Zarządzenie Nr 32/18
Burmistrza Pisza
z dnia 23 maja 2018 r.

w sprawie wprowadzenia w Urzędzie Miejskim w Piszu wewnętrznych uregulowań dotyczących ochrony danych osobowych.

Na podstawie art. 31, 33 ust.1 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2017 r. poz. 1875 z późn.zm.) w związku z Art. 24 ust. 1 i 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia Dyrektywy 95/46 z dnia 27 kwietnia 2016 r.(Dz. Urz. UE L 119 z 04.05.2016) zarządzam co następuje:

§ 1.

Wprowadzam do stosowania w Urzędzie Miejskim w Piszu:

1. Politykę Bezpieczeństwa Ochrony Danych Osobowych w Urzędzie Miejskim w Piszu zwaną dalej „Polityką" stanowiącą Załącznik nr 1 do niniejszego zarządzenia,
2. Instrukcję zarządzania Systemami Informatycznymi – wykaz Zabezpieczeń RODO w Urzędzie Miejskim w Piszu zwaną dalej „Instrukcją" stanowiącą Załącznik nr 2 do niniejszego zarządzenia.

§ 2.

Zobowiązuje się pracowników Urzędu Miejskiego w Piszu do stosowania zasad określonych w Polityce i Instrukcji.

§ 3.

Tracą moc:

1) Zarządzenie Nr 166/04 Burmistrza Pisza z dnia 30 listopada 2004 r. w sprawie ustalenia „Polityki bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Miejskim w Piszu",
2) Zarządzenie Nr 28/12 Burmistrza Pisza z dnia 28 marca 2012 r. w sprawie wprowadzenia w Urzędzie Miejskim w Piszu wewnętrznych uregulowań dotyczących ochrony danych osobowych.

§ 4.

Zarządzenie wchodzi w życie z dniem 25.05.2018 r.

BURMISTRZ
Andrzej Szymborski

r. pr. 26. Jaskuła
22.05.2018 Anna

Załącznik nr 1
do Zarządzenia Nr 82/18
Burmistrza Pisza
2 dnia 23 maja 2018 r.

Polityka Ochrony Danych Osobowych w Urzędzie Miejskim w Piszu

I. WSTĘP

Polityka Ochrony Danych Osobowych w Urzędzie Miejskim w Piszu jest dokumentem opisującym zasady ochrony danych osobowych stosowane przez Administratora w celu spełnienia wymagań Rozporządzenia PE i RE 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) (RODO) i zwana jest w dalszej części Polityką.
Polityka stanowi jeden ze środków organizacyjnych, mających na celu wykazanie, że przetwarzanie danych osobowych odbywa się zgodnie z RODO.

DEFINICJE

Administrator - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.

RODO–rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia Dyrektywy 95/46 z dnia 27 kwietnia 2016 r.(Dz. Urz. UE L 119 z 04.05.2016).

Polityka – rozumie się przez to Politykę Ochrony Danych Osobowych w Urzędzie Miejskim w Piszu.

Urząd – Urząd Miejski w Piszu.

Dane osobowe - to wszelkie informacje związane ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną. Osoba jest uznawana za osobę bezpośrednio lub pośrednio identyfikowalną poprzez odniesienie do identyfikatora, takiego jak nazwa, numer identyfikacyjny, dane dotyczące lokalizacji, identyfikator internetowy lub jeden lub więcej czynników specyficznych dla fizycznego, fizjologicznego, genetycznego, umysłowego, ekonomicznego, kulturowego lub społeczneg, tożsamość tej osoby fizycznej.

Przetwarzanie danych osobowych to dowolna zautomatyzowana lub niezautomatyzowana operacja lub zestaw operacji wykonywanych na danych osobowych lub w zestawach danych osobowych obejmujących zbieranie, rejestrowanie, organizowanie, strukturyzowanie, przechowywanie, adaptację lub zmianę, wyszukiwanie, konsultacje, wykorzystanie, ujawnianie poprzez transmisję, rozpowszechnianie lub udostępnianie w inny sposób, wyrównanie lub połączenie, ograniczenie, usunięcie lub zniszczenie danych osobowych.

Ograniczenie przetwarzania - polega na oznaczeniu przetwarzanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania.

Anonimizacja- zmiana danych osobowych w wyniku której dane te tracą charakter danych osobowych.

Zgoda osoby, której dane dotyczą - oznacza dowolne, dowolnie określone, konkretne, świadome i jednoznaczne wskazanie osoby, której dane dotyczą, za pomocą oświadczenia lub wyraźnego działania potwierdzającego, wyrażającego zgodę na przetwarzanie danych osobowych z nim związanych. Zgoda musi być udokumentowana we właściwy sposób, aby ją udowodnić.

Ocena skutków w ochronie danych - to proces przeprowadzany przez Administratora, jeśli jest wymagany przez obowiązujące prawo i, jeśli to konieczne, z uczestnictwem inspektora ochrony danych, przed przetwarzaniem, w przypadku, gdy istnieje prawdopodobieństwo wysokiego

ryzyka dla praw i wolności osób fizycznych jako rodzaju przetwarzania danych osobowych zachodzący wraz z wykorzystaniem nowych technologii, biorąc pod uwagę charakter, zakres, kontekst i cele przetwarzania. Proces ten musi ocenić wpływ planowanych operacji przetwarzania na ochronę danych osobowych.

Podmiotem danych jest każda osoba fizyczna, która jest przedmiotem przetwarzanych danych.

Odbiorca - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią.

Podmiot przetwarzający(Procesor) to osoba fizyczna lub prawna, organ publiczny, agencja lub jakikolwiek inny organ przetwarzający dane osobowe w imieniu administratora.

Inspektor Ochrony Danych(IOD) - to osoba formalnie wyznaczona przez Administratora w celu informowania i doradzania Administratorowi przetwarzającemu/pracownikom w zakresie obowiązującego prawa o ochronie danych i Polityki oraz w celu monitorowania ich przestrzegania oraz działania jako punkt kontaktowy dla osób, których dane są przetwarzane i organu nadzorczego.

Pseudonimizacja - oznacza przetwarzanie danych osobowych w taki sposób (np. poprzez zastępowanie nazw liczbami), że danych osobowych nie można już przypisać do określonego podmiotu danych bez użycia dodatkowych informacji (np. Listy referencyjnej nazwisk i numerów), pod warunkiem, że takie dodatkowe informacje są przechowywane oddzielnie i podlegają środkom technicznym i organizacyjnym w celu zapewnienia, że dane osobowe nie są przypisane do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

Szczególne kategorie danych osobowych - ujawniają pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, członkostwo w związkach zawodowych i obejmują przetwarzanie danych genetycznych, dane biometryczne w celu jednoznacznej identyfikacji osoby fizycznej, dane dotyczące zdrowia, dane dotyczące życia seksualnego osoby lub orientacji seksualnej. W zależności od obowiązującego prawa, specjalne kategorie danych osobowych mogą również zawierać informacje o środkach zabezpieczenia społecznego lub postępowaniach administracyjnych i karnych oraz o sankcjach.

Profilowanie – jest dowolną formą zautomatyzowanego przetwarzania danych osobowych, która polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.

Naruszenie ochrony danych osobowych - jest to przypadkowy lub niezgodny z prawem incydent prowadzący do zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

II. OCENA SKUTKÓW (ANALIZA RYZYKA)

Ocena skutków jest formalną, określoną w art. 37 RODO procedurą przeprowadzenia analizy ryzyka za wykonanie której odpowiada Administrator. Jeżeli Administrator/IOD przetwarzający nie jest zobowiązany do przeprowadzenia oceny skutków, może mimo to stosować poniższą procedurę do przeprowadzenia analizy ryzyka na potrzeby wykazania rozliczalności spełnienia wymagań RODO.
W przypadku powołania Inspektora Ochrony Danych – ocena skutków musi być wykonana z jego współudziałem.

1. OPIS OPERACJI PRZETWARZANIA (INWENTARYZACJA AKTYWÓW)

2) W celu dokonania analizy ryzyka wymagane jest zidentyfikowanie danych osobowych, które należy zabezpieczyć. Dane te w postaci zbiorów(kategorii osób) zostały wykazane w **Załączniku nr 1 do Polityki.**
3) Opis zbiorów (kategorii osób) powinien obejmować takie informacje, jak:
   a) nazwę zbioru (opis kategorii osób),
   b) opis celów przetwarzania,
   c) charakter, zakres, kontekst danych osobowych,
   d) odbiorcy danych,
   e) funkcjonalny opis operacji przetwarzania,
   f) aktywa służące do przetwarzania danych osobowych (informacje, programy, systemy operacyjne, infrastruktura IT, infrastruktura, pracownicy i współpracownicy, outsourcing), które zostały wykazane w **Załączniku nr 2 do Polityki**,
   g) informacja o konieczności wpisu do rejestru czynności przetwarzania,
   h) informacja o konieczności przeprowadzenia oceny skutków dla zbioru.

2. OCENA NIEZBĘDNOŚCI ORAZ PROPORCJONALNOŚCI (ZGODNOŚĆ Z PRZEPISAMI RODO)

W ramach przeprowadzenia oceny skutków (analizy ryzyka) Administrator przetwarzający dane osobowe (patrz **Załącznik nr 1 do Polityki)** zobowiązany jest do spełnienia wobec nich obowiązków prawnych. W szczególności należy zapewnić, że:

1) Dane te są legalnie przetwarzane na podstawie art. 6 RODO.
2) Dane te są adekwatne w stosunku do celów przetwarzania.
3) Dane te są przetwarzane przez określony czas (retencja danych).
4) Wobec tych osób wykonano tzw. obowiązek informacyjny zgodnie z art. 12, 13 i 14 RODO wraz ze wskazaniem ich praw (np. prawa dostępu do danych, przenoszenia, sprostowania, usunięcia, ograniczenia przetwarzania, sprzeciwu, odwołania zgody).
5) Opracowano klauzule informacyjne dla powyższych osób zgodnie z **Załącznikiem nr 3 do Polityki**.
6) Istnieją umowy powierzenia z podmiotami przetwarzającymi (art. 28 RODO) których wzór stanowi **Załącznik nr 4 do Polityki**, a informacje o podmiotach przetwarzających dane są zamieszczane w rejestrze umów powierzenia, którego wzór stanowi **Załącznik nr 5 do Polityki**.
7) Potwierdzenie spełnienia powyższych wymagań prawnych RODO znajduje się w **Załączniku nr 1 do Polityki**.

3. ANALIZA RYZYKA

Procedura opisuje sposób przeprowadzenia analizy ryzyka w celu zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń wynikających z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.
Przyjęto, że analiza ryzyka przeprowadzana jest dla zbioru lub grupy zbiorów (kategorii osób) lub dla procesów przetwarzania (np. dla zbioru pracowników, zbioru klientów z bazy).

1) **Definicje**
   a) Aktywa – środki materialne i niematerialne mające wpływ na przetwarzanie danych osobowych.
   b) Naruszenie (Incydent) ochrony danych osobowych - to naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia,

zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

c) Zagrożenie - potencjalne naruszenie (potencjalny incydent).
d) Skutki - rezultaty niepożądanego naruszenia (straty w wypadku wystąpienia zagrożenia).
e) Ryzyko - prawdopodobieństwo, że określone zagrożenie wystąpi i spowoduje straty lub zniszczenie zasobów.

2) **Wyznaczenie zagrożeń**
   a) Administrator jest odpowiedzialny za określenie listy zagrożeń, które mogą wystąpić w przetwarzaniu danych w zbiorze, dla kategorii osób lub w procesie przetwarzania.
   b) Zagrożenia powinny być identyfikowane w odniesieniu do uprzednio zidentyfikowanych aktywów.
   c) Wykaz przykładowych zagrożeń znajduje się w **Załączniku nr 6 do Polityki**.

3) **Wyliczenie ryzyka dla zagrożeń**
   a) Administrator określa Prawdopodobieństwo (**P**) wystąpienia poszczególnych zagrożeń w zbiorze lub w procesie przetwarzania.
   b) Proponowaną skalę prawdopodobieństwa prezentuje Tabela A.

Tabela A PRAWDOPODOBIEŃSTWO WYSTĄPIENIA ZAGROŻENIA	SKALA (WAGA)
zagrożenie niskie	1
zagrożenie średnie	2
zagrożenie wysokie	3

   c) Administrator określa Skutki (**S**) wystąpienia incydentów (materializacji zagrożeń), uwzględniając straty finansowe, utratę reputacji, sankcje/skutki karne.
   d) Proponowaną skalę skutków prezentuje Tabela B.

Tabela B SKUTKI WYSTĄPIENIA ZAGROŻENIA	SKALA (WAGA)
małe (do 10.000 PLN, incydent prasowy lokalny)	1
średnie (10.000-100.000 PLN, incydent prasowy ogólnopolski)	2
duże (od 100.000 PLN, naruszenie prawa)	3

   e) Administrator wylicza Ryzyka (R) dla wszystkich zagrożeń i ich skutków w/g formuły: **R = P * S**.

4) **Porównanie wyliczonego ryzyka ze skalą i określenie dalszego postępowania z ryzykiem**
   a) Administrator porównuje wyliczone ryzyka ze skalą i podejmuje decyzje dotyczące dalszego postępowania z ryzykiem.
   b) Proponowaną skalę Ryzyka prezentuje Tabela C.

Tabela C POZIOM RYZYKA	WARTOŚĆ [R = P*S]
ryzyko pomijalne i akceptowalne (akceptujemy)	1-2
ryzyko jest opcjonalne (akceptujemy albo obniżamy)	3-6
ryzyko jest nieakceptowalne (musimy obniżyć)	9

5) **Reakcja na wartość ryzyka**
   a) Akceptacja ryzyka – zabezpieczenia są właściwe – brak potrzeby stosowania dodatkowych zabezpieczeń.
   b) Działania obniżające ryzyko, które może zastosować Administrator:
      – Przeniesienie –przerzucenie ryzyka (outsourcing, ubezpieczenie),

- Unikanie – eliminacja działań powodujących ryzyko (np. zakaz wynoszenia komputerów przenośnych poza obszar Urzędu, niekopiowanie na pendrivy danych),
- Redukcja – zastosowanie zabezpieczeń w celu obniżenia ryzyka (np. zaszyfrowanie pendrivów z danymi wynoszonych poza Urząd).

c) Wykaz przykładowych zabezpieczeń znajduje się w **Załączniku nr 7 do Polityki.**
d) Analizę ryzyka przeprowadza się w specjalnym szablonie przedstawionym w **Załączniku nr 8 do Polityki.**

6) **Ponowna analiza ryzyka**
Ponowna analiza ryzyka przeprowadzana jest cyklicznie lub po znaczących zmianach w przetwarzaniu danych (np. przetwarzanie nowych zbiorów, nowe procesy przetwarzania, zmiany prawne)

4. PLAN POSTĘPOWANIA Z RYZYKIEM

1) Wszędzie, gdzie Administrator decyduje się obniżyć ryzyko, wyznacza listę zabezpieczeń do wdrożenia, termin realizacji i osoby odpowiedzialne
2) Administrator zobowiązany jest do monitorowania wdrożenia zabezpieczeń

III. UPOWAŻNIENIA

1. Administrator/ASI odpowiada za nadawanie i anulowanie upoważnień do przetwarzania danych w zbiorach papierowych i systemach informatycznych.
2. Każda osoba upoważniona musi przetwarzać dane wyłącznie na polecenie Administratora lub na podstawie przepisu prawa.
3. Upoważnienia nadawane są do zbiorów na wniosek przełożonych osób. Upoważnienia określają zakres operacji na danych, np. tworzenie, usuwanie, wgląd, przekazywanie według wzoru stanowiącego **Załącznik nr 9 do Polityki**.
4. Upoważnienia mogą być nadawane w formie poleceń, np. upoważnienia do przeprowadzenia kontroli, audytów, wykonania czynności służbowych, udokumentowanego polecenia Administratora w postaci umowy powierzenia.
5. IOD prowadzi ewidencję osób upoważnionych w celu sprawowania kontroli nad prawidłowym dostępem do danych osób upoważnionych według wzoru stanowiącego **Załącznik nr 10 do Polityki**.

