązków konieczność stosowania się do szczegółowych procedur i zaleceń występuje w przypadku poniższych komórek organizacyjnych oraz stanowisk pracy i ról pełnionych w ramach Polityki Bezpieczeństwa Informacji:

Nazwa komórki organizacyjnej lub stanowiska	Obowiązujące procedury i zalecenia
Wszyscy pracownicy urzędu i jednostek pomocniczych	Załącznik 8. PBI - regulamin pracy w systemie teleinformatycznym
Pracownicy biorący udział w przetwarzaniu danych osobowych	Załącznik 2. PBI – instrukcja ochrony danych osobowych
Osoby odpowiedzialne za obsługę informatyczną (ASI)	Załącznik 3. PBI – Instrukcja Zarządzania Incydentami Bezpieczeństwa Załącznik 4. PBI – Zalecenia i procedury postępowania dla pracowników odpowiedzialnych za obsługę informatyczną Załącznik 5. PBI – Plan Ciągłości Działania
Osoby odpowiedzialne za obsługę kadrową	Załącznik 6. PBI – Zalecenia i procedury postępowania dla pracowników odpowiedzialnych za obsługę kadrową
Inspektor Ochrony Danych	Załącznik 1. PBI – Instrukcja Analizy Ryzyka Załącznik 3. PBI – Instrukcja Zarządzania Incydentami Bezpieczeństwa Załącznik 5. PBI – Plan Ciągłości Działania
Osoby odpowiedzialne za obsługę zamówień publicznych oraz przygotowywanie umów	Załącznik 7. PBI – Zalecenia i procedury obowiązujące przy podpisywaniu umów
Kierownicy komórek organizacyjnych	Załącznik 5. PBI – Plan Ciągłości Działania
Osoby odpowiedzialne za realizację płatności	Załącznik 5. PBI – Plan Ciągłości Działania

ZAŁĄCZNIK 1. PBI - INSTRUKCJA ANALIZY RYZYKA

Niniejsza instrukcja przeznaczona jest dla Inspektora Ochrony Danych i ma na celu ułatwienie mu zadań związanych z obowiązkiem przeprowadzania okresowej analizy ryzyka.

METODA SZACOWANIA RYZYKA

Szacowanie ryzyka polega na określeniu zagrożeń jakim mogą podlegać aktywa oraz określeniu podatności jakie mogą być wykorzystane przez te zagrożenia, a także określeniu i oszacowaniu skutków wystąpienia powyższych zagrożeń. Wybrana na potrzeby Polityki Bezpieczeństwa Informacji metoda bazuje na dwóch następujących parametrach:

- Prawdopodobieństwie zaistnienia negatywnego zdarzenia (P)
- Możliwych skutkach, oraz ich wpływie na pracę organizacji (S)

Parametry te służą do obliczenia wskaźnika ryzyka [R] ze wzoru: $R = P \cdot S$

Szacowanie parametrów przeprowadza się na 3. stopniowej skali wg reguł przedstawionych w punktach kolejnych.

SZACOWANIE SKUTKÓW (S)

Określenie skutków zaistniałych zagrożeń odbywa się z uwzględnieniem zdefiniowanych w punkcie 2.2 Polityki Bezpieczeństwa Informacji poziomów wpływu zgodnie z poniższymi wytycznymi.

Wartość [S]	Skutek / Wpływ na działanie organizacji	Opis
1	Niski	Mała awaria, która nie ma wpływu na bieżące funkcjonowanie organizacji
2	Znaczący	Średnia awaria, nie mająca poważnego wpływu na działalność organizacji lub mająca krótkotrwały poważny wpływ
3		

SZACOWANIE PRAWDOPODOBIEŃSTWA (P)

Oceniając prawdopodobieństwo należy, w miarę możliwości, bazować na danych historycznych. Jeżeli do tej pory organizacja nie prowadziła ewidencji dotyczącej incydentów związanych z bezpieczeństwem oraz bezpieczeństwem informacji, a pracownicy nie są w stanie przypomnieć sobie występujących incydentów, należy oszacować możliwość pojawienia się takiego ryzyka na podstawie doświadczenia poszczególnych uczestników organizacji. Określenie poziomu prawdopodobieństwa powinno odbywać się zgodnie z poniższymi wytycznymi.

Wartość [P]	Opis	Prawdopodobieństwo (częstotliwość wystąpienia)
[illegible]	[illegible]	[illegible]
2	Umiarkowanie możliwe	1 x kilka lat
[illegible]	[illegible]	[illegible]

WYLICZENIE POZIOMU RYZYKA

Po ustaleniu poziomów wpływu oraz prawdopodobieństwa możemy oszacować wartość ryzyka dla wystąpienia danego zdarzenia posługując się wzorem **R = P · S** . W poniższej tabeli zawarto przykłady szacowania ryzyka wystąpienia kilku popularnych zdarzeń zagrażających bezpieczeństwu.

Zdarzenie	Skutek [S]	Prawdopodobieństwo [P]	Ryzyko [R]
Pożar serwerownii	3	1	3
Awaria switcha	2	2	4
Uszkodzenie bazy danych	2	2	4
Kradzież laptopa	1	2	[illegible]
Awaria dysku w serwerze	2	3	6
Aktywacja wirusa szyfrującego	3	3	[illegible]

Należy pamiętać, iż szacowaniu powinny podlegać w pierwszej kolejności zagrożenia związane z aktywami, które w punkcie 2.1 Polityki Bezpieczeństwa Informacji zostały sklasyfikowane jako krytyczne.

REAKCJA NA RYZYKO

Otrzymany w poprzednim punkcie poziom ryzyka należy porównać z kryteriami jego akceptacji zawartymi w poniższej tabeli. Jeżeli wartość ryzyka przekracza poziom akceptowalny należy wdrożyć plan postępowania z ryzykiem i podjąć stosowne działania dążące do unikania, minimalizacji lub przeniesienia ryzyka.

Wartość [R]	Opis	Podejmowane działania
[illegible]	[illegible]	Nie ma potrzeby podejmowania jakichkolwiek działań.
2	Akceptowalne	Działania obniżające ryzyko nie są konieczne ale wskazana jest obserwacja wskaźnika
3 - 4	Warunkowe	Konieczne podjęcie lub zaplanowanie działań zmniejszających ryzyko, chyba że występują przeciwwskazania (np. ekonomiczne)
6	Nieakceptowalne	Konieczne podjęcie lub zaplanowanie działań obniżających poziom ryzyka
[illegible]	[illegible]	Konieczne jest natychmiastowe podjęcie działań obniżających poziom ryzyka lub zatrzymanie zagrożonego procesu.

PLAN POSTĘPOWANIA Z RYZYKIEM

W przypadku, gdy poziom ryzyka przekracza akceptowalną wartość należy podjąć odpowiednie działania mające na celu jego minimalizację. Jeżeli działania takie nie są możliwe z jakichkolwiek względów (ekonomicznych, organizacyjnych, technologicznych) należy rozważyć rozwiązanie polegające na przeniesieniu ryzyka poprzez podpisanie stosownej umowy z podmiotem zewnętrznym (np. ubezpieczycielem lub dostawcą, który przejmie usługę).

Plan postępowania z ryzykiem powinien zawierać minimum informacje na temat tego kto, jakie działania i do kiedy jest zobowiązany podjąć w celu zniwelowania poziomu ryzyka. Poniżej zawarto przykładową tabelę odnoszącą się do ryzyk i koniecznych do podjęcia w związku z nimi działań:

Zagrożenie	Środki zaradcze	Osoba odpowie-dzialna	Termin wykonania
Pożar serwerownii	Zainstalować czujnik dymu		
Awaria switcha	Zakupić sprzęt rezerwowy		
Uszkodzenie bazy danych	Wdrożyć plan backupów		
Kradzież laptopa	Włączyć szyfrowanie dysku		
Awaria dysku w serwerze	Wyposażyć serwer w RAID		
Aktywacja wirusa szyfrującego	Wdrożyć ochronę AV		

ZAŁĄCZNIK 2. PBI - INSTRUKCJA OCHRONY DANYCH OSOBOWYCH

WPROWADZENIE

Niniejsza instrukcja określa reguły przetwarzania danych osobowych oraz sposoby ich zabezpieczania w celu zachowania zgodności z obowiązującymi przepisami prawa, a w szczególności z Ogólnym Rozporządzeniem o Ochronie Danych z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016).

INSPEKTOR OCHRONY DANYCH

1) Administrator Danych Osobowych (zarówno Urząd Miasta i Gminy w Kunowie, jak i każda z jednostek pomocniczych) powołuje Inspektora Ochrony Danych. Powołanie następuje na podstawie pisemnego wniosku, wg wzoru „W1 - Powołanie IOD".