IV. INSTRUKCJA POSTĘPOWANIA Z INCYDENTAMI

Procedura definiuje katalog podatności i incydentów zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie. Jej celem jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa oraz ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadamiania o stwierdzeniu podatności lub wystąpieniu incydentu bezpośredniego przełożonego lub (jeśli jest powołany) IOD.
2. Do typowych podatności bezpieczeństwa danych osobowych należą:
   1) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
   2) niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych,
   3) nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka/ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek).
3. Do typowych incydentów bezpieczeństwa danych osobowych należą:

1) zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),
2) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata/zagubienie danych),
3) umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).

4. W przypadku stwierdzenia wystąpienia incydentu, IOD prowadzi postępowanie wyjaśniające w toku, którego:
   1) ustala zakres i przyczyny incydentu oraz jego ewentualne skutki,
   2) inicjuje ewentualne działania dyscyplinarne,
   3) działa na rzecz przywrócenia działań organizacji po wystąpieniu incydentu,
   4) rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych incydentów w przyszłości lub zmniejszenia strat w momencie ich zaistnienia.
5. Administrator dokumentuje powyższe wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze w rejestrze, którego wzór stanowi **Załącznik nr 11 do Polityki**.
6. Zabrania się świadomego lub nieumyślnego wywoływania incydentów przez osoby upoważnione do przetwarzania danych.
7. W przypadku naruszenia ochrony danych osobowych skutkującego ryzykiem naruszenia praw lub wolności osób fizycznych, Administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu.

V. Regulamin Ochrony Danych Osobowych

Regulamin Ochrony Danych Osobowych w Urzędzie Miejskim w Piszu ma na celu zapewnienie wiedzy pracownikom przetwarzającym dane osobowe odnośnie bezpiecznych zasad przetwarzania. Regulamin ten stanowi **Załącznik nr 12 do Polityki**.
Po zapoznaniu się z zasadami ochrony danych osobowych, pracownicy zobowiązani są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania według wzoru stanowiącego **Załącznik nr 13 do Polityki**.

VI. Szkolenia

1. Każda osoba przed dopuszczeniem do pracy z danymi osobowymi winna być poddana przeszkoleniu i zapoznana z przepisami RODO.
2. Za przeprowadzenie szkolenia odpowiada IOD.
3. W przypadku przeprowadzenia szkolenia wewnętrznego z zasad ochrony danych osobowych wskazane jest udokumentowanie odbycia tego szkolenia za pomocą listy, której wzór stanowi **Załącznik nr14 do Polityki**.
4. Po przeszkoleniu z zasad ochrony danych osobowych, uczestnicy zobowiązani są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania.

VII. Rejestr czynności przetwarzania

1. W przypadku konieczności prowadzenia rejestru czynności przetwarzania przez Administratora, wypełnia on rejestr , którego wzór stanowi **Załącznik nr 15 do Polityki**.
2. W przypadku konieczności prowadzenia rejestru czynności przetwarzania przez Podmiot przetwarzający, wypełnia się rejestr, którego wzór stanowi **Załącznik nr 16 do Polityki**.

VIII. AUDYTY

Zgodnie z art. 32 RODO, Administrator powinien regularnie testować, mierzyć i oceniać skuteczność środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.
W tym celu Administrator stosuje procedurę audytu według **Załącznika nr 17 do Polityki**.

IX. PROCEDURA PRZYWRÓCENIA DOSTĘPNOŚCI DANYCH OSOBOWYCH I DOSTĘPU DO NICH W RAZIE INCYDENTU FIZYCZNEGO LUB TECHNICZNEGO (BCP)

Zgodnie z art. 32 RODO, Administrator powinien zapewnić zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego. Administrator opracował procedury przywracania, opisane w **Załączniku nr 18 do Polityki**.

X. WYKAZ ZABEZPIECZEŃ

1. Administrator prowadzi wykaz zabezpieczeń, które stosuje w celu ochrony danych osobowych zgodnie z Instrukcją zarządzania SI stanowiącą **Załącznik nr 19 do Polityki**.
2. W instrukcji wskazano stosowane zabezpieczenia proceduralne oraz zabezpieczenia jako środki techniczne i organizacyjne.
3. Instrukcja jest aktualizowana po każdej analizie ryzyka/ocenie skutków.

Wykaz zbiorów danych osobowych

Lp.	Nazwa zbioru danych (1)	**Aktywa** 1. Informacje 2. Programy i systemy operacyjne 3. Infrastruktura IT 4. Infrastruktura 5. Pracownicy i współpracownicy 6.Outsorcing	Podstawa przetwarzania	Rejestr czynności przetwarzania	Ocena skutków	Cel przetwarzania Rodzaj i zakres danych Odbiorcy	Opis operacji przetwarzania	Czas przechowywania
		1. Informacje **2. Programy i systemy operacyjne** **3. Infrastruktura IT** **4. Infrastruktura** **5. Pracownicy i współpracownicy** **6. Outsourcing**				**Cel:** Rodzaj danych: Odbiorcy:		

AKTYWA	PODAKTYWA
1. Informacje	**INFORMACJE**
	dane osobowe
	dane dostępowe (loginy, hasła, piny)
	dane dotyczące zabezpieczeń (certyfikaty)
	logi systemowe
	dokumentacja techniczna
	polityki bezpieczeństwa
	procedury odtworzeniowe
	umowy
2. Programy i systemy operacyjne	**OPROGRAMOWANIE**
	systemy operacyjne
	oprogramowanie użytkowe (pakiety biurowe, oprogramowanie biznesowe)
	serwery usługowe (www, poczta, serwery plików, bazy danych, usługi katalogowe)
	oprogramowanie administracyjne (wirtualizacja, inwentaryzacja, monitoring, backup)
	sterowniki
	oprogramowanie układowe (firmware)
	strony www i aplikacje webowe
3. Infrastruktura IT	**SPRZĘT KOMPUTEROWY**
	serwery (fizyczne i wirtualne)
	storage (NAS-y)
	stacje robocze (PC, laptopy)
	urządzenia peryferyjne (drukarki, skanery)
	TELEKOMUNIKACJA
	centrale telefoniczne
	centrale voip
	urządzenia klienckie (telefony, faxy, modemy)
	łącza (Internet, tunele vpn, linie dedykowane)
	NOŚNIKI DANYCH
	elektroniczne nośniki z danymi
	dokumentacja papierowa
	nośniki instalacyjne
	nośniki licencji
	SIEĆ
	usługi sieciowe (DNS, DHCP, VPN, protokoły routingu)
	okablowanie
	urządzenia aktywne (switche, routery, AP, mediakonwertery)
	urządzenia pasywne (krosownice, patchpanele)
	systemy sieciowe (firewalle, bramki, UTMy)
4. Infrastruktura	**OBSZARY CHRONIONE**
	serwerownie
	punkty dystrybucyjne sieci
	punkty składowania i przetwarzania danych (elektronicznych i papierowych)
	studzienki i kanały telekomunikacyjne
	rozdzielnie elektryczne
	stanowiska monitoringu

	SPRZĘT WSPOMAGAJĄCY
	klimatyzatory
	zasilacze awaryjne i agregaty
	monitoring środowiskowy (czujki temp., zalania, dymu)
	systemy automatycznego gaszenia
	systemy alarmowe
	systemy kontroli dostępu
5. Pracownicy i współpracownicy	**PERSONEL**
	kompetencje
	doświadczenie
	know-how
6.Outsorcing	**DOSTAWCY**
	oprogramowania
	usług chmurowych
	usług internetowych (hosting, dns, poczta)
	łączy
	usług serwisowych i gwarancyjnych
	wsparcia technicznego
	personelu

Klauzule informacyjne

Zgodnie z art. 13 ogólnego rozporządzenia PE i RE 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) informuję, iż:

1) administratorem Pani/Pana danych osobowych jest Urząd Miejski w Piszu z siedzibą w 12-200 Pisz, ul. Gustawa Gizewiusza 5,
2) kontakt z Inspektorem Ochrony Danych w Urzędzie Miejskim w Piszu możliwy jest pod adresem email: *inspektor@pisz.home.pl,*
3) Pani/Pana dane osobowe przetwarzane będą w celu..... na podstawie Art. 6 ust. 1 lit. a, b, c, e lub Art.9 ust.2 lit. a, b, c, d, f, g, h, i, - ogólnego rozporządzenia PE i RE 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),
4) odbiorcami Pana/Pani danych osobowych będą (podać informacje o odbiorcach lub kategoriach odbiorców jeżeli istnieją),
5) Pana/Pani dane osobowe przechowywane będą przez okres ..... dni/lat,
6) posiada Pani/Pan prawo do: żądania od Administratora dostępu do danych osobowych, prawo do ich sprostowania, usunięcia lub ograniczenia przetwarzania, prawo do wniesienia sprzeciwu wobec przetwarzania, prawo do cofnięcia zgody w dowolnym momencie,*
7) ma Pan/Pani prawo wniesienia skargi do organu nadzorczego,
8) podanie danych osobowych jest wymogiem ustawowym zawarcia umowy, jednakże niepodanie danych w zakresie wymaganym przez Administratora może skutkować błędnym wydaniem decyzji/naliczeniem podatku,
9) Jeżeli Administrator planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym dane osobowe zostały zebrane: Pana/Pani dane będą przetwarzane w celu wypełnienia obowiązku administracyjnego.

Zgodnie z art. 14 ogólnego rozporządzenia PE i RE 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) informuję, iż:

1) administratorem Pani/Pana danych osobowych jest Urząd Miejski w Piszu z siedzibą w 12-200 Pisz, ul. Gustawa Gizewiusza 5,
2) kontakt z Inspektorem Ochrony Danych w Urzędzie Miejskim w Piszu możliwy jest pod adresem email: *inspektor@pisz.home.pl*
3) Pani/Pana dane osobowe przetwarzane będą w celu..... na podstawie Art. 6 ust. 1 lit. b, c, e lub Art.9 ust.2 lit. a, b, c, d, f, g, h, i, - ogólnego rozporządzenia PE i RE 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),
4) kategoria danych osobowych: dane wrażliwe/niewrażliwe,
5) Pana/Pani dane osobowe pozyskano ze źródeł publicznych,
6) odbiorcami Pana/Pani danych osobowych będzie Urząd Miejski w Piszu,
7) Pana/Pani dane osobowe przechowywane będą przez okres .....dni/lat,
8) posiada Pani/Pan prawo do: żądania od Administratora dostępu do danych osobowych, prawo do ich sprostowania, usunięcia lub ograniczenia przetwarzania, prawo do wniesienia sprzeciwu wobec przetwarzania, prawo do cofnięcia zgody w dowolnym momencie,
9) ma Pan/Pani prawo wniesienia skargi do organu nadzorczego
10) Jeżeli Administrator planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym dane osobowe zostały zebrane: Pana/Pani dane będą przetwarzane w celu wypełnienia obowiązku administracyjnego.

UMOWA
powierzenia przetwarzania danych osobowych

zwana dalej Umową zawarta w Piszu w dniu ..... r. pomiędzy:

Gminą Pisz, ul. Gustawa Gizewiusza 5, 12-200 Pisz z siedzibą w Piszu, posiadającym numer NIP 8491499696 oraz numer REGON 790671538, reprezentowaną przez:
Burmistrza Pisza - .....,
zwaną dalej w Umowie Administratorem,

a

.....
z siedzibą w .....,
zarejestrowaną/ym w ..... pod numerem ....., posiadającą/ym numer NIP ..... oraz numer REGON ....., reprezentowaną/ym przez:
.....,
zwaną/ym dalej Podmiotem przetwarzającym.

§ 1
Definicje

1. Podmiot przetwarzający – podmiot, któremu powierzono przetwarzanie danych osobowych na mocy umowy powierzenia z Administratorem
2. Administrator - organ, jednostka organizacyjna, podmiot lub osoba, decydujące o celach i środkach przetwarzania danych osobowych.
3. Zbiór danych - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.
4. Przetwarzanie danych - jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.
5. Rozporządzenie- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).
6. Podwykonawca przetwarzający - podmiot, któremu Podmiot przetwarzający powierzył w całości lub częściowo przetwarzanie danych osobowych, jako konsekwencję realizowania swojej umowy powierzenia z Administratorem.
7. Umowa – zgodne porozumienie dwóch lub więcej stron ustalające ich wzajemne prawa lub obowiązki.

§ 2
Przedmiot Umowy

1. Przedmiotem Umowy jest powierzenie przez Administratora danych osobowych do przetwarzania przez Podmiot przetwarzający.
2. Celem powierzenia jest:
   ..... *(np. administracja systemami informatycznymi w zakresie danych osobowych przetwarzanych w tych systemach)*

..... *(np. hosting poczty, hosting serwerów w zakresie danych osobowych przetwarzanych w tych systemach)*

§ 3
Odpowiedzialność Podmiotu przetwarzającego

1. Podmiot przetwarzający jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią Umowy.
2. Podmiot przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Administratora i od współpracujących z nim osób.
3. Podmiot przetwarzający jest zobowiązany do niezwłocznego zawiadomienia Administratora o jakimkolwiek incydencie, postępowaniu, a także o wszelkich planowanych lub realizowanych kontrolach dotyczących przetwarzania w Podmiocie przetwarzającym tych danych osobowych, w szczególności prowadzonych przez Urząd Ochrony Danych Osobowych.

§ 4
Prawa Podmiotu przetwarzającego

1. Podmiot przetwarzający ma prawo do dostępu do wszystkich informacji od Administratora mających bezpośredni wpływ na bezpieczeństwo przetwarzania danych osobowych w ramach Umowy.
2. Podmiot przetwarzający ma prawo wstrzymać lub ograniczyć przetwarzanie danych osobowych w ramach Umowy, jeżeli Administrator nie przekaże mu niezbędnych informacji na temat sposobu, zakresu i charakteru przetwarzanych danych lub gdy opóźnia się z ich przekazaniem.

§ 5
Gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych wykonywania usług administracji / serwisowania IT

1. Podmiot przetwarzający zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi Rozporządzenia i chroniło prawa osób, których dane dotyczą.
2. Podmiot przetwarzający przetwarza dane osobowe wyłącznie na udokumentowane polecenie Administratora.
3. Podmiot przetwarzający gwarantuje, że każda osoba realizująca Umowę zobowiązana jest do bezterminowego zapewnienia poufności danych osobowych przetwarzanych w związku z wykonywaniem Umowy, a w szczególności do tego, że nie będzie przekazywać, ujawniać i udostępniać tych danych osobom nieuprawnionym. Jednocześnie każda osoba realizująca Umowę zobowiązana jest do zachowania w tajemnicy sposobów zabezpieczenia danych osobowych.
4. Podmiot przetwarzający zobowiązuje się dopuszczać do przetwarzania danych osobowych osoby realizujące Umowę (podać ewentualnie funkcje osób, serwisanci, konsultanci) poinformowane i przeszkolone z zasad bezpieczeństwa pracy z danych osobowymi.
5. Każda osoba realizująca Umowę zobowiązana jest do przetwarzania danych osobowych do których uzyskała dostęp wyłącznie w zakresie i celu przewidzianym w Umowie.
6. Każda osoba realizująca Umowę zobowiązana jest do niepowodowania niezgodnych z Umową zmian danych lub utraty, uszkodzenia lub zniszczenia tych danych.

7. W przypadku wykorzystania sieci publicznej, każda osoba realizująca Umowę zobowiązuje się do stosowania zabezpieczonego przed podsłuchem połączenia zdalnego (VPN, SSL).
8. Każda osoba realizująca Umowę zobowiązana jest do pracy w systemach Administratora z użyciem uwierzytelnienia.
9. Podmiot przetwarzający zobowiązuje się stosować ochronę powierzonych danych przed niedozwolonym lub niezgodnym z prawem przetwarzaniem (zniszczeniem, utraceniem, zmodyfikowaniem, nieuprawnionym ujawnieniem lub nieuprawnionym dostępem do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych) oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność").
10. Podmiot przetwarzający zastosuje środki zabezpieczenia określone w art. 32 Rozporządzenia, przy czym wdrożone środki zabezpieczenia muszą być adekwatne do zidentyfikowanych ryzyk dla zakresu powierzonego przetwarzania danych.