2) Administrator Danych Osobowych może udzielić pełnomocnictwa Inspektorowi Ochrony Danych do nadawania uprawnień do przetwarzania danych osobowych.

3) Zadaniem Inspektora Ochrony Danych jest nadzorowanie przestrzegania zasad oraz stosowanych środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych w urzędzie i jednostkach pomocniczych.

4) Inspektor Ochrony Danych odpowiedzialny jest za prowadzenie Rejestru Czynności Przetwarzania zawierającego wykaz wszystkich zbiorów danych osobowych oraz procesów ich przetwarzania wraz ze wskazaniem stosowanych w tym celu programów komputerowych i zabezpieczeń technicznych bądź organizacyjnych. Wzór rejestru stanowi załącznik „W6 - Rejestr Czynności Przetwarzania".

5) Inspektorowi Ochrony Danych przysługują następujące uprawnienia związane z regulowaniem zasad bezpieczeństwa danych osobowych:

   a) Szkolenie pracowników z zakresu reguł obowiązujących przy przetwarzaniu danych osobowych

   b) Kontrola wiedzy osób przetwarzających dane osobowe z zakresu obowiązujących przepisów

   c) Wykonywanie planowanych i doraźnych kontroli bezpieczeństwa danych osobowych

   d) Wydawanie zaleceń dotyczących zasad przetwarzania danych osobowych

UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH

1) Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie wydane przez Administratora Danych Osobowych, które jednocześnie złożyły stosowne oświadczenie wg wzoru „W2 upoważnienie-oświadczenie".

2) Zbiór wystawionych upoważnień stanowi ewidencję osób upoważnionych do przetwarzania danych osobowych. Za jego aktualność i bezpieczeństwo odpowiada Inspektor Ochrony Danych

OSOBY UPOWAŻNIONE DO PRZETWARZANIA DANYCH OSOBOWYCH

Do obowiązków osób upoważnionych do przetwarzania danych osobowych należy:

1) Przestrzegania przepisów prawa w zakresie ochrony danych osobowych oraz postanowień Polityki Bezpieczeństwa Informacji;

2) Stosowanie się do zaleceń Inspektora Ochrony Danych;

3) Przetwarzania danych osobowych wyłącznie w zakresie ustalonym indywidualnie przez Administratora Danych Osobowych w pisemnym upoważnieniu i tylko w celu wykonywania nałożonych obowiązków służbowych;

4) Niezwłoczne informowanie Inspektora Ochrony Danych o wszelkich nieprawidłowościach dotyczących bezpieczeństwa danych osobowych wg zasad opisanych w punkcie kolejnym;

5) Ochrona danych osobowych oraz środków wykorzystywanych do ich przetwarzania przed nieuprawnionym dostępem, ujawnieniem, modyfikacją lub zniszczeniem;

6) Korzystanie z systemów informatycznych urzędu w sposób zgodny ze wskazówkami zawartymi w regulaminie pracy na stanowisku komputerowym;

7) Bezterminowe zachowanie w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia;

8) Zachowanie szczególnej staranności w trakcie wykonywania operacji przetwarzania danych osobowych w celu ochrony interesów oraz praw i wolności osób, których dane dotyczą.

9) Konsultowanie z Inspektorem Ochrony Danych oraz Administratorem Systemów Informatycznych każdego przypadku wynoszenia danych osobowych poza miejsce pracy. Bez uprzedniej zgody i odpowiedniego zabezpieczenia danych ich wynoszenie jest zabronione.

NARUSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

1) Przez naruszenie bezpieczeństwa danych osobowych rozumie się wszelkie zdarzenia skutkujące, lub mogące skutkować utratą dostępności, poufności lub integralności danych osobowych. Należą do nich np.

   - Kradzież / zgubienie nośnika danych, dokumentów lub komputera zawierających dane osobowe

   - Ujawnienie danych osobom niepowołanym (np. poprzez pomyłkowe wysłanie maila na nieprawidłowy adres, pozostawienie dokumentów w ogólnodostępnym miejscu, wyrzucenie dokumentów bez ich niszczenia, podanie danych

osobowych w rozmowie telefonicznej bez odpowiedniej weryfikacji tożsamości osoby dzwoniącej)

- Uszkodzenie, lub podejrzenie uszkodzenia danych w wyniku awarii komputera, dysku, sieci komputerowej, oprogramowania.
- Kradzież lub podejrzenie kradzieży danych w wyniku aktywacji złośliwego oprogramowania lub działania cyberprzestępców
- Utrata dostępu do danych np. w wyniku zgubienia/zapomnienia hasła lub aktywacji wirusa szyfrującego dane (tzw. cryptolockery)

2) Każde naruszenie bezpieczeństwa danych osobowych musi być niezwłocznie zgłoszone Inspektorowi Ochrony Danych wraz z podaniem możliwie szczegółowego opisu zdarzenia.

3) Inspektor Ochrony Danych po ocenie wpływu zgłoszonego zdarzenia na bezpieczeństwo danych osobowych zgłasza je w ciągu 72 godzin od momentu stwierdzenia jego wystąpienia do Urzędu Ochrony Danych Osobowych.

PODSTAWOWE ZASADY OCHRONY DANYCH OSOBOWYCH

1) Zebrane dane osobowe należy przetwarzać dla oznaczonych i zgodnych z prawem celów i nie poddawać dalszemu przetwarzaniu niezgodnemu z tymi celami.

2) Należy zadbać, aby przetwarzanie danych osobowych odbywało się zgodnie z zasadami dotyczącymi merytorycznej poprawności oraz adekwatnie do celów w jakich zostały zebrane.

3) Dane osobowe można przetwarzać nie dłużej niż jest to niezbędne do osiągnięcia celu ich przetwarzania i wymagane przepisami prawa

4) Należy zapewnić poufność, integralność oraz dostępność danych osobowych

5) Przetwarzane dane osobowe nie mogą być udostępniane bez zgody osób, których dane dotyczą, chyba że udostępnia się te dane organom państwowym lub organom samorządu terytorialnego w związku z prowadzonym postępowaniem.

OBOWIĄZEK INFORMACYJNY

1) Przygotowując wszelkie papierowe lub elektroniczne dokumenty, na których zbierane są dane osobowe (formularze, ankiety, wnioski, oświadczenia itp.) należy zadbać aby umieszczona na nich została następująca klauzula:

> Zgodnie z art. 13 Ogólnego Rozporządzenia o Ochronie Danych dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016) informujemy, iż:
>
> 1. Administratorem danych osobowych jest *[podać nazwę i adres urzędu lub jednostki pomocniczej]*
>
> 2. Kontakt z Inspektorem Ochrony Danych możliwy jest pod adresem: ..... lub tel. .....

3. Dane osobowe przetwarzane są w ramach obowiązków zdefiniowanych w przepisach prawa - na podstawie Art. 6 ust. 1 lit. c) Ogólnego Rozporządzenia o Ochronie Danych z dnia 27 kwietnia 2016 r.

4. Odbiorcami danych osobowych będą wyłącznie podmioty uprawnione do uzyskania danych osobowych na podstawie przepisów prawa

5. Dane osobowe przetwarzane będą wyłącznie do chwili ustania celu ich przetwarzania wynikającego z przepisów prawa

6. Posiadają Państwo prawo do żądania od administratora dostępu do danych osobowych, prawo do ich sprostowania, usunięcia lub ograniczenia przetwarzania, prawo do cofnięcia zgody na przetwarzanie danych oraz prawo do przenoszenia danych

7. Przysługuje Państwu prawo wniesienia skargi do organu nadzorczego

8. Podanie danych osobowych w zakresie wykraczającym poza przepisy prawa jest dobrowolne

2) W sytuacji, gdy przetwarzanie danych osobowych nie wynika z przepisów prawa nakładających na ADO taki obowiązek lub uprawnienie konieczne jest zapytanie o zgodę na przetwarzanie danych i umieszczenie klauzuli wg poniższego wzoru:

Wyrażam zgodę na przetwarzanie danych osobowych w celu .....

Zgodnie z art. 13 Ogólnego Rozporządzenia o Ochronie Danych z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016) informujemy, iż:

1. Administratorem danych osobowych jest *[podać nazwę i adres urzędu lub jednostki pomocniczej]*

2. Kontakt z Inspektorem Ochrony Danych możliwy jest pod adresem: ..... lub tel. .....

3. Dane osobowe przetwarzane są na podstawie zgody (Art. 6 ust. 1 lit. a) Ogólnego Rozporządzenia o Ochronie Danych z dnia 27 kwietnia 2016 r.

4. Odbiorcami danych osobowych będą wyłącznie podmioty uprawnione do uzyskania danych osobowych na podstawie przepisów prawa

5. Dane osobowe przetwarzane będą przez okres .....

6. Posiadają Państwo prawo do żądania od administratora dostępu do danych osobowych, prawo do ich sprostowania, usunięcia lub ograniczenia przetwarzania, prawo do cofnięcia zgody na przetwarzanie danych oraz prawo do przenoszenia danych

7. Przysługuje Państwu prawo wniesienia skargi do organu nadzorczego

8. Podanie danych osobowych jest dobrowolne, jednakże ich niepodanie może uniemożliwić obsługę zgłaszanej sprawy.

3) Jeżeli umieszczenie pełnej treści klauzuli informacyjnej nie jest możliwe na przyjmowanym formularzu (np. z przyczyn technicznych) należy zadbać aby została ona umieszczona w widocznym miejscu w punkcie przyjmowania dokumentów.

REALIZACJA PRAW OSÓB, KTÓRYCH DANE DOTYCZĄ

1) Wszelkie żądania skorzystania z praw przysługujących osobom, których dane dotyczą (np. udostępnienie, przeniesienie, usunięcie, aktualizacja, cofnięcie zgody, zgłoszenie sprzeciwu wobec przetwarzania) wymagają weryfikacji tożsamości osoby, która zgłasza żądanie.

2) W przypadkach budzących wątpliwość co do zasadności żądania konieczna jest konsultacja z Inspektorem Ochrony Danych.

3) Zgłaszane żądanie wynikające z praw osób, których dane dotyczą muszą być obsłużone bez zbędnej zwłoki w terminie nie przekraczającym 30 dni.

POWIERZENIE I UDOSTĘPNIENIE DANYCH OSOBOWYCH

1) Przez powierzenie rozumie się zlecenie zewnętrznemu podmiotowi operacji przetwarzania danych w imieniu Administratora Danych Osobowych w określonym celu i zakresie i wyłącznie na wyraźne polecenie ADO.

2) Przez udostępnienie rozumie się przekazanie danych osobowych zewnętrznemu podmiotowi w celach niezwiązanych z działalnością Administratora Danych Osobowych. Jest ono dopuszczalne wyłącznie na podstawie przepisów obowiązującego prawa.

3) Zarówno powierzenie, jak i udostępnienie danych wymaga każdorazowej konsultacji i wyraźnej zgody Inspektora Ochrony Danych oraz przygotowania odpowiedniej umowy.

4) Inspektor Ochrony Danych odnotowuje informacje o udostępnieniu lub powierzeniu zbioru danych osobowych w prowadzonym przez siebie Rejestrze Czynności Przetwarzania.

ZAŁĄCZNIK 3. PBI - INSTRUKCJA ZARZĄDZANIA INCYDENTAMI BEZPIECZEŃSTWA I PRZECIWDZIAŁANIA ICH WYSTĘPOWANIU

Niniejsza instrukcja definiuje podział zadań i obowiązków koniecznych do efektywnego zarządzania incydentami bezpieczeństwa zgłaszanymi przez pracowników urzędu oraz jednostek pomocniczych. Ma też na celu zapobieganie powtarzającym się incydentom bezpieczeństwa oraz ciągłe podnoszenie świadomości pracowników na temat nowych zagrożeń i sposobów ich unikania. Za nadzór nad realizacją zapisów niniejszej instrukcji odpowiedzialni są Inspektor Ochrony Danych oraz Administrator Systemów Informatycznych.

ROLA INSPEKTORA OCHRONY DANYCH

Do zadań IOD w procesie zarządzania incydentami bezpieczeństwa należy:

a) prowadzenie działań informacyjnych mających na celu przypominanie pracownikom o obowiązkach i ograniczeniach wynikających z Polityki Bezpieczeństwa Informacji i Instrukcji Ochrony Danych Osobowych
b) powiadamianie pracowników urzędu o zmianach zachodzących w treści dokumentów wchodzących w skład Polityki Bezpieczeństwa Informacji
c) szkolenie pracowników urzędu z zakresu ochrony danych osobowych
d) czuwanie nad całościowym procesem obsługi incydentów bezpieczeństwa, przeciwdziałania ich występowaniu i podnoszenia świadomości zagrożeń
e) ocena incydentów związanych z naruszeniem ochrony danych osobowych pod kątem ich wpływu na prawa i wolności osób, których dane dotyczą
f) zgłaszanie z udziałem ADO przypadków naruszenia bezpieczeństwa danych osobowych w ciągu 72 godzin od chwili ich stwierdzenia do Urzędu Ochrony Danych Osobowych
g) informowanie ADO o konieczności powiadomienia osób, których danych dotyczył incydent w przypadku gdy może on skutkować naruszeniem ich praw lub wolności

ROLA ADMINISTRATORA SYSTEMÓW INFORMATYCZNYCH

Do zadań ASI w procesie zarządzania incydentami bezpieczeństwa należy:

a) ustanowienie zasad i miejsca zgłaszania incydentów bezpieczeństwa i poinformowanie o nich wszystkich pracowników
b) ustanowienie rejestru, w którym przechowywane będą zgłoszenia incydentów bezpieczeństwa
c) czuwanie nad prawidłowością przebiegu procesu obsługi incydentów bezpieczeństwa
d) samodzielna obsługa oraz współpraca z Inspektorem Ochrony Danych w celu obsługi incydentów bezpieczeństwa dotyczących przetwarzania danych osobowych
e) powiadamianie ADO o występowaniu incydentów bezpieczeństwa, których nie udało się skutecznie obsłużyć, a które zagrażają poważnymi konsekwencjami
f) opracowywanie rozwiązań mogących ograniczyć występowanie znanych incydentów bezpieczeństwa
g) pomoc pracownikom w identyfikacji incydentów bezpieczeństwa i przypominanie o konieczności i sposobie ich zgłaszania
h) Niezwłoczne informowanie Inspektora Ochrony Danych o incydentach związanych z przetwarzaniem danych osobowych
i) śledzenie informacji o nowych wektorach ataków i zagrożeniach związanych z socjotechnikami, dla których celem mogą stać się pracownicy
j) informowanie pracowników urzędu o nowych zagrożeniach i metodach ich identyfikacji poprzez dostarczanie materiałów informacyjnych lub prowadzenie okresowych szkoleń

ZAŁĄCZNIK 4. PBI - ZALECENIA I PROCEDURY POSTĘPOWANIA DLA PRACOWNIKÓW ODPOWIEDZIALNYCH ZA OBSŁUGĘ INFORMATYCZNĄ

Poniższe zalecenia i procedury określają obowiązujące zasady postępowania, którymi powinny się kierować osoby odpowiedzialne za utrzymanie systemów teleinformatycznych oraz systemów zabezpieczenia fizycznego. Konieczność stosowania poniższych zaleceń wynika bezpośrednio z zapisów prawa związanych z ochroną danych osobowych, ochroną informacji niejawnych oraz rozporządzeniem o Krajowych Ramach Interoperacyjności, a także dobrych praktyk bezpieczeństwa.

ZALECENIA DOTYCZĄCE ADMINISTRACJI SYSTEMAMI

Instalacja aktualizacji systemów operacyjnych i aplikacji
Wszelkie aktualizacje systemu operacyjnego i używanych aplikacji związane z bezpieczeństwem lub poprawkami dotyczącymi stabilności pracy powinny być instalowane natychmiast po ich wydaniu przez producenta. Proces taki powinien być zautomatyzowany przy użyciu odgórnej polityki GPO lub odpowiedniej konfiguracji stacji roboczych. Jeżeli zalecenie to koliduje z działaniem krytycznych systemów produkcyjnych, aktualizacje powinny być wprowadzane ręcznie, kiedy tylko pojawi się taka możliwość.
Szyfrowanie kopii zapasowych i archiwalnych przechowywanych na zewnątrz
Wszelkie dane przechowywane przez urząd i jednostki pomocnicze na zewnątrz powinny być zaszyfrowane, aby uniemożliwić dostęp do nich osobom nieupoważnionym, a w przypadku ich kradzieży uniemożliwić ich odczyt.
Ochrona kopii zapasowych
Kopie zapasowe zawierające konfiguracje systemów oraz przetwarzane dane powinny być przechowywane w bezpiecznym miejscu o ograniczonym dostępie.
Programy antywirusowe
Każdy system komputerowy powinien posiadać zainstalowane i aktywowane bieżące wersje programów antywirusowych. Zalecane jest aby konfiguracja tych programów zabezpieczona była przy pomocy hasła i wymuszała jak najczęstsze pobieranie sygnatur.
Informacja o stosowanych systemach
Administratorzy systemów teleinformatycznych nie mogą ujawniać jakichkolwiek informacji związanych ze stosowanymi przez urząd i jednostki pomocnicze rozwiązaniami, systemami lub urządzeniami bez pozytywnej weryfikacji osoby występującej z wnioskiem o udzielenie powyższych informacji.
Media elektroniczne
Wszelkie media elektroniczne, które zawierają informacje nie przeznaczone dla ogółu, powinny być fizycznie zamykane w bezpiecznym miejscu. Dotyczy to też nośników instalacyjnych oraz licencji wykorzystywanego w urzędzie i jednostkach pomocniczych oprogramowania.
Dezaktywacja portów urządzeń sieciowych
Urządzenia sieciowe powinny być skonfigurowane tak, aby poszczególne ich porty nie będące w użyciu przez komputery pracowników były nieaktywne i uniemożliwiały podłączanie nieautoryzowanych komputerów lub innych urządzeń.
Dostęp dla gości
Wszelkie udostępnione dla ogółu punkty dostępu do sieci ethernet (również punkty dostępu bezprzewodowego) muszą łączyć się jedynie z wydzielonym segmentem sieci, uniemożliwiając dostęp do sieci wewnętrznej. Z punktów takich możliwy powinien być dostęp jedynie do sieci