§ 6
Korzystanie przez Podmiot przetwarzający z usług innego podmiotu przetwarzającego

1. Podmiot przetwarzający nie korzysta z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody Administratora.
2. W przypadku ogólnej pisemnej zgody Podmiot przetwarzający informuje Administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, dając tym samym Administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian.
3. Podpowierzenie przetwarzania przez Podmiot przetwarzający innemu podmiotowi przetwarzającemu wymaga formy pisemnej. W przypadku podpowierzenia, na podwykonawcę zostaną nałożone takie same obowiązki, jak wynikają z Umowy. Podmiot przetwarzający odpowiada za działania podmiotu przetwarzającego (podwykonawcy) tak, jak za własne.

§ 7
Czas trwania Umowy

1. Umowa zostaje zawarta na czas .....
2. Podmiot przetwarzający uprawniony jest do przetwarzania powierzonych danych do dnia wygaśnięcia lub rozwiązania Umowy.
3. W terminie 14 dni od wygaśnięcia lub rozwiązania Umowy Podmiot przetwarzający zobowiązany jest usunąć powierzone dane osobowe, jeżeli dokonał ich jakichkolwiek kopii lub utrwalił je na jakichkolwiek nośnikach, chyba, że obowiązek ich dalszego przetwarzania przez Podmiot przetwarzający wynika z odrębnych przepisów prawa.

§ 8
Charakter przetwarzania

1. Przetwarzanie danych osobowych odbywa się w formie papierowej oraz przy wykorzystaniu systemów informatycznych.
2. Dane osobowe wykorzystywane są do .....
(*np. organizacji administrowania programami informatycznymi, stworzenia listy płac, stworzenia listy uczestników wycieczki, podać inne*).

§ 9
Obowiązki i prawa administratora

1. Na żądanie Administratora Podmiot przetwarzający udostępni mu wszelkie informacje niezbędne do wykazania spełnienia obowiązków spoczywających na Podmiocie przetwarzającym oraz umożliwi Administratorowi lub audytorowi upoważnionemu przez Administratora przeprowadzanie audytów, w tym inspekcji, współpracując przy działaniach sprawdzających i naprawczych.
2. Podmiot przetwarzający udzieli pomocy Administratorowi w realizacji obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III Rozporządzenia, jak również w zakresie zapewnienia realizacji obowiązków wynikających z art. 32–36 Rozporządzenia.

§ 10
Rozwiązanie umowy

1. Zleceniodawca może rozwiązać Umowę, gdy podmiot przetwarzający przetwarza dane osobowe niezgodnie z Umową.
2. W sytuacji, gdy Podmiot przetwarzający podpowierzy przetwarzanie danych osobowych innemu podmiotowi bez zgody Administratora może on rozwiązać Umowę bez wypowiedzenia.
3. Rozwiązanie Umowy może nastąpić, gdy pomimo zobowiązania Podmiot przetwarzający nie usunął uchybień wykazanych podczas przeprowadzonej przez Administratora kontroli zgodności jej wykonania z Umową i Rozporządzeniem.

§ 11
Postanowienia końcowe

1. Wszelkie zmiany Umowy powinny być dokonane w formie pisemnej pod rygorem nieważności.
2. W sprawach nieuregulowanych Umową, zastosowanie znajdują przepisy polskiego prawa, w tym Kodeksu cywilnego.
3. Spory wynikłe z tytułu Umowy będzie rozstrzygał Sąd właściwy ze względu na siedzibę Administratora.
4. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.

....

Załącznik nr 5 do Polityki

Rejestr umów powierzenia

Lp.	Nazwa Administratora	Kategoria osób których dane dotyczą, kategoria danych osobowych, zakres przetwarzanych danych	Numer umowy powierzenia	Zakres czynności przetwarzania

Lista potencjalnych zagrożeń

Zagrożenie	Opis zagrożenia
Phishing, cybersquatting *(podrabianie stron)*	• Mail z prośbą o zalogowanie się (pod pretekstem weryfikacji danych lub informowania o próbie włamania na konto) do „podróbki" strony, np. bankowej, lub pseudo konta gmail i w rezultacie przejęcie hasła, • zachęcanie do zalogowania się do podrobionej strony o „wiarygodnym" adresie www. Zamiast logować się do www.mbank.pl logowanie byłoby w www.rnbank.pl.
Nakłanianie do wykonania czynności	• mail z dyspozycją przelewu wysłany do księgowej z rzekomego konta „Prezesa", • fax/mail z fakturą od rzekomego „dostawcy" z informacją o zmianie numeru konta bankowego do opłacenia faktur.
Instalacja szkodliwego oprogramowania/działanie szkodliwego oprogramowania	Szkodliwe oprogramowanie (backdoory, exploity, exploitpaki, keyloggery). *Najczęściej instalowane są poprzez otwarcie „zainfekowanego" załącznika z maila lub poprzez kliknięcie na zarażoną stronę. Maile takie zachęcają do otwarcia załącznika lub kliknięcia na hiperlink (mail z fakturą do opłacenia, mail z DHL o przesyłce, mail z rzekomym pismem urzędowym). W efekcie możemy zarazić nasz komputer lub wiele komputerów w sieci.* *Działające szkodliwe oprogramowanie może wywołać różnorodne skutki:* • *przejęcie konta pocztowego do wysyłki spamu,* • *użycie przejętych komputerów do kupowania kryptowalut,* • *użycie przejętych komputerów do ataków DOS,* • *użycie przejętych komputerów do śledzenia haseł użytkowników celem uzyskania dostępu do systemów i plików,* • *użycie przejętych komputerów do uzyskania pełnego dostępu do wewnętrznej sieci i kopiowania danych i baz danych (kradzież).* *Szkodliwe oprogramowanie:* *Wirusy i trojany – instalują się często z nielegalnym oprogramowaniem. Zawierają ukrytą funkcjonalność, działają na szkodę użytkownika.* *Backdoory - instalują się z maili lub z hiperlinków w mailach. Po uruchomieniu umożliwiają intruzowi ponowny dostęp i stałą kontrolę nad komputerem. Taki komputer-zombie może być użyty do wszelkich zachcianek intruza.* *Keyloggery - programy przechwytujące hasła wpisywane na klawiaturze przez użytkownika i oddające je intruzowi.* *Exploity / exploitpaki - Oprogramowanie wykorzystujące znane luki w systemach. Uruchomiony pozwala na przejęcie systemu przez intruza.*
Podrzucone nośniki danych	Atakujący pozostawia w Urzędzie lub w Wydziale Finansowym specjalnie przygotowany pendrive z zainstalowanym samouruchamiającym się szkodliwym programem. W wielu przypadkach z CIEKAWOŚCI pracownicy sprawdzają jego zawartość wkładając go do portu USB. W wyniku tego uruchamiają nieświadomie szkodliwe oprogramowanie (backdoory, exploity, exploitpaki, keyloggery).

Ataki telefoniczne	• intruz podający się za „naszego informatyka" prosi o podanie hasła pod pretekstem sprawdzania lub naprawy naszego systemu informatycznego, • intruz przedstawia się jako „serwisant Orange lub Netii" naprawiający usterkę i prosi o wejście na określoną stronę internetową w ramach testowania łącza internetowego, • intruz przedstawia się jako inżynier Microsoftu lub programista dostawcy oprogramowania. Podsyła „aktualizację" lub prosi o udostępnienie pulpitu.
Łamanie haseł	Łamanie haseł metodami słownikowymi i siłowymi (brute force): • do baz danych, • do serwera, • do aplikacji www (np. do wordpressa), • do poczty, • do windows na stacjach roboczych, • do routera, • do firewalla.
Łatwo dostępne, łatwe lub standardowe hasła	• ujawnianie haseł, • nieprawidłowe przechowywanie (karteczki, pliki), • stosowanie domyślnych haseł producenta, • stosowanie słownikowych lub popularnych haseł, np. Grazynka1, qwerty, 12345678, • stosowanie jednego hasła do wielu (często wszystkich) systemów.
Ataki na sprzęt - Włamania do urządzeń nieaktualizowanych	Ataki na urządzenia sieciowe oraz inne, które działają dzięki umieszczonemu na nich oprogramowaniu (firmware) Zagrożenie dla następujących elementów: • routery, • switche, • access pointy, • firewall, • macierz, • dysk NAS. *Brak aktualizacji tego oprogramowania (firmware) skutkuje podatnością na włamania, kradzież danych, zakłócanie pracy.*
Ataki na sprzęt - Włamania do urządzeń nieodpowiednio skonfigurowanych	Ataki na błędnie skonfigurowany sprzęt lub sprzęt działający z ustawieniami fabrycznymi. Zagrożenie dla następujących elementów: • routery, • switche, • access pointy, • firewalle, • macierze, • dyski NAS. *Błędy konfiguracyjne popełniane przez administratorów sieci mogą ułatwiać hackerom włamanie się do sieci lub urządzenia. Powodem jest najczęściej brak profesjonalnej wiedzy u osób konfigurujących urządzenia. Przykładem jest np. pozostawienie domyślnych haseł lub dostępu do strony konfiguracyjnej routera z poziomu Internetu.*
Ataki na sprzęt - Włamania z użyciem niezabezpieczonych interfejsów lokalnych	Atakujący wpina się do urządzeń IT przez ich niezabezpieczone porty konfiguracyjne (USB, Ethernet lub COM - szeregowe) Zagrożenie dla następujących elementów: • routery,

	• switche, • firewalle, • macierze, • serwery. *Administratorzy sieci często pozostawiają te porty niezabezpieczone, co powoduje ryzyko wpięcia się do powyższych urządzeń i ich skonfigurowania przez hakera.*
Ataki na sprzęt - Włamania za pośrednictwem niepotrzebnych usług (np. telnet na routerze)	Atakujący wykorzystuje do włamania usługi sieciowe, których działanie w danym środowisku nie jest wymagane Zagrożenie dla następujących usług: • DHCP, • DNS, • SSH, • http, • telnet, • FTP, • SMTP, • SNMP. *Urządzenia sieciowe posiadają często włączone wszystkie możliwe usługi sieciowe (DHCP, DNS, SSH, HTTP, telnet, FTP), mimo iż nie wszystkie z nich są potrzebne w danym środowisku. Każda z tych usług jest obsługiwana przez oprogramowanie, które może zawierać błędy.*
Ataki na oprogramowanie - wykorzystanie znanych dziur w nieaktualizowanym oprogramowaniu	Atak z wykorzystaniem znanych dziur w niezaktualizowanym oprogramowaniu Zagrożenie dla programów: • systemy operacyjne na stacjach roboczych, • systemy serwerowe, • przeglądarki www, • Wordpress, Drupal, • dedykowany CMS, • Adobe, • Flash, • Java. *Istniejące błędy oprogramowania pozwalające na przełamanie zabezpieczeń są upubliczniane po tym, jak producent oprogramowania przygotuje odpowiednią łatę lub aktualizację. Jeżeli nie zainstalujemy tych aktualizacji, narażamy się na atak, np. zdalny dostęp do systemu lub wykonanie złośliwego kodu (instalacja backdoora, exploita, ransomeware).*
Podsłuch	• podsłuch danych przesłanych drogą mailową, • podsłuch danych podczas korzystania z aplikacji webowych, • podsłuch podczas korzystania z formularzy kontaktowych, • podsłuch podczas zdalnego dostępu do sieci wewnętrznej przez Internet.
Ataki na oprogramowanie - włamania z wykorzystaniem luk typu zero day	Zero-day to błędy w oprogramowaniu, do których autor nie przygotował jeszcze poprawek / aktualizacji. Informacje o nich są sprzedawane i wykorzystywane przez intruzów.
Ataki na oprogramowanie - włamania z wykorzystaniem najczęstszych błędów programistycznych	*Programiści pisząc programowanie często popełniają te same, znane błędy.* *Przykładowo: możliwość wpisania ujemnej liczby sztuk w formularzu zamówienia, możliwość odgadnięcia numeru zamówienia innego klienta i wpisanie go w pasku adresu przeglądarki w celu wyświetlenia szczegółów.*

Włamania z wykorzystaniem API (interfejsów programistycznych)	*Niektóre aplikacje pozwalają na zdalne zarządzanie nimi przez specjalnie zaprojektowane funkcje/usługi sieciowe. Np. baza danych może pozwalać na podłączenie się do niej administratorowi sieci w celu wykonania prac naprawczych lub backupu. Dostęp ten odbywa się przy użyciu domyślnych loginów i haseł, co stanowi zagrożenie.*
Ataki na oprogramowanie - namierzanie wersji testowych (np. strona www)	*Niektóre aplikacje posiadają swoje kopie utrzymywane do celów testowych. Są one często gorzej zabezpieczone i łatwiej jest się do nich włamać, a mogą zawierać również krytyczne dane ze środowiska produkcyjnego. Przykładem może być kopia serwera wykonana w celu przetestowania nowej wersji aplikacji. Często udaje się je namierzyć wpisując np. zamiast adresu www.strona.pl adres test.strona.pl .*
Skanowanie sieci i usług	*Udostępniane w Internecie serwery, urządzenia sieciowe i aplikacje oraz serwisy www mogą być namierzane przez intruzów poprzez skanowanie adresów IP. Polega to na próbach łączenia się z wszystkimi znanymi usługami w celu sprawdzenia, które z nich są dostępne w naszej sieci i w jakiej wersji. Dzięki temu możliwe jest znalezienie usług nieaktualnych i zawierających błędy.*
Włamanie do sieci poprzez WIFI	Uzyskanie dostępu do sieci wewnętrznej poprzez włamanie się do sieci bezprzewodowej
Włamanie z sieci zewnętrznej do sieci wewnętrznej	Włamania z zewnątrz poprzez nieodpowiednio zabezpieczone i skonfigurowane punkty styku z Internetem oraz udostępnione w Internecie serwery i aplikacje.
Nieuprawniony dostęp do sieci z użyciem hakerskiego urządzenia	Możliwość wpięcia hakerskiego urządzenia do łatwo dostępnych urządzeń sieciowych wewnątrzorganizacyjnych, celem uzyskania dostępu do sieci przez to urządzenie z zewnątrz. Możliwość uruchomienia tzw. wrogiego access pointa w celu przechwycenia klientów sieci bezprzewodowej. Zagrożenie dla następujących elementów: • gniazdka sieciowe w korytarzach, w sali konferencyjnej, • skanery, drukarki na korytarzach, • switche w miejscach dostępnych.
Atak ransomeware	Ransomeware - program do szyfrowania plików. Instaluje się z maili lub z hiperlinków w mailach lub poprzez odwiedziny zainfekowanej strony. Są też znane przypadki infekcji poprzez sieć lokalną. Odszyfrowanie wymaga zapłaty np. 500 USD. Bardzo groźny.
ATAKI MAN-IN-THE-MIDDLE	Zmuszenie komputerów w sieci lokalnej do komunikowania się za pośrednictwem komputera intruza. Umożliwia przechwytywanie i podsłuchiwanie ruchu w sieci.
Eskalacja uprawnień	• zwiększenie uprawnień użytkownika przez wykorzystanie błędów programistycznych, • przejęcie uprawnień użytkownika zaawansowanego, • przejęcie uprawnień administratora, • przejęcie uprawnień systemowych, • przejęcie innych poświadczeń (certyfikaty elektroniczne, pliki cookies z identyfikatorami sesji).
Atak DOS/DDOS	Atak na system komputerowy lub usługę sieciową w celu uniemożliwienia działania. Atak dotyczy głownie stron i aplikacji www. Np. wypełnienie i wysłanie kilka milionów razy formularza kontaktowego (za pomocą skryptu) i spowodowanie zapełnienia dysku. *Zmasowany atak pojedynczego atakującego (DOS) lub z wielu komputerów jednocześnie (DDOS) na jakąś stronę www lub na portal, aby ją przeciążyć i „zakorkować".*

Nieuprawniony dostęp lub włamanie do pomieszczeń	Dostęp do: • budynków, • pomieszczeń biurowych, • archiwów, • serwerowni, • miejsc przechowywania kopii bezpieczeństwa. Może skutkować: • dostępem do danych w wersji papierowej, • dostępem do plików lub aplikacji lub baz danych, • zainstalowaniem nieautoryzowanych urządzeń do dostępu do sieci wewnętrznej, • kradzieżą komputerów, nośników.
Kradzież/zagubienie sprzętu i nośników poza organizacją	Kradzież / zagubienie: • laptopów, • smartfonów, • pendrive, • dysków wymiennych.
Nieuprawniony dostęp do infrastruktury IT oraz do programów	• brak kontroli nad dostępem do serwera, plików, programów, komputerów, • nadane zbyt wysokie uprawnienia użytkownikom, • dostęp osób nieupoważnionych do kopii bezpieczeństwa, • łatwy dostęp osób nieupoważnionych do danych prezentowanych na monitorach, drukarkach, kserokopiarkach, • niezabezpieczona praca zdalna użytkowników lub serwisu IT.
Udostępnianie danych osobom nieupoważnionym z sieci publicznej (przez Internet)	• dostęp do danych osobowych poprzez stronę www bez logowania się, • dostęp do danych osobowych poprzez stronę www po zalogowaniu się (użytkownik może przeglądać dane osobowe innych użytkowników), • dostęp do katalogów udostępnionych pod publicznym adresem IP plików z danymi osobowymi lub kopii bezpieczeństwa (bez logowania się), • udostępnianie plików zaindeksowanych przez roboty google na skutek braku komend chroniących katalogi webowe przez taką indeksacją, • przesłanie lub wydawanie informacji osobie nieupoważnionej.
Awarie / uszkodzenia elementów IT	Awarie: • dysków, • stacji roboczych, • urządzeń sieciowych/routerów, • drukarek / skanerów, • serwera.
Błąd/awaria oprogramowania	Awarie: • programu kadrowo-płacowego, • poczty, • aplikacji www (np. do wordpressa) • bazy danych.
Pożar/eksplozja	• pożar obiektu, • pożar serwerowni, • pożar serwera, • zniszczenie serwerowni (np. wybuch gazów technicznych).
Zalanie	• zalanie serwerowni,

	• zalanie archiwum (powódź, zalanie z rur).
Przegrzanie/zbyt duża wilgotność	• wysoka temperatura w serwerowni, • wysoka wilgotność w archiwum.
Awaria zasilania	• skoki napięcia, • przerwy w dostawie zasilania.
Nieuprawniona modyfikacja/usunięcie	• niezamierzone lub pomyłkowe zmodyfikowanie/usunięcie danych, • sfałszowanie danych przez osoby z wewnątrz lub zewnątrz organizacji.
Nieuprawnione kopiowanie danych	• kopiowanie danych z katalogów, dysków, baz, programów, • kserowanie i robienie zdjęć przez pracownika lub przez osobę obcą.
Brak/błędy w wykonywaniu kopii bezpieczeństwa	• doraźne lub za rzadkie wykonywanie kopii, • błędy podczas procesu wykonywania kopi, • niemożność odtworzenia kopii ze względu na zmiany w oprogramowaniu.
Nieprawidłowe/brak procedur niszczenia nośników z danymi	• wyrzucenie uszkodzonych nośników bez ich zniszczenia, • wyrzucanie dokumentów papierowych na śmietnik lub pozostawienie dokumentów w miejscu publicznym, • wyrzucenie niezniszczonych , HD, pendrive, DVD.
Nieprawidłowe/brak procedur napraw w serwisach zewnętrznych	• naprawa sprzętu z nośnikami bez umowy lub bez standardu bezpiecznej naprawy.
Nieprzestrzeganie procedur	• świadome naruszenie pisemnych lub ustnych procedur np. niewylogowywanie się z systemu, przekazywanie haseł osobom nieupoważnionym, naruszenie polityki czystego ekranu lub czystego biurka, • naruszenia powyżej wskazane na skutek braków z powodów niewiedzy.
Pomyłki i błędy administratorów, użytkowników	• udostępnienia katalogów i dysków, serwerów ftp, aplikacji z danymi do powszechnego dostępu przez sieć publiczną –z powodu „ułatwienia pracy" administratorów systemów, • łatwe logowanie się do baz i programów „login admin, hasło admin1", • dostęp do programów testowych (z prawdziwymi danymi osobowymi) bez logowania, • pomyłkowe udostępnienie, wysłanie do złego odbiorcy, błędne zabezpieczenia.
Błędy projektowe/konfiguracyjne	• błędy programistów prowadzące do udostępniania danych z tworzonych lub administrowanych programów • niezabezpieczenie danych w katalogach i bazach webowych i przed indeksacją robotów google.
Brak aktualnej dokumentacji (instrukcji, opisów, dokumentacji technicznej sprzętu i oprogramowania)	• brak instrukcji, opisów, dokumentacji technicznej sprzętu i oprogramowania, • brak instrukcji instalacyjnych i konfiguracyjnych środowiska lub oprogramowania. *Zagrożenie związane z możliwymi trudnościami w odtworzeniu środowiska i zarządzania nim, gdy np. odejdzie pracownik IT lub będzie on niedostępny podczas krytycznej awarii.*
Nieprawidłowe/brak umowy o współpracy	Nieprecyzyjnie określone odpowiedzialności we współpracy, co stwarza ryzyko braku zabezpieczeń.
Nieprawidłowe/brak umowy gwarancyjnej lub wsparcia serwisowego	*Należy uwzględnić, że umowy wymagają przedłużania, czas reakcji nie oznacza czasu naprawy.*

Upadek firmy outsourcingowej lub dostawczej	• brak zastępstw, np. dla hostingodawcy poczty, dla wsparcia do zakupionej aplikacji, • utrata usługi/aplikacji, którą świadczy pomiot przetwarzając.
Awaria łączy telekomunikacyjnych	Krytyczne dla administratora świadczącego usługi wymagające Internetu, usługi chmurowe, ISP oraz dostawcy platform SaaS.

Lista potencjalnych zabezpieczeń

Zabezpieczenie	Opis	Rodzaj zabezpieczenia
Regulamin ODO dla pracowników i współpracowników	Zabezpieczenia: osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy, osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych i podpisują stosowne oświadczenie poufności	Zabezpieczenia organizacyjne
Szkolenia personelu	Zabezpieczenia: szkolenia wewnętrzne	Zabezpieczenia organizacyjne
Audyty	Procedury: procedura audytu	Zabezpieczenia organizacyjne
Testy penetracyjne	Zabezpieczenia: testy penetracyjne	Zabezpieczenia organizacyjne
Procedury przywracania w razie incydentu	Procedury: plan ciągłości działania	Zabezpieczenia organizacyjne
Polityka kluczy/polityka kontroli dostępu	Procedury: polityka kluczy, polityka kontroli dostępu, Zabezpieczenia: kontrola kluczy zapasowych, zakaz wstępu osób nieupoważnionych, kontrola wydawania kluczy, kontrola składowania kluczy	Zabezpieczenia fizyczne
Dostęp do pomieszczeń i sprzętu	Zabezpieczenia: ograniczenie dostępu do pomieszczeń, komputerów, drukarek, xero osobom nieupoważnionym, chyba że w obecności osoby upoważnionej	Zabezpieczenia fizyczne
Zabezpieczenie dostępu do pomieszczeń (w tym biurowych)	Zabezpieczenia: drzwi zamykane na klucz, drzwi ognioodporne, drzwi antywłamaniowe, drzwi zamykane siłownikami	Zabezpieczenia fizyczne
Zabezpieczenie dostępu do serwerowni	Zabezpieczenia: drzwi zamykane na klucz, wejście kodowane	Zabezpieczenia fizyczne
Zabezpieczenie dostępu do archiwum	Zabezpieczenia: drzwi zamykane na klucz	Zabezpieczenia fizyczne
Zabezpieczenie dokumentacji w pomieszczeniach	Zabezpieczenia: zamknięte niemetalowe szafy, zamknięte metalowe szafy, sejf, skrytki na klucze	Zabezpieczenia fizyczne
Systemy alarmowe/zabezpieczenia antywłamaniowe	Zabezpieczenia: system alarmowy, kraty, rolety	Zabezpieczenia fizyczne
Ochrona fizyczna obiektu/pomieszczeń	Zabezpieczenia: ochrona własna, firma ochroniarska	Zabezpieczenia fizyczne
Strefy dostępu	Zabezpieczenia: Organizacja stref ograniczonego dostępu	Zabezpieczenia fizyczne
System ppoż	Zabezpieczenia: system w obiekcie, system gaszenia serwerowni, gaśnice	Zabezpieczenia techniczne
Mnitoring środowiskowy	Zabezpieczenia: w archiwum - czujniki wilgotności, w serwerowni - czujnik temperaturowy	Zabezpieczenia techniczne
Klimatyzacja	Zabezpieczenia: klimatyzacja w serwerowni	Zabezpieczenia techniczne
Monitoring wizyjny	Zabezpieczenia: monitoring wizyjny w obrębie obiektu i otoczeniu	Zabezpieczenia techniczne

Systemy UPS/agregaty prądotwórcze	Zabezpieczenia: zastosowano UPS podtrzymujący zasilanie serwera, UPS kluczowych elementów systemu IT	Zabezpieczenia techniczne
Systemy antywirusowy i antyspamowy	Zabezpieczenia: wersja stanowiskowa, serwerowa, licencjonowany, aktualizowany online, skanowanie poczty, skanowanie portów USB, wersja na komputery, smartfony, tablety	Zabezpieczenia informatyczne
Sewery proxy i bramki filtrujące	Zabezpieczenia: skan niebezpiecznej zawartości, blokada ruchu na podstawie bazy reputacji, blokada dostępu do określonych stron	Zabezpieczenia informatyczne
Systemy firewall, NG firewall, UTM	Zabezpieczenia: UTM do ochrony dostępu do sieci komputerowej, firewall sprzętowy, firewall programowy	Zabezpieczenia informatyczne
Monitorowanie zużycia	Zabezpieczenia: systemy monitorujące stan usług i zasobów krytycznych, serwerów, baz danych i urządzeń sieciowych	Zabezpieczenia informatyczne
Systemy do inwentaryzacji	Zabezpieczenia: system do inwentaryzacji sprzętu, zarządzania licencjami, monitoring użytkowników	Zabezpieczenia informatyczne
Szyfrowanie	Zabezpieczenia: szyfrowanie poczty (SSL), szyfrowanie połączeń internetowych SSL/VPN, szyfrowanie Pendrive, szyfrowanie dysków komputerów przenośnych (bitlocker), szyfrowanie plików (7zip)	Zabezpieczenia informatyczne
Hardening	Włączenie szyfrowania, zmiana domyślnych haseł, wyłączenie niepotrzebnych funkcji i usług, bazuje na dobrych praktykach lub standardach , dodatki noscript i adblocker do przeglądarek	Zabezpieczenia informatyczne
Redundancja krytycznych zasobów	Zabezpieczenia: redundancja łącz	Zabezpieczenia informatyczne
Aktualizacje systemu	Zabezpieczenia: zarządzanie aktualizacjami systemu operacyjnego, aplikacji, przeglądarek internetowych	Zabezpieczenia informatyczne
Backupy i archiwizacja	Procedury: procedura tworzenia kopii zapasowych, Zabezpieczenia: Backup serwerów, aplikacji, plików, konfiguracji, licencji, haseł, zabezpieczenie przed ransomeware, kopie poza serwerownią, niszczenie/czyszczenie nośników przed utylizacją	Zabezpieczenia informatyczne
Rozliczalnosć operacji	Zabezpieczenie: program/aplikacja posiada mechanizm odnotowywania wykonywania operacji na danych osobowych. Odnotowane i logowane są: tworzenie rekordu, zmiana, usunięcie, wgląd w dane, użytkownik dokonujący zmian, każdy użytkownik posiada swój indywidualny login	Zabezpieczenia informatyczne

Postępowanie z nośnikami	Procedury: procedura postępowania z nośnikami i sprzętem poza organizacją, regulamin korzystania z komputerów przenośnych, Zabezpieczenia: ograniczono możliwość kopiowania danych na pendrive, zastosowano blokadę portów USB do korzystania z pendrive, wymuszono użycie szyfrowanych firmowych pendirve	Zabezpieczenia informatyczne
Zabezpieczenie pracy użytkowników	Procedury: procedura korzystania z internetu, procedura korzystania z poczty elektronicznej, Zabezpieczenia: zahasłowane wygaszacze ekranu aktywowane w przypadku nieaktywności użytkownika, poufne ustawienie monitorów, filtry polaryzacyjne, terminacja sesji	Zabezpieczenia informatyczne
Wirtualizacja	Zabezpieczenia: wirtualizacja	Zabezpieczenia informatyczne
Niszczenie nośników	Procedury: procedura niszczenia nośników, Zabezpieczenia: niszczarki ścinkowe, niszczarki o podwyższonym standardzie, niszczenie/czyszczenie nośników przed utylizacją, firma niszcząca dokumenty	Zabezpieczenia informatyczne
Zarządzanie uprawnieniami	Procedury: procedura zarządzania uprawnieniami, Zabezpieczenia: minimalizacja uprawnień, separacja obowiązków, zarządzanie uprawnieniami, konta firmowe + prywatne	Zabezpieczenia informatyczne
Uwierzytelnianie	Procedury: polityka haseł, Zabezpieczenia: długość hasła, częstotliwość zmiany, wymuszenie zmiany, uwierzytelnianie za pomocą kodu PIN, uwierzytelnianie biometryczne, hasło na BIOS. Uwierzytelnianie do aplikacji, stacji roboczej,smartfona dysku sieciowego, sieci, poczty,	Zabezpieczenia informatyczne
Umowy serwisowe	Procedury: Umowy powierzenia, SLA, kary umowne	Zabezpieczenia zewnętrzne
Procedury napraw w serwisach zewnętrznych	Procedury: procedury napraw w serwisach zewnętrznych	Zabezpieczenia zewnętrzne
Outsourcing	Zabezpieczenia: korzystanie z hostingu	Zabezpieczenia zewnętrzne

Arkusz analiza ryzyka

P-Prawdopodobieństwo incydentu (skala od 1 do 3), S-Skutki wystąpienia incydentu (skala od 1 do 3), R-Ryzyko wystąpienia incydentu (skala od 1 do 9), Formuła: R=P*S

Zagrożenie	Opis zagrożenia	P	S	R	Zabezpieczenie
Phishing, cybersquatting (podrabianie stron)	• mail z prośbą o zalogowanie się (pod pretekstem weryfikacji danych lub informowanie o próbie włamania na konto) do „podróbki" strony, np. bankowej, lub pseudo konta gmail i w rezultacie przejęcie hasła, • zachęcanie do zalogowania się do podrobionej strony o „wiarygodnym" adresie www. Zamiast logować się do www.mbank.pl logowanie byłoby w www.rnbank.pl.				**Procedura:** • szkolenia personelu, • regulamin ODO. **Zabezpieczenie:** • systemy antywirusowy i antyspamowy, • serwery proxy i bramki filtrujące: o blokada ruchu na podstawie bazy reputacji, o blokada dostępu do określonych stron.
Nakłanianie do wykonania czynności	• mail z dyspozycją przelewu wysłany do księgowej z rzekomego konta „Prezesa", • fax/mail z fakturą od rzekomego „dostawcy" z informacją o zmianie numeru konta bankowego do opłacenia faktur.				**Procedura:** • szkolenia personelu, • regulamin ODO, • wewnętrzny regulamin Wydziału Finansowego dotyczący zasad akceptacji i modyfikacji przelewów.
Instalacja szkodliwego oprogramowania / działanie szkodliwego oprogramowania	Szkodliwe oprogramowanie (backdoory, exploity, exploitpaki, keyloggery). *Najczęściej instalowane są poprzez otwarcie „zainfekowanego" załącznika z maila lub poprzez kliknięcie na zarażoną stronę. Maile takie zachęcają do otwarcia załącznika lub kliknięcia na hiperlink (mail z fakturą do opłacenia, mail z DHL o przesyłce, mail z rzekomym pismem urzędowym). W efekcie możemy zarazić nasz komputer lub wiele komputerów w sieci.* *Działające szkodliwe oprogramowanie może wywołać różnorodne skutki:* • *przejęcie konta pocztowego do wysyłki spamu,* • *użycie przejętych komputerów do ataków DOS,* • *użycie przejętych komputerów do śledzenia haseł użytkowników celem uzyskania dostępu do systemów i plików,* • *użycie przejętych komputerów do uzyskania pełnego dostępu do wewnętrznej sieci i kopiowania danych i baz danych (kradzież).* *Szkodliwe oprogramowanie:* *Wirusy i trojany – instalują się często z nielegalnym oprogramowaniem. Zawierają ukrytą funkcjonalność, działają na szkodę użytkownika.* *Backdoory - instalują się z maili lub z hiperlinków w mailach. Po uruchomieniu umożliwiają intruzowi ponowny dostęp i stałą kontrolę nad komputerem. Taki komputer-zombie może być użyty do wszelkich zachcianek intruza.* *Keyloggery - programy przechwytujące hasła wpisywane na klawiaturze przez użytkownika i oddające je intruzowi.* *Exploity / exploitpaki - oprogramowanie wykorzystujące znane luki w systemach. Uruchomiony pozwala na przejęcie systemu przez intruza.*				**Procedura:** • Szkolenia personelu, • regulamin ODO. **Zabezpieczenie:** • systemy antywirusowy i antyspamowy, • serwery proxy i bramki filtrujące: o skan niebezpiecznej zawartości, o blokada ruchu na podstawie bazy reputacji, o blokada dostępu do określonych stron.