Internet i jedynie do powszechnych usług typu e-mail, www, DNS. W miarę możliwości zalecane jest wdrożenie rozwiązań pozwalających na ewidencjonowanie danych dotyczących osób korzystających z dostępu dla gości i czasu, w którym ten dostęp był im przyznawany.
Dostęp bezprzewodowy
Wszyscy użytkownicy, którzy korzystają z bezprzewodowego dostępu do sieci lokalnej powinni korzystać z mechanizmów zabezpieczeń minimum WPA2. Zalecaną formą zabezpieczenia jest WPA2-Enterprise w połączeniu z certyfikatami lub serwerem uwierzytelniającym np. radius.
Okresowy przegląd konfiguracji
Minimum raz w roku, lub przy okazji każdej znaczącej modernizacji infrastruktury administratorzy systemów teleinformatycznych powinni dokonać przeglądu konfiguracji mającego na celu stwierdzenie jej aktualności. Przegląd powinien uwzględniać m.in. ocenę stosowanych mechanizmów bezpieczeństwa i aktualność kont użytkowników.
Zbieranie i analiza logów systemowych
Administratorzy systemów teleinformatycznych powinni zadbać o mechanizmy pozwalające na gromadzenie i bezpieczne przechowywanie (najlepiej centralne) logów systemowych pochodzących z wszystkich elementów infrastruktury sklasyfikowanych jako krytyczne (punkt 2.1 PBI). Powinni również dokonywać regularnego przeglądu tych logów lub, w miarę możliwości, wdrożyć rozwiązania pozwalające na ich automatyczną analizę.
Monitorowanie dostępności i bezpieczeństwa
Administratorzy systemów teleinformatycznych powinni wdrożyć rozwiązania pozwalające na monitorowanie dostępności i bezpieczeństwa zasobów sieciowych i systemowych sklasyfikowanych jako krytyczne lub ważne (punkt 2.1 PBI). Do rozwiązań tego typu zalicza się systemy typu HIDS, IDS, IPS oraz systemy monitoringu sieci bazujące na protokołach SNMP lub NetFlow.
Backup i archiwizacja
Administratorzy systemów teleinformatycznych powinni sprawować nadzór nad regularnym wykonywaniem kopi bezpieczeństwa systemów objętych wysokim lub krytycznym poziomem ochrony (punkt 2.1 PBI). Powinni również podejmować działania polegające na upewnianiu się, że tworzone kopie bezpieczeństwa dają się odtworzyć a zawarte w nich dane pozwalają na odtworzenie systemów objętych backupem. Ponadto przynajmniej jedna aktualna kopia bezpieczeństwa powinna być przechowywana poza miejscem pracy systemów, w formie offline (uniemożliwiającej jej skasowanie w wyniku pomyłki lub działania intruzów).

ZALECENIA DOTYCZĄCE NADAWANIA, MODYFIKOWANIA I ODBIERANIA UPRAWNIEŃ

Zmiana przywilejów dostępu
Wszelkie prośby o zmianę praw dostępu użytkownika muszą być zatwierdzone pisemnie przez przełożonego danej osoby na formularzu wg wzoru „**W3 - nadanie uprawnień**". Po dokonaniu zmiany należy przy pomocy poczty e-mail przesłać potwierdzenie do przełożonego, który o nią występował.
Tworzenie nowych kont
Prośba o utworzenie nowego konta dla pracownika, wykonawcy zlecenia lub innej upoważnionej osoby musi mieć formę pisemną wg wzoru „**W3 - nadanie uprawnień**" i być podpisana przez przełożonego danej osoby lub osobę zlecającą jej pracę. Po utworzeniu nowego konta należy o tym fakcie powiadomić osobę wnioskującą o jego założenie za pomocą poczty e-mail.
Wyłączanie kont nieaktywnych
Wszelkie konta dostępowe do systemów teleinformatycznych powinny podlegać regularnym,

okresowym przeglądom w celu identyfikacji użytkowników zakładanych tymczasowo lub zwolnionych z pracy, których konta pozostają aktywne.
Blokowanie kont po kilku próbach dostępu
Systemy teleinformatyczne powinny być skonfigurowane w sposób taki, aby automatycznie blokowały konta użytkowników, którzy 5-krotnie z rzędu podali niepoprawne hasło w procesie logowania. Konto zablokowane z powodu kilkukrotnej próby zalogowania się z niepoprawnym hasłem może zostać automatycznie odblokowane po upływie min. 30 minut.
Konta dla gości
Konta dla gości powinny zostać zlikwidowane we wszystkich systemach komputerowych i urządzeniach sieciowych, poza wydzielonymi punktami, z których możliwy jest dostęp wyłącznie do sieci Internet. Osoba nie będąca pracownikiem i nie posiadająca imiennego konta użytkownika nie powinna mieć możliwości dostępu do jakichkolwiek zasobów systemu teleinformatycznego.

ZALECENIA DOTYCZĄCE DOSTĘPU ZDALNEGO

Nadawanie zdalnego dostępu do zasobów sieci (VPN)
Zabronione jest ujawianie szczegółów lub instrukcji dotyczących zdalnego dostępu, w tym adresów punktów dostępu do sieci oraz danych logowania, jeżeli wnioskujący o taki dostęp nie został: ▪ zweryfikowany przez swojego przełożonego jako pracownik uprawniony do otrzymania takiej informacji przy pomocy odpowiedniego oświadczenia wg wzoru „**W4 - zdalny dostęp dla pracownika**" ▪ zweryfikowany przez kierownictwo jako zewnętrzny wykonawca określonych prac uprawniony do łączenia się z siecią w określonym przedziale przy pomocy oświadczenie wg wzoru „**W5 - zdalny dostęp dla osoby z zewnątrz**" Po pozytywnej weryfikacji i nadaniu uprawnień do zdalnego dostępu należy fakt ten potwierdzić przy pomocy poczty e-mail przełożonemu osoby, która składała wniosek.
Zdalny dostęp do komputerów
Zdalny dostęp do komputerów przy pomocy usług typu Team Viewer lub Pulpit Zdalny nie powinien być stosowany jako stałe rozwiązanie. Dopuszczalne jest jedynie krótkotrwałe udostępnianie powyższych usług na potrzeby wykonania jednorazowych prac. Prośba o udzielenie takiego dostępu musi być wystosowana przez przełożonego danego pracownika, a jej wykonanie potwierdzone przez administratora systemu za pomocą poczty elektronicznej. Ze względu na brak odpowiednich mechanizmów kryptograficznych zabrania się wykorzystywania do dostępu zdalnego oprogramowania bazującego na protokole VNC, chyba że zadba się o dodatkową warstwę szyfrującą np. w postaci tunelu ssh.
Zdalny dostęp do komputera dla podmiotów zewnętrznych
W przypadku wystąpienia konieczności nadania dostępu zdalnego podmiotom zewnętrznym (np. przedstawicielom producenta używanego w organizacji oprogramowania w celu realizacji obsługi serwisowej) należy zadbać o to, by konto udostępniane do tego celu było każdorazowo blokowane po zakończeniu prac. Jego odblokowanie powinno następować tylko po stwierdzeniu konieczności przeprowadzenia obsługi serwisowej.

ZALECENIA DOTYCZĄCE HASEŁ

Wymagana siła haseł
Wszystkie konta administracyjne do systemów teleinformatycznych muszą posiadać hasło

odpowiadające poniższym regułom:

- hasło nie może bazować na jakimkolwiek słowie, imieniu lub nazwie występującej w dowolnym języku (również jeżeli słowo to będzie zmodyfikowane przez dodanie członu liczbowego lub stosowanie dużych i małych liter)
- hasło nie może bazować na danych możliwych do powiązania z osobą (np. data urodzenia, imiona dzieci i małżonków, numer rejestracyjny pojazdu, itp.)
- hasło musi zawierać minimum 3 z czterech grup znaków: małe litery, wielkie litery, cyfry, znaki specjalne i długość min. 8 znaków lub długość co najmniej 11 znaków jeżeli nie podlega innym wymogom dotyczącym siły hasła

W miarę możliwości technicznych powyższe wymagania należy wymusić również w stosunku do haseł użytkowników.