Arkusz analiza ryzyka

Podrzucone nośniki danych	Atakujący pozostawia w biurze lub w dziale księgowości specjalnie przygotowany pendrive z zainstalowanym samouruchamiającym się szkodliwym programem. W wielu przypadkach z CIEKAWOŚCI pracownicy sprawdzają jego zawartość wkładając go do portu USB. W wyniku tego uruchamiają nieświadomie szkodliwe oprogramowanie (backdoory, exploity, exploitpaki, keyloggery).				**Procedura:** • szkolenia personelu, • regulamin ODO. **Zabezpieczenie:** • blokada portów USB na stacjach roboczych, • dopuszczenie do użycia wyłącznie zakwalifikowanych pendrive.
Ataki telefoniczne	• intruz podający się za „naszego informatyka" prosi o podanie hasła pod pretekstem sprawdzania lub naprawy naszego systemu informatycznego, • intruz przedstawia się jako „serwisant Orange lub Netii" naprawiający usterkę i prosi o wejście na określoną stronę internetową w ramach testowania łącza internetowego, • intruz przedstawia się jako inżynier Microsoftu lub programista dostawcy oprogramowania. Podsyła „aktualizację" lub prosi o udostępnienie pulpitu.				**Procedura:** • szkolenia personelu, • regulamin ODO.
Łamanie haseł	Łamanie haseł metodami słownikowymi i siłowymi (brute force): • do baz danych, • do serwera, • do aplikacji www (np. do wordpressa), • do poczty, • do windows na stacjach roboczych, • do routera, • do firewalla.				**Procedura:** • metody i środki uwierzytelnienia (polityka haseł), • szkolenia personelu. **Zabezpieczenia:** • testy penetracyjne.
Łatwo dostępne, łatwe lub standardowe hasła	• ujawnianie haseł, • nieprawidłowe przechowywanie (karteczki, pliki), • stosowanie domyślnych haseł producenta, • stosowanie słownikowych lub popularnych haseł, np. Grazynka1, qwerty, 12345678, • stosowanie jednego hasła do wielu (często wszystkich) systemów.				**Procedura:** • metody i środki uwierzytelnienia (polityka haseł), • szkolenia personelu, **Zabezpieczenia:** • długość hasła – co najmniej 8 znaków, • hasło zawiera duże, małe litery cyfry lub znaki specjalne, • częstotliwość zmiany hasła – 30/90 dni, • mechanizm wymuszenia zmiany hasła, • uwierzytelnianie za pomocą kodu PIN / biometryczne, • uwierzytelnianie do: o aplikacji, o stacji roboczych, o dysku sieciowego, o sieci, o poczty, o smartfona

Arkusz analiza ryzyka

					• testy penetracyjne.
Ataki na sprzęt - Włamania do urządzeń nieaktualizowanych	Ataki na urządzenia sieciowe oraz inne, które działają dzięki umieszczonemu na nich oprogramowaniu (firmware / strowniki). Zagrożenie dla nast. elementów: • routery, • switche, • access pointy, • firewall, • macierz, • dysk NAS, • drukarki i skanery. *Brak aktualizacji tego oprogramowania (firmware) skutkuje podatnością na włamania, kradzież danych, zakłócanie pracy.*				**Procedura:** • procedura zabezpieczenia systemu informatycznego. **Zabezpieczenia:** • testy penetracyjne.
Ataki na sprzęt - Włamania do urządzeń nieodpowiednio skonfigurowanych	Ataki na błędnie skonfigurowany sprzęt lub sprzęt działający z ustawieniami fabrycznymi. Zagrożenie dla nast. elementów: • routery, • switche, • access pointy, • firewall, • macierz, • dyski NAS, • drukarki i skanery. *Błędy konfiguracyjne popełniane przez administratorów mogą ułatwiać hackerom włamanie się do sieci lub urządzenia. Powodem jest najczęściej brak profesjonalnej wiedzy u osób konfigurujących urządzenia. Przykładem jest np. pozostawienie domyślnych haseł lub dostępu do strony konfiguracyjnej routera z poziomu Internetu.*				**Procedura:** • procedura zabezpieczenia systemu informatycznego. **Zabezpieczenia:** • zmiana domyślnych haseł na urządzeniach, • zmiana domyślnej nazwy konta administratora w urządzeniu, • testy penetracyjne.
Ataki na sprzęt - Włamania z użyciem niezabezpieczonych interfejsów lokalnych	Atakujący wpina się do urządzeń IT przez ich niezabezpieczone porty konfiguracyjne (USB, Ethernet lub COM - szeregowe) Zagrożenie dla nast. elementów: • routery, • switche, • firewalle, • macierze, • serwery, • drukarki i skanery. *Administratorzy sieci często pozostawiają te porty niezabezpieczone, co powoduje ryzyko wpięcia się do powyższych urządzeń i ich skonfigurowania przez hakera.*				**Procedura:** • procedura zabezpieczenia systemu informatycznego **Zabezpieczenia:** • dostęp do portów fizycznych (gniazd - np. szeregowy, USB, Ethernet) zabezpieczono hasłem, aby przypadkowa osoba, która podłączy do nich swój komputer nie mogła zmienić konfiguracji, *Zabezpieczenie dostępu do portów fizycznych (np. gniazd szeregowych, USB) za pomocą hasła ma na celu uniemożliwienie dostępu do konfiguracji urządzenia nawet w sytuacji, gdy komuś uda się do niego podłączyć fizyczne. Urządzenie zapyta wówczas o hasło dostępu, podobnie jak w przypadku zdalnej konfiguracji. Domyślnie hasło dostępowe często nie jest wymagane jeżeli mamy bezpośredni dostęp do portów urządzenia, co z punktu widzenia bezpieczeństwa stanowi zagrożenie.*

Arkusz analiza ryzyka

					• umieszczenie krytycznych elementów infrastruktury w zamykanych na klucz szafach serwerowych, • kontrola dostępu do pomieszczeń serwerowni i punktów dystrybucyjnych sieci, • testy penetracyjne.
Ataki na sprzęt - Włamania za pośrednictwem niepotrzebnych usług (np. telnet na routerze)	Atakujący wykorzystuje do włamania usługi sieciowe, których działanie w danym środowisku nie jest wymagane. Zagrożenie dla nast. usług: • DHCP, • DNS, • SSH, • http, • telnet, • FTP, • SMTP, • SNMP. *Urządzenia sieciowe posiadają często włączone wszystkie możliwe usługi sieciowe (DHCP, DNS, SSH, HTTP, telnet, FTP), mimo iż nie wszystkie z nich są potrzebne w danym środowisku. Każda z tych usług jest obsługiwana przez oprogramowanie, które może zawierać błędy.*				**Procedura:** • procedura wykonywania przeglądów i konserwacji, • procedura zabezpieczenia systemu informatycznego. **Zabezpieczenia:** • wyłączenie niepotrzebnych serwisów (ogranicza ilość dziur i możliwość przechwycenia / podsłuchania ruchu lub haseł), • włączone tylko te usługi, które są niezbędne do działania danego środowiska, • monitorowanie aktywnych usług, • skanery podatności (stosowany jest system wykrywania słabości i zagrożeń), • security information and event managment (analityczny system do wykrywania zagrożeń, • testy penetracyjne.
Ataki na oprogramowanie - Wykorzystanie znanych dziur w nieaktualizowanym oprogramowaniu	Atak z wykorzystaniem znanych dziur w niezaktualizowanym oprogramowaniu. Zagrożenie dla programów: • systemy operacyjne na stacjach roboczych, • systemy serwerowe, • przeglądarki www, • Wordpress, Drupal,, <sklepy internetowe>, • Dedykowany CMS, • Adobe, • Flash, • Java. *Istniejące błędy oprogramowania pozwalające na przełamanie zabezpieczeń są upubliczniane po tym, jak producent oprogramowania przygotuje odpowiednią łatę lub aktualizację. Jeżeli nie zainstalujemy tych aktualizacji, narażamy się na atak, np. zdalny dostęp do systemu lub wykonanie złośliwego kodu (instalacja backdoora, exploita, ransomeware).*				**Procedura:** • procedura zabezpieczenia systemu informatycznego, • procedura wykonywania przeglądów i konserwacji. **Zabezpieczenia:** • stosowane jest darmowe/komercyjne oprogramowanie do inwentaryzacji zainstalowanego oprogramowania na stacjach roboczych (serwerach) oraz do kontroli procesu aktualizacji (patche/łatki), • aktualizacja oprogramowania zgodnie z zaleceniami producentów oraz opinią rynkową co do bezpieczeństwa i stabilności nowych wersji (np. aktualizacje, service pack-i, łatki), • skanery podatności (stosowany jest system wykrywania słabości i zagrożeń), • security Information and Event Managment (analityczny system do wykrywania zagrożeń), • testy penetracyjne.
Podsłuch	• podsłuch danych przesłanych drogą mailową, • podsłuch danych podczas korzystania z aplikacji webowych, • podsłuch podczas korzystania z formularzy kontaktowych, • podsłuch podczas zdalnego dostępu do sieci wewnętrznej przez Internet.				**Procedura:** • procedura zabezpieczenia systemu informatycznego. **Zabezpieczenia:** • szyfrowanie poczty wysyłanej (SSL), • szyfrowanie połączeń internetowych SSL/VPN, • szyfrowanie plików (7zip) wysyłanych mailowo,

Arkusz analiza ryzyka

					• ograniczenie fizycznego dostępu do miejsc, gdzie znajdują się nienadzorowane gniazdka sieciowe (np. sale konferencyjne, korytarze), • dezaktywacja nieużywanych gniazd sieciowych przez wypięcie przewodu lub wyłączenie portu na switchu, *Dezaktywacja gniazdek sieciowych, które nie są używane w danym pomieszczeniu przez komputery i drukarki ma na celu uniemożliwienie podpięcia się do nich intruza z własnym laptopem lub urządzeniem szpiegującym. Gniazda nieużywane powinny być odłączone fizycznie od switcha w szafie, lub konfiguracyjnie poprzez wyłączenie zbędnych portów na switchu.* • testy penetracyjne.
Ataki na oprogramowanie – włamania z wykorzystaniem luk typu zero day	Zero-day to błędy w oprogramowaniu, do których autor nie przygotował jeszcze poprawek / aktualizacji. Informacje o nich są sprzedawane i wykorzystywane przez intruzów.				**Procedura:** • procedura zabezpieczenia systemu informatycznego. **Zabezpieczenia:** • oprogramowanie antywirusowe, • testy penetracyjne.
Ataki na oprogramowanie - Włamania z wykorzystaniem najczęstszych błędów programistycznych	*Programiści pisząc programowanie często popełniają te same, znane błędy.* *Przykładowo: możliwość wpisania ujemnej liczby sztuk w formularzu zamówienia, możliwość odgadnięcia numeru zamówienia innego klienta i wpisanie go w pasku adresu przeglądarki w celu wyświetlenia szczegółów.*				**Procedura:** • procedura zabezpieczenia systemu informatycznego. **Zabezpieczenia:** • testy penetracyjne.
Włamania z wykorzystaniem API (interfejsów programistycznych)	*Niektóre aplikacje pozwalają na zdalne zarządzanie nimi przez specjalnie zaprojektowane funkcje/usługi sieciowe. Np. baza danych może pozwalać na podłączenie się do niej administratorowi w celu wykonania prac naprawczych lub backupu. Dostęp ten odbywa się przy użyciu domyślnych loginów i haseł, co stanowi zagrożenie.*				**Procedura:** • procedura zabezpieczenia systemu informatycznego. **Zabezpieczenia:** • zmiana domyślnych loginów i haseł, • wyłączenie zdalnego dostępu, gdy nie jest wymagany, • testy penetracyjne.
Ataki na oprogramowanie - Namierzanie wersji testowych (np. strona www)	*Niektóre aplikacje posiadają swoje kopie utrzymywane do celów testowych. Są one często gorzej zabezpieczone i łatwiej jest się do nich włamać, a mogą zawierać również krytyczne dane ze środowiska produkcyjnego. Przykładem może być kopia serwera wykonana w celu przetestowania nowej wersji aplikacji. Często udaje się je namierzyć wpisując np. zamiast adresu www.strona.pl adres test.strona.pl.*				**Procedura:** • procedura zabezpieczenia systemu informatycznego. **Zabezpieczenia:** • zmiana domyślnych loginów i haseł, • stosowanie tych samych zasad bezpieczeństwa, co do systemów produkcyjnych, • testy penetracyjne.
Skanowanie sieci i usług	*Udostępniane w Internecie serwery, urządzenia sieciowe i aplikacje oraz serwisy www mogą być namierzane przez intruzów poprzez skanowanie adresów IP. Polega to na próbach łączenia się z wszystkimi znanymi usługami w celu sprawdzenia, które z nich są dostępne w naszej sieci i w jakiej wersji. Dzięki temu możliwe jest znalezienie usług nieaktualnych i zawierających błędy.*				**Procedura:** • procedura zabezpieczenia systemu informatycznego. **Zabezpieczenia:** • firewalle, • wyłączanie niepotrzebnych usług na urządzeniach sieciowych i serwerach.
Włamanie do sieci poprzez WIFI	Uzyskanie dostępu do sieci wewnętrznej poprzez włamanie się do sieci bezprzewodowej				**Procedura:** • procedura zabezpieczenia systemu informatycznego. **Zabezpieczenia:** • odseparowanie wifi dla gości/klientów od sieci wewnętrznej. • stosowanie odpowiednich standardów szyfrowania