Zmiana haseł

Hasło na koncie użytkownika może być zmienione przez administratora tylko na prośbę właściciela konta, lub pisemny wniosek jego przełożonego. Administrator, do którego kierowana jest prośba o zmianę hasła powinien się upewnić, czy wnioskodawca jest tym, za kogo się podaje.

Rozpowszechnianie nowych haseł

Nowe hasła muszą być traktowane jako informacje poufne i rozpowszechniane bezpiecznymi metodami - w przypadku pracowników lokalnych przekazywane osobiście, w przypadku pracowników zdalnych listem poleconym lub przesyłką kurierską, do rąk własnych, z uwzględnieniem koperty uniemożliwiającej podgląd zawartości. W przypadku przekazywania haseł na odległość zabrania się przesyłania tym samym kanałem, razem z hasłem informacji o nazwie logowania. Nie zaleca się przekazywania haseł za pomocą SMS-ów i komunikatorów internetowych, ze względu na możliwość przechwycenia takiej transmisji oraz funkcje urządzeń mobilnych pozwalające na archiwizowanie przesyłanych wiadomości na serwerach operatorów.

Hasła domyślne

Wszelkie urządzenia sieciowe lub elementy oprogramowania, które po dostarczeniu przez producenta posiadają hasła ustawione na wartość domyślną, muszą przejść procedurę zmiany hasła.

Periodyczna zmiana haseł na kontach uprzywilejowanych

Hasła na kontach użytkowników uprzywilejowanych służących do zarządzania infrastrukturą teleinformatyczną powinny być zmieniane minimum raz na rok.

Periodyczna zmiana haseł na kontach użytkowników

System informatyczny powinien być skonfigurowany w taki sposób, aby wymuszać zmianę hasła na kontach użytkowników przynajmniej raz na 180 dni, chyba że użytkownik ten nie bierze udziału w procesie przetwarzania danych osobowych, wówczas dopuszczalny jest okres 1 roku.

Ustawianie hasła na nowym koncie

Nowe konta użytkowników powinny być zakładane z hasłem jednorazowym lub hasłem o bardzo krótkim okresie ważności. Po pierwszym wejściu na takie konto użytkownik powinien dokonać zmiany hasła.

Ujawnianie haseł

Administratorzy systemów teleinformatycznych nie mogą pod żadnym pozorem ujawniać haseł dostępowych do urządzeń, serwerów i systemów, którymi administrują osobom innym, niż najbliżsi współpracownicy, którzy realizują te same zadania.

ZALECENIA DOTYCZĄCE WDROŻEŃ NOWYCH SYSTEMÓW

Bezpieczeństwo w fazie projektowania
Wszelkie planowane do wdrożenia systemy teleinformatyczne powinny już na etapie projektowania i specyfikowania wymogów funkcjonalnych być zaopatrzone w funkcje zapewniające wysoki poziom bezpieczeństwa, w tym poufności, dostępności i rozliczalności.
Bezpieczeństwo domyślne
Wszelkie wdrażane systemy teleinformatyczne powinny na etapie uruchamiania zostać skonfigurowane w sposób gwarantujący najwyższy poziom bezpieczeństwa, w tym poufności, dostępności i rozliczalności. Należy ze szczególnym uwzględnieniem zadbać o wyłączenie domyślnych kont użytkowników i zmianę domyślnych haseł producenta oraz dezaktywację usług, których obecność w systemie nie jest wymagana.

ZALECENIA DOTYCZĄCE ZABEZPIECZEŃ DANYCH OSOBOWYCH

Pseudonimizacja danych

W sytuacji, gdy czynność przetwarzania danych powierzana jest podmiotowi zewnętrznemu lub wiąże się z ryzykiem naruszenia praw i wolności osób, których dane są przetwarzane należy postępować wg następującej procedury:

1. Ustalić, czy czynność przetwarzania wymaga by przetwarzaniu podlegały również dane umożliwiające identyfikację osoby (dane osobowe).
2. Jeżeli przetwarzanie może się odbywać z pominięciem danych osobowych należy dokonać czasowego oddzielenia danych podlegających przetwarzaniu od danych umożliwiających identyfikację osób, których dotyczą.
3. Oddzielenie powinno się odbyć poprzez przypisanie wspólnego identyfikatora danym osobowym i danym poddawanym czynności przetwarzania, a następnie wydzieleniu i zachowaniu ich w oddzielnych zbiorach.
4. Wydzielone w ten sposób zbiory nie mogą być przechowywane w tym samym miejscu
5. Należy zachować szczególną uwagę, aby możliwe było późniejsze połączenie obu zbiorów przy użyciu wspólnego identyfikatora.

Szyfrowanie danych

W każdym przypadku, gdy dane osobowe muszą być wyniesione poza miejsce pracy należy zastosować zabezpieczenie kryptograficzne nośnika lub komputera, na którym dane będą wynoszone. Szyfrowanie powinno się odbyć wg następujących zasad:

1. Do szyfrowania dysków w komputerach zaleca się używać funkcję BitLocker systemu Windows
2. W przypadku gdy nie jest to możliwe zastosować można inne znane i powszechnie używane rozwiązania szyfrujące na poziomie dysku lub partycji zawierającej dane osobowe
3. Do szyfrowania zaleca się stosować algorytm AES256
4. W przypadku konieczności zaszyfrowania pojedynczego pliku lub grupy plików, np. w celu wysłania ich pocztą e-mail zaleca się zabezpieczenie ich przy użyciu oprogramowania 7zip
5. Hasła użyte do szyfrowania należy objąć szczególną ochroną przed ich ujawnieniem lub zgubieniem (np. wykorzystując menedżer haseł KeePassX i zapisując jedną kopię jego bazy danych na dysku podlegającym procedurze backupu.

ZAŁĄCZNIK 5. PBI - PLAN CIĄGŁOŚCI DZIAŁANIA

Celem niniejszego planu jest przygotowanie procedur i zaleceń mogących posłużyć jako instrukcje w chwili wystąpienia nieprzewidzianych awarii lub katastrof powodujących niedostępność krytycznych dla urzędu i jednostek pomocniczych zasobów, danych lub personelu. Ze względu na swój charakter Plan Ciągłości Działania powinien być przechowywany w sposób gwarantujący dostęp do niego niezależnie od mogących wystąpić niekorzystnych okoliczności. Aby uniknąć sytuacji, w której dostęp do Planu Ciągłości Działania jest niemożliwy np. w wyniku awarii serwera, braku Internetu lub pożaru pomieszczenia należy zadbać o to, aby kopie poniższych procedur przechowywane były w kilku niezależnych miejscach na różnych rodzajach nośników, np. w formie wydrukowanej u kierowników jednostek organizacyjnych plus w formie elektronicznej na serwerze plików i komputerach kierowników oraz pracowników działu IT.

PRZECIWDZIAŁANIE NIEDOSTĘPNOŚCI PERSONELU

Kierownicy jednostek organizacyjnych zobligowani są do takiego zarządzania zasobami osobowymi, które umożliwi zastępowalność kompetencji na wypadek nieobecności dowolnego z pracowników. Należy unikać sytuacji, w której określone kompetencje posiada tylko jeden pracownik w dziale. Jeżeli do realizacji zadań konieczny jest dostęp do określonych zasobów (np. dokumentów, systemów, pomieszczeń) należy zadbać o to, aby dostęp ten posiadało więcej osób z danej jednostki organizacyjnej. Należy również unikać sytuacji, w której realizacja zadań zależna jest od wydania decyzji, do której podjęcia uprawniona jest tylko jedna osoba.

PRZECIWDZIAŁANIE NIEDOSTĘPNOŚCI USŁUG

Jeżeli do realizacji zadań w urzędzie i jednostkach pomocniczych konieczne jest korzystanie z usług dostarczanych przez firmy zewnętrzne należy zadbać o to, aby świadczone one były w sposób ciągły. Osoby odpowiedzialne za obsługę teleinformatyczną powinny zadbać m.in. o odnawianie niezbędnych umów serwisowych i licencyjnych związanych z użytkowanym sprzętem i oprogramowaniem.
Osoby odpowiedzialne za realizację płatności powinny zadbać o to, aby płatności za usługi dostarczane przez zewnętrznych dostawców były realizowane w terminie. Ich brak może bowiem spowodować wyłączenie krytycznej usługi jak np. dostęp do Internetu, poczty e-mail, telefonów.

PRZECIWDZIAŁANIE NIEDOSTĘPNOŚCI ZASOBÓW

Osoby odpowiedzialne za obsługę informatyczną oraz utrzymanie krytycznych usług zobligowane są do opracowywania procedur odtworzeniowych umożliwiających podjęcie działań naprawczych na wypadek awarii dowolnego z zasobów niezbędnych do realizacji zadań urzędu. Do zasobów tych należą wszystkie systemy informatyczne wchodzące w skład aktywów sklasyfikowanych w punkcie 2.1 PBI jako krytyczne i ważne. Procedury naprawcze powinny zostać również zdefiniowane na wypadek braku dostępności któregoś z poniższych zasobów:

- serwery
- sieć LAN
- poczta e-mail
- Internet
- łącza WAN/VPN
- drukarki
- telefony/faksy
- zasilanie

Procedury odtworzeniowe powinny zawierać m.in. instrukcje przywracania krytycznych zasobów i systemów z kopii zapasowych. Dla każdego z krytycznych elementów infrastruktury powinny zostać przygotowane plany zastąpienia go sprzętem zastępczym i informacje o tym, skąd taki sprzęt może zostać pozyskany. W przypadku braku własnych zasobów należy wskazać możliwość skorzystania z usług zewnętrznych dostawców i wskazać kontakty, przy użyciu których usługi te mogą zostać aktywowane. Jeżeli dla któregokolwiek z elementów krytycznych infrastruktury brak jest sprzętu zastępczego, należy fakt ten zgłosić kierownictwu. Opracowane procedury przywracania zasobów powinny zostać dołączone do niniejszego dokumentu i być stale aktualizowane przez ich autorów, a okresowo również testowane (nie rzadziej niż raz w roku).

ROLA INSPEKTORA OCHRONY DANYCH

Ze względu na szeroki zakres zagadnienia i rozproszoną na całą strukturę organizacyjną odpowiedzialność zaleca się aby Inspektor Ochrony Danych pełnił rolę przewodnią w procesie kompletowania i utrzymywania dokumentacji związanej z Planem Ciągłości Działania. Zadaniem IOD jest dopilnowanie aby osoby odpowiedzialne za utrzymanie krytycznych usług przygotowały dla nich procedury odtworzeniowe na wypadek awarii. IOD powinien też zadbać o to aby procedury te były stale aktualizowane stosownie do zmieniającego się otoczenia oraz okresowo, nie rzadziej niż raz w roku testowane. IOD powinien też upewnić się, że procedury odtworzeniowe są dostępne niezależnie od rodzaju i skali awarii. Razem z procedurami odtworzeniowymi zaleca się również przechowywać aktualną listę kontaktów do osób decyzyjnych oraz pracowników biorących udział w przywracaniu usług.

PROCEDURY ODTWORZENIOWE

Przykład procedury odtworzeniowej, który można stosować jako wzorcowy zawarty został poniżej. Należy zwrócić uwagę na fakt, iż w przypadku zawarcia w procedurze punktów wymagających posiadania odpowiednich narzędzi, np. nośników instalacyjnych, kluczy licencyjnych, konfiguracji, backupu danych, haseł administracyjnych itp. narzędzia te muszą być dostępne w każdej sytuacji. Należy przewidzieć możliwe do wystąpienia okoliczności, które mogą spowodować niedostępność określonych zasobów. Przykładowo: w procedurze przywracania do pracy uszkodzonego serwera nie można bazować na pakietach instalacyjnych lub kluczach, które przechowywane są wyłącznie na tym serwerze. Należy zadbać o to, aby wszystkie wymagane do przywrócenia danej usługi elementy były dostępne niezależnie od stanu serwerów, sieci, łączy, dostępności do określonych pomieszczeń czy możliwości skontaktowania się z konkretną osobą.

Procedura przywracania zasobu	
Nazwa zasobu: *serwer plików*	**Lokalizacja:** *serwerownia*
Sprzęt zastępczy: *stary serwer z zasobów własnych*	**Lokalizacja awaryjna:** *punkt dystrybucyjny sieci*
Narzędzia niezbędne do przeprowadzenia procedury: 1. *Nośnik instalacyjny Windows Server 2008R2* 2. *Klucz licencyjny Windows Server 2008R2* 3. *Sterowniki producenta serwera (HP ProLiant)* 4. *Nośnik instalacyjny oprogramowania do backupu* 5. *Nośnik z backupem danych serwera plików* 6. *Hasło administratora domeny AD*	Miejsce przechowywania narzędzi: 1. *Szafa pancerna w dziale IT* 2. *Szafa pancerna w dziale IT* 3. *Strona internetowa producenta serwera* 4. *Strona internetowa producenta oprogramowania* 5. *Taśma magnetyczna w serwerowni* 6. *Koperta w szafie pancernej w dziale IT*

Dane konfiguracyjne zasobu

Adres IP: *192.168.0.2/24*
Nazwa systemowa: *„file-serwer01"*
Nazwa udziału sieciowego: *„wspolny"*
Nazwa domeny: *domena.local*

Prawa zapisu i odczytu do udziału przysługują grupom:
księgowość, dział IT, kadry, kierownicy

Prawa odczytu udziału przysługują grupom: *pracownicy, stażyści*

Brak uprawnień do udziału dla pozostałych grup.

Czynności do wykonania

1. *Instalacja systemu Windows Server 2008R2 z nośnika instalacyjnego*
2. *Pobranie i dogranie sterowników do komponentów serwera ze strony producenta HP*
3. *Aktywacja systemu i konfiguracja (adres IP, nazwa systemowa, usługa serwera plików)*
4. *Pobranie i instalacja oprogramowania do backupu „DataProtector"*
5. *Odtworzenie danych serwera plików z nośnika backupowego*
6. *Konfiguracja backupu dla serwera tymczasowego*
7. *Konfiguracja praw dostępu dla użytkowników domeny AD*
8. *Testy dostępności usługi dla poszczególnych grup użytkowników*

ZAŁĄCZNIK 6. PBI - ZALECENIA I PROCEDURY POSTĘPOWANIA PRZEZNACZONE DLA PRACOWNIKÓW ODPOWIEDZIALNYCH ZA OBSŁUGĘ KADROWĄ

Poniższe zalecenia i procedury określają obowiązujące zasady postępowania, którymi powinny się kierować osoby odpowiedzialne za politykę kadrową urzędu i jednostek pomocniczych. Na zatrudnionych do obsługi kadrowej osobach ciąży szczególny obowiązek ochrony pracowników przed osobami próbującymi uzyskać ich dane osobowe. Specjaliści od zarządzania kadrami odpowiadają również za ochronę przed nieautoryzowanym dostępem ze strony byłych pracowników.

Proces rekrutacji
Jeżeli zbierane w procesie rekrutacji dane osobowe przekraczają zakres danych wynikający z kodeksu pracy (imię, nazwisko, adres, imiona rodziców, przebieg nauki i zatrudnienia), wówczas ich przetwarzanie możliwe jest wyłącznie na podstawie zgody kandydata. Jeżeli zebrane w procesie rekrutacji dane osobowe planuje się wykorzystać w przyszłości, kandydat powinien na to wyrazić zgodę. W innym przypadku dane powinny być usunięte po zakończeniu procesu rekrutacji. Przykład prawidłowego pytania o zgodę na przetwarzanie danych w procesie rekrutacji i po jego zakończeniu zawarty został poniżej. Wszelkie dokumenty (CV, listy motywacyjne itp., które kandydaci do pracy pozostawiają bez poniższej klauzuli powinny być im zwrócone lub zniszczone): *Wyrażam zgodę na przetwarzanie moich danych osobowych do celów bieżącej i przyszłych rekrutacji zgodnie z przepisami Ogólnego Rozporządzenia o Ochronie Danych z dnia 27 kwietnia 2016r.*
Zatrudnienie nowego pracownika
W przypadku zatrudniania nowego pracownika osoba odpowiedzialna za obsługę kadrową wydaje mu kartę nadania uprawnień wg wzoru „**W3 - nadanie uprawnień**". Na podstawie tej karty pracownicy odpowiedzialni za obsługę informatyczną nadają nowemu pracownikowi odpowiednie uprawnienia w systemach. Karta ta po nadaniu uprawnień wraca do kadr i musi być przechowywana z aktami pracownika.
Zakończenie umowy o pracę lub inną formę współpracy
Kiedy umowa o pracę lub inną formę współpracy pomiędzy pracownikiem a urzędem lub jednostką pomocniczą ustaje, osoba odpowiedzialna za obsługę kadrową w porozumieniu z bezpośrednim przełożonym powinna niezwłocznie: ▪ skutecznie (np. za potwierdzeniem mailowym) poinformować o tym fakcie osoby odpowiedzialne za obsługę informatyczną i dopilnować aby na karcie nadania uprawnień wypełnionej w chwili zatrudniania pracownika administratorzy systemów informatycznych potwierdzili fakt odebrania jej uprawnień do wszystkich systemów. ▪ jeżeli zachodzi taka konieczność poinformować personel pilnujący wejść do pomieszczeń o zakazie dostępu dla byłego pracownika ▪ rozesłać do wszystkich pracowników za pomocą poczty elektronicznej informację o zakończenia stosunku pracy danego pracownika
Poufne informacje wykorzystywane w procesie rekrutacyjnym
Ogłoszenia i inne formy publicznej rekrutacji kandydatów na wolne miejsca pracy powinny być skonstruowane w taki sposób, aby w miarę możliwości unikać w stawianych wymaganiach identyfikacji sprzętu komputerowego i oprogramowania używanego przez urząd.