Arkusz analiza ryzyka

					• stosowanie mocnych haseł dostępowych
Włamanie z sieci zewnętrznej do sieci wewnętrznej	Włamania z zewnątrz poprzez nieodpowiednio zabezpieczone i skonfigurowane punkty styku z Internetem oraz udostępnione w Internecie serwery i aplikacje.				**Procedura:** • procedura zabezpieczenia systemu informatycznego. **Zabezpieczenia:** • sewery i bramki filtrujące: o skan niebezpiecznej zawartości, o blokada ruchu na podstawie bazy reputacji, o blokada dostępu do określonych stron. • firewall/UTM do ochrony dostępu do sieci komputerowej: o firewall sprzętowy, o firewall programowy. • system IDS/IPS do ochrony dostępu do sieci komputerowej, • skanery podatności (stosowany jest system wykrywania słabości i zagrożeń), • security Information and Event Managment (analityczny system do wykrywania zagrożeń, • testy penetracyjne.
Nieuprawniony dostęp do sieci z użyciem hakerskiego urządzenia	Możliwość wpięcia hakerskiego urządzenia do łatwo dostępnych urządzeń sieciowych wewnątrzorganizacyjnych, celem uzyskania dostępu do sieci przez to urządzenie z zewnątrz. Możliwość uruchomienia tzw. wrogiego access pointa w celu przechwycenia klientów sieci bezprzewodowej. Zagrożenie dla nast. elementów: • gniazdka sieciowe w korytarzach, w sali konferencyjnej, • skanery, drukarki na korytarzach, • switche w miejscach dostępnych.				**Procedura:** • procedura zabezpieczenia systemu informatycznego. **Zabezpieczenia:** • okablowanie i elementy sieci są fizycznie zabezpieczone przed ingerencją osób postronnych, • blokada portów USB na stacjach roboczych, • dezaktywacja nieużywanych gniazd sieciowych poprzez wypięcie przewodu lub wyłączenie portu na switchu. *Dezaktywacja gniazdek sieciowych, które nie są używane w danym pomieszczeniu przez komputery i drukarki ma na celu uniemożliwienie podpięcia się do nich intruza z własnym laptopem lub urządzeniem szpiegującym. Gniazda nieużywane powinny być odłączone fizycznie od switcha w szafie, lub konfiguracyjnie poprzez wyłączenie zbędnych portów na switchu.*
Atak ransomeware	Ransomeware - Program do szyfrowania plików. Instaluje się z maili lub z hiperlinków w mailach lub poprzez odwiedziny zainfekowanej strony. Są też znane przypadki infekcji poprzez sieć lokalną. Odszyfrowanie wymaga zapłaty np. 500 USD. Bardzo groźny.	2	3	6	**Procedura:** • procedura zabezpieczenia systemu informatycznego, • procedura tworzenia kopii zapasowych, • szkolenia personelu, • regulamin ODO. **Zabezpieczenia:** • systemy antywirusowy i antyspamowy, • kopie bezpieczeństwa kluczowych danych zabezpieczone przed szyfrowaniem przez ransomeware (np. utrzymanie poza siecią, najlepiej na nośnikach typu taśmy lub utrzymywanie obrazów-kopii wirtualnych serwerów), • serwery proxy i bramki filtrujące: o blokada ruchu na podstawie bazy reputacji,

Arkusz analiza ryzyka

					○ blokada dostępu do określonych stron.
ATAKI MAN-IN-THE-MIDDLE	Zmuszenie komputerów w sieci lokalnej do komunikowania się za pośrednictwem komputera intruza. Umożliwia przechwytywanie i podsłuchiwanie ruchu w sieci.				**Procedura:** • procedura zabezpieczenia systemu informatycznego. **Zabezpieczenia:** • systemy antywirusowe, • testy penetracyjne.
Eskalacja uprawnień	• Zwiększenie uprawnień użytkownika przez wykorzystanie błędów programistycznych, • Przejęcie uprawnień użytkownika zaawansowanego, • Przejęcie uprawnień administratora, • Przejęcie uprawnień systemowych, • Przejęcie innych poświadczeń (certyfikaty elektroniczne, pliki cookies z identyfikatorami sesji).				**Procedura:** • procedura nadawania uprawnień do przetwarzania danych osobowych • procedura wykonywania przeglądów i konserwacji **Zabezpieczenia:** • regularny przegląd logów i uprawnień • monitorowanie logowania na konta administracyjne • testy penetracyjne
Atak DOS/DDOS	Atak na system komputerowy lub usługę sieciową w celu uniemożliwienia działania. Atak dotyczy głownie stron i aplikacji www. Np. wypełnienie i wysłanie kilka milionów razy formularza kontaktowego (za pomocą skryptu) i spowodowanie zapełnienia dysku. *Zmasowany atak pojedynczego atakującego (DOS) lub z wielu komputerów jednocześnie (DDOS) na jakąś stronę www lub na portal, aby ją przeciążyć i „zakorkować".*				**Procedura:** • procedura zabezpieczenia systemu informatycznego **Zabezpieczenia:** • WAF (Web application firewall) • firewall • testy penetracyjne
Nieuprawniony dostęp lub włamanie do pomieszczeń	Dostęp do: • budynków, • pomieszczeń biurowych, • archiwów, • serwerowni, • miejsc przechowywania kopii bezpieczeństwa. Może skutkować: • dostępem do danych w wersji papierowej, • dostępem do plików lub aplikacji lub baz danych, • zainstalowaniem nieautoryzowanych urządzeń do dostępu do sieci wewnętrznej, • kradzieżą komputerów, nośników.				**Procedury:** • polityka kluczy, • polityka kontroli dostępu. **Zabezpieczenia:** • kontrola kluczy zapasowych/kontrola wydawania kluczy/kontrola składowania kluczy, • proceduralne ograniczenie dostępu do pomieszczeń osobom nieupoważnionym (zakaz wstępu), • praca personelu sprzątającego w godzinach pracy i w obecności osób upoważnionych, • rozmieszczenie komputerów/drukarek/xero ograniczające dostęp osób nieupoważnionych, • dostęp osób nieupoważnionych w obecności osoby upoważnionej, • zabezpieczenie dostępu do pomieszczeń (drzwi zamykane na klucz/drzwi ognioodporne/drzwi antywłamaniowe/drzwi zamykane siłownikami), • zabezpieczenie dostępu do serwerowni (drzwi zamykane na klucz/zamki podklamkowe/zamek kodowy/czytnik biometryczny), • zabezpieczenie dostępu do archiwum (drzwi zamykane na klucz/zamek kodowy), • zabezpieczenie dokumentacji/danych w pomieszczeniach (zamknięte niemetalowe szafy/zamknięte metalowe szafy/sejf/skrytki na klucze),

Arkusz analiza ryzyka

					• systemy alarmowe/zabezpieczenia antywłamaniowe (system alarmowy/kraty/ rolety), • ochrona fizyczna obiektu/pomieszczeń (ochrona własna/firma ochroniarska), • system kontroli dostępu (wdrożone strefy ograniczonego dostępu).
Kradzież/zagubienie sprzętu i nośników poza organizacją (jeśli dane osobowe występują na tych nośnikach)	Kradzież / zagubienie: • laptopów, • smartfonów, • pendrive, • dysków wymiennych.				**Procedury:** • regulamin użytkowania komputerów przenośnych, • procedura zabezpieczenia systemu informatycznego. **Zabezpieczenia:** • szyfrowanie laptopów (bitlocker, Veracrypt), • stosowanie szyfrowanych dysków przenośnych, • stosowanie szyfrowanych pendrive, • uwierzytelnianie do urządzeń typu smartfon.
Nieuprawniony dostęp do infrastruktury IT oraz do programów	• brak kontroli nad dostępem do serwera, plików, programów, komputerów, • nadane zbyt wysokie uprawnienia użytkownikom, • dostęp osób nieupoważnionych do kopii bezpieczeństwa, • łatwy dostęp osób nieupoważnionych do danych prezentowanych na monitorach, drukarkach, kserokopiarkach, • niezabezpieczona praca zdalna użytkowników lub serwisu IT.				**Procedury:** • procedura nadawania uprawnień do przetwarzania danych osobowych, • procedura zabezpieczenia systemu informatycznego, • procedura wykonywania przeglądów i konserwacji, **Zabezpieczenia:** • szyfrowanie baz danych, aby hacker lub przypadkowy użytkownik nie „widział" danych w bazie, • „obiegówka" jako system zarządzania uprawnieniami, • program do zarządzania uprawnieniami (np. help desk ze zleceniami administrowania użytkownikami w organizacji), • zarządzanie uprawnieniami – profile użytkowników, • program do monitorowania połączeń i działań administratorów/wsparcia technicznego z zewnątrz, • minimalizacja uprawnień, • separacja obowiązków, • konta firmowe odseparowane od prywatnych, • separacja sieci wewnętrznej od sieci przeznaczonej dla gości (dla wifi i dla Ethernet) np. w salach konferencyjnych, • dopuszczenie do użycia wyłącznie zakwalifikowanych pendrive, • praca terminalowa zabezpieczona VPN • uwierzytelnianie użytkowników z zewnątrz poprzez akceptację wybranych adresów IP • blokada logowania się po kilku błędnie podanych hasłach • systemy DLP (data leak/loss prevention/protection) *Data Loss Prevention* *Ochrona przed utratą danych (DLP) jest konieczna dla zapobiegania przypadkowym i złośliwym wyciekom istotnych danych, takich jak informacje o klientach, dane finansowe, własność intelektualna lub tajemnice handlowe. Każdy taki incydent może*

Arkusz analiza ryzyka

					kosztować miliony złotych, doprowadzając do utraty reputacji i klientów, kar finansowych, a nawet spraw sądowych. *Identyfikowanie, śledzenie i zabezpieczanie wszystkich poufnych informacji: przechowywanych, używanych, a także przesyłanych to prawdziwe wyzwanie dla każdej organizacji. Jest to zadanie coraz trudniejsze z uwagi na wzrastające czynniki ryzyka, do których można zaliczyć: zestresowanych pracowników obawiających się zwolnień, coraz większą mobilność pracowników.* **Procedury:** • procedura nadawania uprawnień do przetwarzania danych osobowych, • procedura zabezpieczenia systemu informatycznego, • procedura wykonywania przeglądów i konserwacji, • szkolenia personelu, • regulamin ODO. **Zabezpieczenia:** • oświadczenia poufności, • zahasłowane wygaszacze ekranu aktywowane po 15 minutach nieaktywności użytkownika, • ustawienie monitorów uniemożliwiające wgląd w dane osób postronnych • polityka czystego ekranu, • filtry polaryzacyjne na monitorach, • drukarki wyposażone w kontrolę wydruków (PIN).
Udostępnianie danych osobom nieupoważnionym z sieci publicznej (przez Internet)	• dostęp do danych osobowych poprzez stronę www bez logowania się, • dostęp do danych osobowych poprzez stronę www po zalogowaniu się (użytkownik może przeglądać dane osobowe innych użytkowników), • dostęp do katalogów udostępnionych pod publicznym adresem IP plików z danymi osobowymi lub kopii bezpieczeństwa (bez logowania się), • udostępnianie plików zaindeksowanych przez roboty google na skutek braku komend chroniących katalogi webowe przez taką indeksacją, • przesłanie lub wydawanie informacji osobie nieupoważnionej.				**Procedura** • procedura wykonywania przeglądów i konserwacji, • regulamin ODO. **Zabezpieczenia** • uwierzytelnianie dostępu do zasobów, • testy penetracyjne, • blokada robotów, • systemy DLP (data leak/loss prevention/protection).
Awarie/uszkodzenia elementów IT	Awarie: • dysków, • stacji roboczych, • urządzeń sieciowych/routerów, • drukarek/skanerów, • serwera.				**Procedury:** • procedura wykonywania przeglądów i konserwacji. **Zabezpieczenia:** • redundancja serwera,

Arkusz analiza ryzyka

					• system do inwentaryzacji sprzętu, • system do zarządzania licencjami, • plan ciągłości działania.
Błąd/awaria oprogramowania	Awarie: • programu kadrowo-płacowego, • poczty, • aplikacji www (np. wordpressa), • bazy danych,				**Procedury:** • procedura wykonywania przeglądów i konserwacji, **Procedury:** • zabezpieczenia techniczne. **Zabezpieczenia:** • wirtualizacja.
Pożar / eksplozja	• pożar obiektu • pożar serwerowni • pożar serwera • zniszczenie serwerowni (np. wybuch gazów technicznych)				**Procedury:** • zabezpieczenia techniczne. **Zabezpieczenia:** • gaśnice, • system ppoż, • serwerownia z materiałów niepalnych, • czujnik dymu w serwerowni, • system gaszenia serwerowni gazami technicznymi.
Zalanie	• zalanie serwerowni • zalanie archiwum (powódź, zalanie z rur)				**Procedury:** • zabezpieczenia techniczne, **Zabezpieczenia:** • podłoga techniczna, • składowanie dokumentacji papierowej na podwyższeniu, • digitalizacja dokumentów archiwalnych.
Przegrzanie/zbyt duża wilgotność	• wysoka temperatura w serwerowni • wysoka wilgotność w archiwum				**Procedury:** • zabezpieczenia techniczne, **Zabezpieczenia:** • klimatyzacja w serwerowni, • powiadamianie administratora systemu informatycznego o alertach temperatury, • monitoring środowiskowy w serwerowni - czujnik temperaturowy, • monitoring środowiskowy w archiwum - czujniki wilgotności.

Arkusz analiza ryzyka

Awaria zasilania	• skoki napięcia • przerwy w dostawie zasilania				**Procedury:** • zabezpieczenia techniczne **Zabezpieczenia:** • sieć stabilizowana, • UPS podtrzymujący zasilanie serwera, • UPS kluczowych elementów systemu IT,
Nieuprawniona modyfikacja/usunięcie	• niezamierzone lub pomyłkowe zmodyfikowanie / usunięcie danych • sfałszowanie danych przez osoby z wewnątrz lub zewnątrz organizacji				**Procedury:** • procedura zabezpieczenia systemu informatycznego **Zabezpieczenia:** • rozliczalność operacji o kluczowe programy/systemy logują operacje tworzenia, zmiany, usuwania rekordu, wglądu w dane, eksportu danych, o każdy użytkownik programu/systemu posiada swój indywidualny login.
Nieuprawnione kopiowanie danych	• kopiowanie danych z katalogów, dysków, baz, programów • kserowanie i robienie zdjęć przez pracownika lub przez osobę obcą				**Procedury:** • procedura zabezpieczenia systemu informatycznego • regulamin ODO **Zabezpieczenia:** • rozliczalność operacji o kluczowe programy/systemy logują operacje tworzenia, zmiany, usuwania rekordu, wglądu w dane, eksportu danych, o każdy użytkownik programu/systemu posiada swój indywidualny login. • blokada portów USB, • blokada funkcji eksportu danych w kluczowych programach/systemach.
Brak/błędy w wykonywaniu kopii bezpieczeństwa	• doraźne lub za rzadkie wykonywanie kopii, • błędy podczas procesu wykonywania kopi, • niemożność odtworzenia kopii ze względu na zmiany w oprogramowaniu.				**Procedury:** • procedura tworzenia kopii zapasowych **Zabezpieczenia:** • wirtualizacja kopii, • wykonywany jest backup serwerów/aplikacji/plików/konfiguracji/licencji/haseł, • backup jest zabezpieczony przed ransomeware, • kopie zapasowe przechowywane są poza serwerownią, • testowanie możliwości odtworzenia kopii, • niszczenie/czyszczenie nośników przed utylizacją.

Arkusz analiza ryzyka

Nieprawidłowe/brak procedur niszczenia nośników z danymi	• wyrzucenie uszkodzonych nośników bez ich zniszczenia, • wyrzucanie dokumentów papierowych na śmietnik lub pozostawienie dokumentów w miejscu publicznym, • wyrzucenie niezniszczonych , HD, pendrive, DVD.				**Procedury:** • utylizacja elektronicznych nośników i wydruków oraz czyszczenie danych. **Zabezpieczenia:** • niszczarki paskowe, niszczarki o podwyższonym standardzie, • niszczenie/czyszczenie nośników przed utylizacją, • firma niszcząca dokumenty.
Nieprawidłowe/brak procedur napraw w serwisach zewnętrznych	• naprawa sprzętu z nośnikami bez umowy lub bez standardu bezpiecznej naprawy.				**Procedury:** • procedura wykonywania przeglądów i konserwacji.
Nieprzestrzeganie procedur	• świadome naruszenie pisemnych lub ustnych procedur np. niewylogowywanie się z systemu, przekazywanie haseł osobom nieupoważnionym, naruszenie polityki czystego ekranu lub czystego biurka, • naruszenia powyżej wskazane na skutek braków w inteligencji lub z powodów niewiedzy.				**Procedury:** • szkolenia personelu, • regulamin ODO.
Pomyłki i błędy administratorów, użytkowników	• udostępnienia katalogów i dysków, serwerów ftp, aplikacji z danymi do powszechnego dostępu przez sieć publiczną –z powodu „ułatwienia pracy" administratorów systemów, • łatwe logowanie się do baz i programów „login admin, hasło admin1", • dostęp do programów testowych (z prawdziwymi danymi osobowymi) bez logowania, • pomyłkowe udostępnienie, wysłanie do złego odbiorcy, błędne zabezpieczenia.				**Procedury:** • procedura zabezpieczenia systemu informatycznego, • szkolenia personelu, • regulamin ODO.
Błędy projektowe/ konfiguracyjne	• błędy programistów prowadzące do udostępniania danych z tworzonych lub administrowanych programów, • niezabezpieczenie danych w katalogach i bazach webowych i przed indeksacją robotów gogle.				**Zabezpieczenie** • procedura zabezpieczenia systemu informatycznego, • zabezpieczenie baz i katalogów webowych przed indeksacją wyszukiwarek.
Brak aktualnej dokumentacji (instrukcji, opisów, dokumentacji technicznej sprzętu i oprogramowania)	• brak instrukcji, opisów, dokumentacji technicznej sprzętu i oprogramowania, • brak instrukcji instalacyjnych i konfiguracyjnych środowiska lub oprogramowania.				**Procedury:** • procedury przywracania

Arkusz analiza ryzyka

	Zagrożenie związane z możliwymi trudnościami w odtworzeniu środowiska i zarządzania nim, gdy np. odejdzie pracownik IT lub będzie on niedostępny podczas krytycznej awarii.				
Nieprawidłowe / brak umowy o współpracy	Nieprecyzyjnie określone odpowiedzialności we współpracy, co stwarza ryzyko braku zabezpieczeń.				**Zabezpieczenia:** • umowa powierzenia • pisemne upoważnienia dla podmiotu współpracującego z jasnymi warunkami bezpiecznej pracy z danymi powierzonymi
Nieprawidłowe / brak umowy gwarancyjnej lub wsparcia serwisowego	*Należy uwzględnić, że umowy wymagają przedłużania, czas reakcji nie oznacza czasu naprawy.*				**Zabezpieczenie** • stosowane są umowy powierzenia • w umowach stosuje się SLA • w umowach stosuje się kary umowne za niewywiązywanie się z realizacji umów • stosowana jest "Procedura napraw w serwisach zewnętrznych"
Upadek firmy outsourcingowej lub dostawczej	• brak zastępstw, np. dla hostingodawcy poczty, dla wsparcia do zakupionej aplikacji, • utrata usługi/aplikacji, którą świadczy pomiot przetwarzający.				**Zabezpieczenie** • redundancja firmy/osoby.
Awaria łączy telekomunikacyjnych	Krytyczne dla administratora świadczącego usługi wymagające „internetu", usługi chmurowe, ISP oraz dostawcy platform SaaS				• redundancja łączy.

Data nadania upoważnienia: .....

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Nr .....

1. Upoważniam Panią/Pana* .....
   zatrudnioną/ego* na stanowisku .....
   w Wydziale ..... w Urzędzie Miejskim w Piszu do dostępu do następujących danych osobowych:
   .....
   .....
   .....
   .....
   - innych, poza ustalonym zakresem, w ramach doraźnych zleconych zadań przez Burmistrza Pisza, jego Zastępcę, Sekretarza Gminy Pisz oraz Naczelnika Wydziału, niezbędnych do realizowania zadań wymienionych w ustawie z dnia 8 marca 1990 o samorządzie gminnym (Dz. U. z 2017 r. poz. 1875 z późn. zm.).

.....
(pieczęć i podpis Administratora/IOD)

2. Identyfikator: .....

3. Okres trwania upoważnienia:
   Upoważnienie obowiązuje do dnia odwołania lub wygasa z chwilą ustania zatrudnienia w Urzędzie Miejskim w Piszu.
4. Osoba upoważniona do przetwarzania danych, objętych zakresem, o którym mowa wyżej, jest zobowiązana do zachowania ich w tajemnicy, również po ustaniu zatrudnienia oraz zachowania w tajemnicy informacji o ich zabezpieczeniu.

.....
(pieczęć i podpis ASI/informatyka)

*) niepotrzebne skreślić

Ewidencja osób upoważnionych do przetwarzania danych osobowych

☐	DRUKUJ UPOW.	Imię	Nazwisko	Stanowisko	Jednostka organizacyjna	Nazwa zbioru danych	Zakres upoważnienia:	Data nadania upoważnienia	Data ustania upoważnienia
☐									
☐									
☐									
☐									
☐									
☐									
☐									
☐									
☐									
☐									
☐									
☐									
☐									
☐									

Rejestr naruszeń ochrony danych osobowych oraz incydentów bezpieczeństwa danych

Opis / okoliczności naruszenia/incydentu	Ilość osób dotknięta naruszeniem/incydentem	Skutki naruszenia/incydentu	Działania zaradcze	Data rozpoczęcia wdrożenia działań	Data zakończenia wdrażania działań	Osoba odpowiedzialna za wdrożenie działań

Załącznik nr 12 do Polityki

Regulamin Ochrony Danych Osobowych w Urzędzie Miejskim w Piszu

Niniejszy regulamin stanowi wykaz podstawowych obowiązków z zakresu przestrzegania zasad ochrony danych osobowych zgodnie z przepisami RODO dla:

- Pracowników
- Współpracowników
- Pracowników podmiotów trzecich, posiadających dostęp do danych osobowych przetwarzanych przez Administratora / Podmiot przetwarzający
- Użytkowników systemów informatycznych z dostępem do danych osobowych przetwarzanych przez Administratora / Podmiot przetwarzający

Każda z w/w osób powinna zapoznać się z poniższym regulaminem oraz zobowiązać się do stosowania zasad w nim zawartych

SPIS TREŚCI

I. ZASADY BEZPIECZNEGO UŻYTKOWANIA SPRZĘTU IT, DYSKÓW, PROGRAMÓW

1. W przypadku, gdy użytkownik przetwarzający dane osobowe korzysta ze Sprzętu IT zobowiązany jest do jego zabezpieczenia przed zniszczeniem lub uszkodzeniem. Przez Sprzęt IT rozumie się: komputery stacjonarne, monitory, drukarki, skanery, ksera, laptopy, służbowe tablety i smartfony.
2. Użytkownik jest zobowiązany zgłosić zagubienie, utratę lub zniszczenie powierzonego mu Sprzętu IT.
3. Samowolne instalowanie otwieranie (demontaż) Sprzętu IT, instalowanie dodatkowych urządzeń (np. twardych dysków, pamięci) lub podłączanie jakichkolwiek niezatwierdzonych urządzeń do systemu informatycznego jest zabronione.
4. Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym (np. klientom, pracownikom innych działów) wglądu do danych wyświetlanych na monitorach komputerowych – **tzw. Polityka czystego ekranu.**
5. Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu (WINDOWS + L) lub wylogować się z systemu bądź z programu.
6. Po zakończeniu pracy, użytkownik zobowiązany jest:
   1) wylogować się z systemu informatycznego, a jeśli to wymagane - następnie wyłączyć sprzęt komputerowy,
   2) zabezpieczyć stanowisko pracy, w szczególności wszelkie nośniki magnetyczne i optyczne na których znajdują się dane osobowe.
7. Użytkownik jest zobowiązany do usuwania plików z nośników/dysków do których mają dostęp inni użytkownicy nieupoważnieni do dostępu do takich plików (np. podczas współużytkowania komputerów).
8. Jeśli użytkownik jest uprawniony do niszczenia nośników, powinien TRWALE zniszczyć sam nośnik lub trwale usunąć z niego dane (np. zniszczenie płyt DVD w niszczarce).
9. Użytkownicy komputerów przenośnych, na których znajdują się dane osobowe lub z dostępem do danych osobowych przez Internet zobowiązani są do stosowania zasad bezpieczeństwa zawartych w Regulaminie użytkowania komputerów przenośnych

II. ZARZĄDZANIE UPRAWNIENIAMI - PROCEDURA ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY

1. Każdy użytkownik (np. komputera stacjonarnego, laptopa, dysku sieciowego, programów w których użytkownik pracuje, poczty elektronicznej) musi posiadać swój własny indywidualny identyfikator (login) do logowania się.
2. Tworzenie kont użytkowników wraz z uprawnieniami (np. komputera stacjonarnego, laptopa, dysku sieciowego, programów w których użytkownik pracuje, poczty elektronicznej) odbywa się na polecenie przełożonych, a wykonywane jest przez Administratora Systemów Informatycznych (ASI)/informatyka.
3. Użytkownik nie może samodzielnie zmieniać swoich uprawnień (np. zostać administratorem Windows na swoim komputerze).
4. Każdy użytkownik musi posiadać indywidualny identyfikator. Zabronione jest umożliwianie innym osobom pracy na koncie innego użytkownika.
5. Zabrania się pracy wielu użytkowników na wspólnym koncie.

6. Użytkownik (np. komputera stacjonarnego, laptopa, dysku sieciowego, programów w których użytkownik pracuje, poczty elektronicznej) rozpoczyna pracę z użyciem identyfikatora i hasła.
7. Użytkownik jest zobowiązany do powiadomienia ASI/informatyka o próbach logowania się do systemu osoby nieupoważnionej, jeśli system to sygnalizuje.
8. W przypadku, gdy użytkownik podczas próby zalogowania się zablokuje system, zobowiązany jest powiadomić o tym ASI/informatyka.
9. Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu lub wylogować się z systemu. Jeżeli tego nie uczyni, po upływie **15** minut system automatycznie aktywuje wygaszacz.
10. Zabrania się uruchamiania jakiejkolwiek aplikacji lub programu na prośbę innej osoby, o ile nie została ona zweryfikowana jako pracownik działu informatyki. Dotyczy to zwłaszcza programów przesłanych za pomocą poczty elektronicznej lub wskazanych w formie odnośnika internetowego.
11. Po zakończeniu pracy, użytkownik zobowiązany jest:
    1) wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy,
    2) zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację oraz nośniki magnetyczne i optyczne, na których znajdują się dane osobowe

III. Polityka haseł

1. Hasła powinny składać się z co najmniej 8 znaków.
2. Hasła powinny zawierać duże litery + małe litery + cyfry lub znaki specjalne.
3. Hasła nie mogą być łatwe do odgadnięcia. Nie powinny być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion i nazwisk osób bliskich, imion zwierząt, popularnych dat, popularnych słów, typowych zestawów: 123456, qwerty.
4. Hasła nie powinny być ujawniane innym osobom. Nie należy zapisywać haseł na kartkach i w notesach, nie naklejać na monitorze komputera, nie trzymać pod klawiaturą lub w szufladzie.
5. W przypadku ujawnienia hasła – należy natychmiast je zmienić.
6. Hasła muszą być zmieniane co 30 dni.
7. Jeżeli system nie wymusza zmiany haseł, użytkownik zobowiązany jest do samodzielnej zmiany hasła.
8. Użytkownik systemu w trakcie pracy w aplikacji może zmienić swoje hasło.
9. Użytkownik zobowiązuje się do zachowania hasła w poufności, nawet po utracie przez nie ważności.
10. Zabrania się używania w serwisach internetowych takich samych lub podobnych haseł jak w systemie komputerowym Urzędu Miejskiego w Piszu zwanego dalej Urzędem..
11. Zabrania się stosowania tego samego hasła jako zabezpieczenia w dostępie do różnych systemów.
12. 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.

IV. Zabezpieczenie dokumentacji papierowej z danymi osobowymi

1. Upoważnieni pracownicy są zobowiązani do stosowania tzw. „**Polityki czystego biurka**". Polega ona na zabezpieczaniu (zamykaniu) dokumentów oraz nośników np. w szafach, biurkach, pomieszczeniach przed kradzieżą lub wglądem osób

nieupoważnionych po godzinach pracy lub podczas ich nieobecności w trakcie godzin pracy.
2. Upoważnieni pracownicy zobowiązani są do niszczenia dokumentów i wydruków w niszczarkach lub utylizacji ich w specjalnych bezpiecznych pojemnikach z przeznaczeniem do bezpiecznej utylizacji.
3. Zabrania się pozostawiania dokumentów z danymi osobowymi poza zabezpieczonymi pomieszczeniami, np. na korytarzach, na kserokopiarkach, drukarkach, w pomieszczeniach konferencyjnych.
4. Zabrania się wyrzucania niezniszczonych dokumentów na śmietnik lub porzucania ich na zewnątrz, np., na terenach publicznych miejskich lub w lesie.

V. ZASADY WYNOSZENIA NOŚNIKÓW Z DANYMI POZA URZĄD

1. Użytkownicy nie mogą wynosić na zewnątrz Urzędu wymiennych elektronicznych nośników informacji z zapisanymi danymi osobowymi bez zgody pracodawcy/zleceniodawcy. Do takich nośników zalicza się: wymienne twarde dyski, pen-drive, płyty CD, DVD, pamięci typu Flash.
2. Dane osobowe wynoszone poza Urząd muszą być zaszyfrowane (szyfrowane dyski, zahasłowane pliki).
3. Należy zapewnić bezpieczne przewożenie dokumentacji papierowej w plecakach, teczkach.
4. Należy korzystać ze sprawdzonych firm kurierskich.
5. W przypadku, gdy dokumenty przewozi pracownik, zobowiązany jest do zabezpieczenia przewożonych dokumentów przed zagubieniem i kradzieżą.
6. W sytuacji przekazywania nośników z danymi osobowymi poza Urząd można stosować następujące zasady bezpieczeństwa:
   1) adresat powinien zostać powiadomiony o przesyłce,
   2) dane przed wysłaniem powinny zostać zaszyfrowane, a hasło podane adresatowi inną drogą,
   3) stosować bezpieczne koperty depozytowe,
   4) przesyłkę należy przesyłać przez kuriera.

VI. ZASADY KORZYSTANIA Z INTERNETU

1. Użytkownik zobowiązany jest do korzystania z Internetu wyłącznie w celach służbowych.
2. Zabrania się zgrywania na dysk twardy komputera oraz uruchamiania jakichkolwiek programów nielegalnych oraz plików pobranych z niewiadomego źródła. Pliki takie powinny być ściągane tylko za każdorazową zgodą osoby upoważnionej do administrowania infrastrukturą IT (np. ASI/informatyk) i tylko w uzasadnionych przypadkach.
3. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z Internetu.
4. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hackerskim, pornograficznym, lub innym zakazanym przez prawo (na większości stron tego typu jest zainstalowane szkodliwe oprogramowanie infekujące w sposób automatyczny system operacyjny komputera szkodliwym oprogramowaniem).
5. Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł.
6. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka) oraz adresu www

rozpoczynającego się frazą "https:". Dla pewności należy „kliknąć" na ikonkę kłódki i sprawdzić, czy właścicielem certyfikatu jest wiarygodny właściciel.

7. Należy zachować szczególną ostrożność w przypadku podejrzanego żądania lub prośby zalogowania się na stronę (np. na stronę banku, portalu społecznościowego, e-sklepu, poczty mailowej) lub podania naszych loginów i haseł, PIN-ów, numerów kart płatniczych przez Internet. Szczególnie tyczy się to żądania podania takich informacji przez rzekomy bank.
8. Zabrania się samowolnego podłączania do komputerów modemów, telefonów komórkowych i innych urządzeń dostępowych (np.: typu BlueConnect, iPlus, OrangeGo). Zabronione jest też łączenie się przy pomocy takich urządzeń z Internetem w chwili, gdy komputer użytkownika podłączony jest do sieci firmowej.