Osobiste dane pracownika
Osoby odpowiedzialne za obsługę kadrową nie mogą ujawniać informacji osobistych dotyczących aktualnie zatrudnionych lub byłych pracowników, osób wykonujących zlecenia, konsultantów czy zatrudnionych tymczasowo, chyba że pracownik wyraził na to pisemną zgodę.

ZAŁĄCZNIK 7. PBI – ZALECENIA I PROCEDURY OBOWIĄZUJĄCE PRZY SPORZĄDZANIU UMÓW

ZALECENIA DO STOSOWANIA W TRAKCIE PRZYGOTOWANIA UMOWY

Poniższe zalecenia i procedury określają obowiązujące zasady postępowania, którymi powinny się kierować osoby odpowiedzialne za powstawanie zapytań ofertowych, przebieg procedur przetargowych oraz wybór dostawców i podpisywanie z nimi umów. W tym celu zalecana jest ścisła współpraca pomiędzy osobami zajmującymi się zamówieniami publicznymi oraz obsługą prawną i przygotowywaniem umów.

Przygotowanie Specyfikacji
Podczas definiowania wymogów dla zamawianych rozwiązań, które należą do grup aktywów objętych wysokim lub krytycznym poziomem ochrony (punkt 2.1 PBI), lub mają na nie bezpośredni wpływ, należy zwrócić szczególną uwagę na zagwarantowanie wysokiego poziomu świadczonych usług oraz wysoką jakość dostarczanych produktów. Poziom usług powinien być zdefiniowany za pomocą konkretnych i mierzalnych parametrów, które będą umożliwiały weryfikację jakości. Przykładem takiego parametru może być dostępność określająca procentowo w jakim zakresie dana usługa jest dostępna dla jej użytkowników w skali roku. Przykładowo do określania dostępności łączy internetowych stosuje się parametr z przedziału 99,5-99,9% oznaczający iż usługa dostępu do Internetu może być niedostępna przez kilka do kilkudziesięciu godzin w ciągu roku.
Przygotowanie Umowy
Równie istotną kwestią jak specyfikacja wymogów jest ich skuteczne egzekwowanie poprzez odpowiednie zapisy w umowach zawieranych z dostawcami. W tym celu wszystkie zapisy dotyczące np. gwarantowanego poziomu usług (umowy SLA) powinny przewidywać kary umowne, które dostawca będzie zobowiązany wypłacić w przypadku niewywiązania się z zapisów umowy. Kary te powinny byc odpowiednio wysokie I adekwatne do ryzyka wiążącego się z niespełnieniem wymogów umowy przez dostawcę. Weryfikacji powinny również podlegać domyślne kary, których wysokość często dostawcy określają sami wg kryteriów im odpowiadających.
Powierzanie danych osobowych
W sytuacji, gdy w ramach zawieranej umowy konieczne jest powierzenie danych osobowych zewnętrznemu podmiotowi należy każdorazowo fakt ten skonsultować z Inspektorem Ochrony Danych i uzyskać od niego wyraźną akceptację. Powierzenie danych osobowych wymaga podpisania odrębnej umowy powierzenia lub zawarcia w innej umowie, ewentualnie aneksie do niej klauzul wymienionych w punkcie kolejnym.

OBOWIĄZKOWE KLAUZULE W UMOWACH POWIERZENIA DANYCH OSOBOWYCH

W przypadku, gdy w ramach podpisywanej umowy podmiot zewnętrzny uzyskuje dostęp do danych osobowych lub w inny sposób bierze udział w ich przetwarzaniu konieczne jest spełnienie przez niego wymogów zdefiniowanych w artykule 28 Ogólnego Rozporządzenia o Ochronie Danych (RODO). Do ich spełnienia podmiot przetwarzający zostaje zobligowany poprzez zawarcie w umowie z nim poniższych klauzul. Wymóg ten jest podyktowany przepisami o ochronie danych osobowych (Artykuł 28 Ogólnego Rozporządzenia o Ochronie Danych z dnia 27 kwietnia 2016 r.):

Powierzenie przetwarzania danych osobowych

Administrator Danych Osobowych (dalej „Administrator") powierza Podmiotowi Przetwarzającemu, w trybie art. 28 ogólnego rozporządzenia o ochronie danych z dnia 27 kwietnia 2016 r. (zwanego w dalszej części „Rozporządzeniem") dane osobowe do przetwarzania wyłącznie na zasadach i w celu określonym w niniejszej Umowie.
Podmiot przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą umową, Rozporządzeniem oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
Podmiot przetwarzający oświadcza, iż stosuje środki bezpieczeństwa spełniające wymogi Rozporządzenia.

Zakres i cel przetwarzania danych

1. Podmiot Przetwarzający będzie przetwarzał, powierzone na podstawie umowy następujące dane osobowe Administratora:
   .....
   .....
2. Powierzone przez Administratora dane osobowe będą przetwarzane przez Podmiot przetwarzający wyłącznie w celu:
   ...
   .....
   .....

Obowiązki podmiotu przetwarzającego

1. Podmiot przetwarzający zobowiązuje się, przy przetwarzaniu powierzonych danych osobowych, do ich zabezpieczenia poprzez stosowanie odpowiednich środków technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanym z przetwarzaniem danych osobowych, o których mowa w art. 32 Rozporządzenia.
2. Podmiot przetwarzający zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych.
3. Podmiot przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji niniejszej umowy.
4. Podmiot przetwarzający zobowiązuje się zapewnić zachowanie w tajemnicy, (o której mowa w art. 28 ust 3 pkt b Rozporządzenia) przetwarzanych danych przez osoby, które upoważnia do przetwarzania danych osobowych w celu realizacji niniejszej umowy, zarówno w trakcie zatrudnienia ich w podmiocie przetwarzającym, jak i po jego ustaniu.
5. Podmiot przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem usuwa / zwraca Administratorowi wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.
6. W miarę możliwości Podmiot przetwarzający pomaga Administratorowi w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą oraz wywiązywania się z obowiązków określonych w art. 32-36 Rozporządzenia.
7. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi minimum w ciągu 36 godzin od chwili stwierdzenia takiego naruszenia.

Prawo kontroli

1. Administrator danych zgodnie z art. 28 ust. 3 pkt h) Rozporządzenia ma prawo kontroli, czy środki zastosowane przez Podmiot Przetwarzający przy

przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia umowy.
2. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora danych.
3. Podmiot przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia.

Dalsze powierzenie danych do przetwarzania

1. Podmiot przetwarzający może powierzyć dane osobowe objęte niniejszą umową do dalszego przetwarzania podwykonawcom jedynie w celu wykonania umowy po uzyskaniu uprzedniej pisemnej zgody Administratora danych.
2. Przekazanie powierzonych danych do państwa trzeciego może nastąpić jedynie na pisemne polecenie Administratora danych chyba, że obowiązek taki nakłada na Podmiot przetwarzający prawo Unii lub prawo państwa członkowskiego, któremu podlega Podmiot przetwarzający. W takim przypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający informuje Administratora danych o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
3. Podwykonawca, winien spełniać te same gwarancje i obowiązki jakie zostały nałożone na Podmiot przetwarzający w niniejszej Umowie.
4. Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora za nie wywiązanie się ze spoczywających na podwykonawcy obowiązków ochrony danych.

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. Podmiot przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora danych o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Podmiot przetwarzający danych osobowych określonych w umowie, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, skierowanych do Podmiotu przetwarzającego, a także o wszelkich planowanych, o ile są wiadome, lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania w Podmiocie przetwarzającym tych danych osobowych, w szczególności prowadzonych przez inspektorów upoważnionych przez Generalnego Inspektora Ochrony Danych Osobowych lub Urząd Ochrony Danych Osobowych. Niniejszy ustęp dotyczy wyłącznie danych osobowych powierzonych przez Administratora danych.

Rozwiązanie umowy

Administrator danych może rozwiązać niniejszą umowę ze skutkiem natychmiastowym gdy Podmiot przetwarzający:
1. pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli nie usunie ich w wyznaczonym terminie;
2. przetwarza dane osobowe w sposób niezgodny z umową;
3. powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody Administratora danych;

Zasady zachowania poufności

1. Podmiot przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Administratora danych i od współpracujących z nim osób oraz danych uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy w formie ustnej, pisemnej lub elektronicznej („dane poufne").
2. Podmiot przetwarzający oświadcza, że w związku ze zobowiązaniem do zachowania w tajemnicy danych poufnych nie będą one wykorzystywane, ujawniane ani udostępniane

bez pisemnej zgody Administratora danych w innym celu niż wykonanie Umowy, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub Umowy.

Postanowienia końcowe

1. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach dla każdej ze stron.
2. W sprawach nieuregulowanych zastosowanie będą miały przepisy Kodeksu cywilnego oraz Rozporządzenia.
3. Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej umowy będzie sąd właściwy Administratora

ZAŁĄCZNIK 8. PBI - REGULAMIN PRACY W SYSTEMIE TELEINFORMATYCZNYM

Niniejszy regulamin zawiera zalecenia związane z bezpieczeństwem systemów informatycznych, komputerów, nośników danych oraz poczty elektronicznej, a także bezpiecznym korzystaniem z sieci Internet. Ich stosowanie jest konieczne w celu zapewnienia wysokiego poziomu bezpieczeństwa i spełnienia wymogów prawnych dotyczących m.in. ochrony danych osobowych.

1. Zabrania się ujawniania informacji o metodach dostępu do systemów teleinformatycznych (w tym nazwy i adresy systemów, sieci wifi, loginy, hasła) innym pracownikom lub osobom z zewnątrz.
2. Wewnętrzne dokumenty przeznaczone do wyrzucenia muszą być zniszczone za pomocą niszczarki do papieru. Wszelkie przeznaczone do wyrzucenia media i nośniki danych typu płyty CD/DVD, przenośne pamięci USB oraz dyski twarde muszą być przekazane do administratora systemów informatycznych w celu trwałego usunięcia danych lub zniszczenia.
3. Zabrania się wprowadzania poleceń do komputera i dokonywania zmian ustawień systemowych na prośbę innej osoby, chyba że osoba ta została zweryfikowana jako pracownik odpowiedzialny za obsługę informatyczną.
4. Zabrania się uruchamiania jakiejkolwiek aplikacji lub programu na prośbę innej osoby, o ile nie została ona zweryfikowana jako pracownik odpowiedzialny za obsługę informatyczną. Dotyczy to zwłaszcza programów przesłanych za pomocą poczty elektronicznej lub wskazanych w formie odnośnika internetowego.
5. Zabrania się pobierania i instalowania oprogramowania na prośbę innych osób, jeżeli nie zostały one zweryfikowane jako pracownicy odpowiedzialni za obsługę informatyczną.
6. Zabrania się instalowania i deinstalowania na własną rękę jakichkolwiek programów, narzędzi i komponentów systemu operacyjnego bez konsultacji z pracownikami odpowiedzialnymi za obsługę informatyczną.
7. Zabrania się przesyłania haseł lub innych informacji dostępowych za pośrednictwem poczty elektronicznej bez ich odpowiedniego zabezpieczenia kryptologicznego.
8. Zabrania się usuwania lub dezaktywowania jakichkolwiek programów antywirusowych, firewalli i innych programów strzegących bezpieczeństwa systemu bez wcześniejszej zgody informatyków.
9. Zabrania się podłączania do komputerów na własną rękę modemów, telefonów komórkowych i innych urządzeń dostępowych typu BlueConnect, iPlus, OrangeGo. Zabronione jest też łączenie się przy pomocy takich urządzeń z Internetem w chwili, gdy komputer użytkownika podłączony jest do sieci urzędu.
10. Zabrania się pobierania, instalowania i używania jakichkolwiek narzędzi stworzonych w celu pokonywania zabezpieczeń systemowych, łamania haseł, dekodowania zaszyfrowanych informacji lub usuwania ograniczeń licencyjnych.
11. Zabrania się ujawniania na grupach dyskusyjnych, forach internetowych, blogach itp. jakichkolwiek szczegółów dotyczących funkcjonowania systemów, w tym informacji na temat wykorzystywanego służbowo sprzętu i oprogramowania oraz informacji kontaktowych innych, niż ogólnodostępne w materiałach zewnętrznych.
12. Zabrania się odczytywania w komputerach mediów i urządzeń służących do przechowywania danych, których pochodzenie nie jest znane. Pozostawione na biurku pracownika lub znalezione płyty CD/DVD lub pamięci przenośne typu pendrive mogą być podrzucone przez intruza i zawierać niebezpieczne oprogramowanie aktywowane automatycznie w momencie ich odczytu.
13. Użytkownik komputera oddalając się na dłużą chwilę od swojego stanowiska pracy zobowiązany jest blokować ekran przy pomocy kombinacji klawiszy WIN+L (klawisz WIN to klawisz z logiem systemu Windows). Zalecane jest także ustawienie wygaszacza ekranu, który uruchamia się automatycznie po 15-minutowym okresie bezczynności, a w chwili wznowienia pracy żąda podania hasła użytkownika.

14. Przy opuszczaniu stanowiska pracy na dłuższy czas, a zwłaszcza po zakończeniu obowiązków służbowych danego dnia użytkownik komputera zobowiązany jest do jego całkowitego wyłączenia.
15. Wszelkie przesyłane pocztą elektroniczną załączniki otrzymywane od nieznanych nadawców powinny być weryfikowane przed otwarciem. Na szczególną ostrożność zasługują też pochodzące od znanych nadawców załączniki w formatach innych niż powszechnie stosowane do zapisu dokumentów, a zwłaszcza pliki o rozszerzeniach typu .exe, .bat, .cab, .msi, .reg, .ini. Załączniki takie mimo iż przesłane z konta zaufanej osoby mogą być efektem działania wirusa.
16. Zabrania się użytkownikom poczty elektronicznej konfigurowania swoich kont pocztowych do automatycznego przekierowywania wiadomości na adres zewnętrzny.
17. Wiadomość pocztowa, która wydaje się pochodzić od osoby zaufanej i zawiera prośbę o udzielenie poufnych informacji lub wykonanie czynności mogących mieć wpływ na bezpieczeństwo systemu informatycznego wymaga dodatkowej formy uwierzytelnienia. Odbiorca takiej wiadomości powinien skontaktować się z jej nadawcą w celu upewnienia się, czy rzeczywiście wysyłał on prośbę. Może też zażądać od wnioskodawcy złożenia prośby w formie pisemnej i opatrzenie jej własnoręcznym podpisem.
18. Zabrania się uczestniczenia w ankietach telefonicznych i internetowych dotyczących, w których podawane są szczegóły na temat miejsca pracy i używanych systemów oraz oprogramowania.
19. Zabrania się pozostawiania w poczcie głosowej innych pracowników wiadomości zawierających informacje o hasłach.
20. Zabrania się ujawniania komukolwiek swojego hasła dostępowego do systemu jak i innych haseł stosowanych do uwierzytelniania się w programach lub systemach.
21. Zabrania się używania na wszelkiego rodzaju serwisach internetowych takich samych lub podobnych haseł jak w systemach komputerowych w miejscu pracy.
22. Zabrania się stosowania tego samego hasła jako zabezpieczenia w dostępie do różnych systemów.
23. Zabrania się definiowania haseł, w których jeden człon pozostaje niezmienny, a drugi zmienia się według przewidywalnego wzorca (np. Anna001, Anna002, Anna003 itd.). Nie powinno się też stosować haseł, w których któryś z członów stanowi imię, nazwę lub numer miesiąca lub inny możliwy do odgadnięcia klucz.
24. Przechowywanie zanotowanych haseł do systemu jest niezalecane. Jeżeli ze względu na dużą złożoność hasła występuje konieczność jego zapisania, to przechowywane ono powinno być przy użyciu odpowiedniego oprogramowania, tzw. menedżera haseł (np. KeePassX). W jego instalacji powinien asystować pracownik działu informatycznego.

Integralną część niniejszego regulaminu stanowią procedury zawarte w „Polityce Bezpieczeństwa Informacji". Podpisując Regulamin pracy w systemie teleinformatycznym pracownik akceptuje ich treść i zobowiązuje się do śledzenia ewentualnych zmian oraz odpowiedniego stosowania się do ich postanowień.

Data i podpis pracownika