VII. ZASADY KORZYSTANIA Z POCZTY ELEKTRONICZNEJ

1. Przesyłanie danych osobowych z użyciem maila poza Urząd może odbywać się tylko przez osoby do tego upoważnione.
2. W przypadku przesyłania danych osobowych poza Urząd należy wysyłać pliki zaszyfrowane/spakowane (np. programem 7 zip, winzipem, winrarem) i zahasłowane, gdzie hasło powinno być przesłane do odbiorcy telefonicznie, odrębnym mailem lub SMS.
3. W przypadku zabezpieczenia plików hasłem, obowiązuje co najmniej 8 znaków: duże i małe litery i cyfry lub znaki specjalne, a hasło należy przesłać odrębnym mailem lub inną metodą, np. telefonicznie lub SMS-em.
4. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.
5. Zaleca się, aby użytkownik podczas przesyłania danych osobowych mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.
6. **WAŻNE:** Nie otwierać załączników (.zip, .xlsm, .pdf, .exe) w mailach o niezidentyfikowanej tożsamości!!!!! Są to zwykle „wirusy", które infekują komputer oraz często pozostałe komputery w sieci. WYSOKIE RYZYKO BEZPOWROTNEJ UTRATY DANYCH
7. **WAŻNE:** Nie wolno „klikać" na hiperlinki w mailach, gdyż mogą to być hiperlinki do stron z „wirusami". Użytkownik „klikając" na taki hiperlink infekuje komputer oraz inne komputery w sieci. WYSOKIE RYZYKO BEZPOWROTNEJ UTRATY DANYCH
8. Należy zgłaszać ASI/informatykowi przypadki podejrzanych emaili.
9. Użytkownicy nie powinni rozsyłać „niezawodowych" emaili w formie „łańcuszków szczęścia", np. Życzenia Świąteczne adresowane do 230 osób.
10. Podczas wysyłania maili do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości – UDW". Zabronione jest rozsyłanie maili do wielu adresatów z użyciem opcji „Do wiadomości"!
11. Użytkownicy powinni okresowo kasować niepotrzebne maile.
12. Konta pocztowe firmowe są odseparowane od poczty prywatnej.
13. Mail służbowy jest przeznaczony wyłącznie do wykonywania obowiązków służbowych.
14. Zakazuje się wysyłania korespondencji służbowej na prywatne skrzynki pocztowe pracowników lub innych osób.
15. Użytkownicy mają prawo korzystać z poczty mailowej dla celów prywatnych wyłącznie okazjonalnie i powinno być to ograniczone do niezbędnego minimum.
16. Zabrania się użytkownikom poczty elektronicznej konfigurowania swoich kont pocztowych do automatycznego przekierowywania wiadomości na adres zewnętrzny.
17. Korzystanie z maila dla celów prywatnych nie może wpływać na jakość i ilość świadczonej przez użytkownika pracy oraz na prawidłowe i rzetelne wykonywanie przez niego obowiązków służbowych.

18. Przy korzystaniu z maila, użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i prawa autorskiego.
19. Użytkownicy nie mają prawa korzystać z maila w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania.
20. Użytkownik bez zgody pracodawcy/zleceniodawcy nie ma prawa wysyłać wiadomości zawierających dane osobowe dotyczące pracodawcy/zleceniodawcy, jego pracowników, klientów, dostawców lub kontrahentów za pośrednictwem Internetu, w tym przy użyciu prywatnej elektronicznej skrzynki pocztowej.

VIII. Ochrona antywirusowa

1. Użytkownicy zobowiązani są do skanowania plików wprowadzanych z zewnętrznych nośników programem antywirusowym, jeśli system antywirusowy taką funkcje posiada.
2. Zakazane jest wyłączanie systemu antywirusowego podczas pracy systemu informatycznego przetwarzającego dane osobowe.
3. W przypadku stwierdzenia zainfekowania systemu lub pojawienia się komunikatów „np.; Twój system jest zainfekowany!, zainstaluj program antywirusowy", użytkownik obowiązany jest poinformować niezwłocznie o tym fakcie ASI/informatyka lub osobę upoważnioną.

IX. Skrócona instrukcja postępowania w przypadku naruszenia ochrony danych osobowych

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadomienia pracodawcy/zleceniodawcy w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych.
2. Do sytuacji wymagających powiadomienia, należą:
   1) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
   2) niewłaściwe zabezpieczenie Sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych,
   3) nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka, czystego ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek).
3. Do incydentów wymagających powiadomienia, należą:
   1) zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),
   2) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata lub zagubienie danych),
   3) umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych lub sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów lub danych, działanie wirusów i innego szkodliwego oprogramowania).
4. Typowe przykłady incydentów wymagające reakcji:
   1) ślady na drzwiach, oknach i szafach wskazują na próbę włamania,
   2) dokumentacja jest niszczona bez użycia niszczarki,
   3) fizyczna obecność w budynku lub pomieszczeniach osób zachowujących się podejrzanie,
   4) otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe,
   5) ustawienie monitorów pozwala na wgląd osób postronnych w dane osobowe,

6) wynoszenie danych osobowych w wersjach papierowej i elektronicznej na zewnątrz Urzędu bez upoważnienia pracodawcy/zleceniodawcy,
7) udostępnienie danych osobowych osobom nieupoważnionym w formach papierowej, elektronicznej i ustnej,
8) telefoniczne próby wyłudzenia danych osobowych,
9) kradzież, zagubienie komputerów lub CD, twardych dysków, pen-drive z danymi osobowymi,
10) maile zachęcające do ujawnienia identyfikatora i/lub hasła,
11) pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów,
12) hasła do systemów przyklejone są w pobliżu komputera.

X. OBOWIĄZEK ZACHOWANIA POUFNOŚCI I OCHRONY DANYCH OSOBOWYCH

1. Każda z osób dopuszczona do przetwarzania danych osobowych jest zobowiązana do:
   1) przetwarzania danych osobowych wyłącznie w zakresie i celu przewidzianym w powierzonych przez pracodawcę/zleceniodawcę zadaniach,
   2) zachowania w tajemnicy danych osobowych do których ma dostęp w związku z wykonywaniem zadań powierzonych przez pracodawcę/zleceniodawcę,
   3) niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych zadań przez pracodawcę/zleceniodawcę,
   4) zachowania w tajemnicy sposobów zabezpieczenia danych osobowych,
   5) ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych, nieuprawnionym dostępem do danych osobowych oraz przetwarzaniem.
2. Jeśli jest to przewidziane, osoba dopuszczona do przetwarzania odbywa szkolenie z zasad ochrony danych osobowych.
3. Osoby zapoznane z treścią niniejszego Regulaminu zobowiązane są podpisać „Oświadczenie o poufności".
4. Zabrania się przekazywania bezpośrednio lub przez telefon danych osobowych osobom nieupoważnionym lub osobom których tożsamości nie można zweryfikować lub osobom podszywającym się pod kogoś innego.
5. Zabrania się przekazywania lub ujawniania danych osobom lub instytucjom, które nie mogą wykazać się jasną podstawą prawną do dostępu do takich danych.
6. Zabrania się ujawniania na grupach dyskusyjnych, forach internetowych, blogach itp. jakichkolwiek szczegółów dotyczących funkcjonowania Urzędu, w tym informacji na temat sprzętu i oprogramowania, z jakiego korzysta Urząd, oraz informacji kontaktowych innych, niż ogólnodostępne w materiałach zewnętrznych.

XI. POSTĘPOWANIE DYSCYPLINARNE

1. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego Regulaminu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych lub naruszenie zasad współpracy.
2. Postępowanie sprzeczne z powyższymi zobowiązaniami, może też być uznane przez pracodawcę/zleceniodawcę za naruszenie przepisów karnych zawartych w ogólnym Rozporządzeniu PE i RE 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).

Załącznik nr 13 do Polityki

..... Pisz, dnia .....20..... r.

(imię i nazwisko) *(miejscowość, data)*

OŚWIADCZENIE O POUFNOŚCI

Oświadczam, iż zapoznano mnie z przepisami dotyczącymi ochrony danych osobowych, w szczególności ogólnego Rozporządzenia PE i RE 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) oraz odnośnymi wymaganiami Regulaminu Ochrony Danych Osobowych w Urzędzie Miejskim w Piszu.

W szczególności zobowiązuję się do:

- przetwarzania danych osobowych wyłącznie w zakresie i celu przewidzianym w powierzonych przez Administratora zadaniach,
- zachowania w tajemnicy danych osobowych do których mam lub będę mieć dostęp w związku z wykonywaniem zadań powierzonych przez Administratora,
- niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych zadań przez Administratora,
- zachowania w tajemnicy sposobów zabezpieczenia danych osobowych,
- ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych, nieuprawnionym dostępem do danych osobowych oraz przetwarzaniem.

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami może być uznane przez Administratora za naruszenie przepisów Rozporządzenia PE i RE 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).

.....

podpis oświadczającego

Załącznik nr 13 do Polityki

.....

(imię i nazwisko)

Pisz, dnia .....20..... r.

(miejscowość, data)

OŚWIADCZENIE O POUFNOŚCI

Oświadczam, iż zapoznano mnie z przepisami dotyczącymi ochrony danych osobowych, w szczególności ogólnego Rozporządzenia PE i RE 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) oraz odnośnymi wymaganiami Regulaminu Ochrony Danych Osobowych w Urzędzie Miejskim w Piszu.

W szczególności zobowiązuję się do:

- zachowania w tajemnicy danych osobowych w sytuacji dostępu do nich podczas wykonywania czynności zleconych,
- zabezpieczenia tych danych przed dostępem osób nieupoważnionych a następnie przekazanie ich do dyspozycji osób upoważnionych,
- zgłaszania sytuacji (incydentów) naruszenia zasad ochrony danych osobowych Inspektorowi Ochrony Danych lub bezpośredniemu przełożonemu.

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami może być uznane przez Administratora za naruszenie przepisów Rozporządzenia PE i RE 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).

.....

podpis oświadczającego

Lista uczestników szkolenia z zakresu ochrony danych osobowych

Prowadzący: .....

Miejsce i data szkolenia: .....

L.p.	Imię uczestnika	Nazwisko uczestnika	Podpis

Rejestr czynności przetwarzania prowadzony przez Administratora

Na podstawie Art. 30, ust. 1 RODO

c1) opis kategorii osób, których dane dotyczą (nazwa zbioru)	
c2) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych	
a1) imię i nazwisko/nazwa oraz dane kontaktowe administratora	
a2) imię i nazwisko / nazwa oraz dane kontaktowe współadministratorów	
a3) imię i nazwisko lub nazwa oraz dane kontaktowe przedstawiciela administratora	
a4) dane kontaktowe inspektora ochrony danych;	
b) cele przetwarzania	
d1) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione	
d2) kategorie odbiorców w państwach trzecich lub w organizacjach międzynarodowych	
e) nazwa państwa trzeciego lub organizacji międzynarodowej, gdy mają zastosowanie tam przekazania danych osobowych	
f) planowane terminy usunięcia poszczególnych kategorii danych	
g) ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO.	

Rejestr czynności przetwarzania prowadzony przez Podmiot przetwarzający

Na podstawie Art. 30, ust. 2 RODO

A1) nazwa oraz dane kontaktowe podmiotu przetwarzającego	
A2.1) nazwa oraz dane kontaktowe administratora w imieniu którego działa podmiot przetwarzający	*(tu należy wstawić listę klientów, którym świadczone są usługi w oparciu o umowy powierzenia)*
B2.1) opis kategorii przetwarzań dokonywanych w imieniu administratora	*(tu należy wstawić zakres usług outsourcingowych, jakie świadczone są klientom z powyższej listy)*
A2.2) nazwa oraz dane kontaktowe administratora w imieniu którego działa podmiot przetwarzający	*(tu należy wstawić listę klientów, którym świadczone są usługi w oparciu o umowy powierzenia)*
B2.2) opis kategorii przetwarzań dokonywanych w imieniu administratora	*(tu należy wstawić zakres usług outsourcingowych, jakie świadczone są klientom z powyższej listy)*
A4) dane kontaktowe inspektora ochrony danych;	
C1) kategorie odbiorców w państwach trzecich lub w organizacjach międzynarodowych	
C2) nazwa państwa trzeciego lub organizacji międzynarodowej, gdy mają zastosowanie tam przekazania danych osobowych	
D) ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO.	

Procedura audytu

Celem audytów wewnętrznych jest ocena, czy system ochrony danych osobowych jest skutecznie wdrożony i funkcjonuje zgodnie z wymaganiami RODO. Audyty prowadzone są w sposób obiektywny i bezstronny. Przestrzegana jest zasada, że audytorzy nie audytują własnej pracy.

1. Administrator/IOD jest odpowiedzialny za planowanie i przeprowadzanie audytów wewnętrznych z roczną częstotliwością lub częściej.
2. Administrator/IOD opracowuje programy audytów biorąc pod uwagę ważność procesów przetwarzania oraz audytowanych obszarów, jak też wyniki wcześniejszych audytów. Określa on kryteria audytu, jego cel, zakres i ewentualnie metody.
3. Administrator/IOD wyznacza audytora do przeprowadzenia audytu.
4. Audytor jest zobowiązany do przygotowania się do przeprowadzenia audytu, zapoznając się z opisem audytowanego obszaru, stosowanych procedur i wyników poprzednich audytów.
5. Audytor realizuje działania audytowe mające na celu uzyskanie obiektywnych dowodów potwierdzających poprawność realizowanych zadań, procedur, polityk, zabezpieczeń, celów, spełniania wymagań RODO.
6. W przypadku stwierdzenia uchybień mających wpływ na skuteczność działania systemu ochrony danych zgodnego z RODO, audytor identyfikuje tzw. uchybienia lub spostrzeżenia.
7. Wynik audytu zostaje udokumentowany przez audytora i przekazany Administratorowi/IOD.
8. Administrator/IOD dokonuje przeglądu i analizy wyniku audytu oraz decyduje o inicjowaniu działań korygujących, w przypadku zaistnienia poważnych uchybień.

Plan ciągłości działania

SPIS TREŚCI

I. Plan awaryjny odtworzenia systemu informatycznego po awarii krytycznej

1. Zasady postępowania przy odtworzeniu systemu informatycznego w lokalizacji podstawowej
   a) w przypadku stwierdzenia krytycznej awarii serwera podstawowego wszystkie dane uruchamiane są z drugiego serwera zapasowego z podłączeniem redundantnym. ASI odpina serwer podstawowy i sprawdza przyczynę awarii,
   b) po uruchomieniu serwera podstawowego ASI podłącza go do sieci,
   c) przewidywany czas operacji uruchomienia serwera – 2 dni.
2. Zasady postępowania przy odtworzeniu systemu informatycznego w lokalizacji alternatywnej
   a) w przypadku zniszczenia miejsca serwerowni wraz z serwerem, należy zaplanowaną uprzednio lokalizację przeznaczyć na alternatywną serwerownię,
   b) przygotowanie serwerowni wymaga: zapewnienia energii elektrycznej, UPS, łącz telekomunikacyjnych,
   c) ASI jest odpowiedzialny za dostawę serwera zapasowego, jego konfigurację, wgranie danych z kopii zapasowych,
   d) po uruchomieniu serwera ASI podłącza go do sieci,
   e) przewidywany czas operacji uruchomienia serwera zapasowego – 3 dni.

II. Plan awaryjny na wypadek braku zasilania w sieci komputerowej

1. Sieć komputerowa podłączona jest do UPS wyposażonego w baterie wystarczające na ok. 5 godz. pracy.
2. W przypadku dłuższej awarii sieci zasilającej ASI zobowiązany jest do powiadomienia wszystkich użytkowników o konieczności zakończenia pracy w systemach.
3. ASI wykonuje kopie podstawowych danych.
4. Awaria trwająca powyżej 5 godzin wymaga uruchomienia generatora prądu.

III. Plan awaryjny na wypadek utraty dostępu do sieci internet

1. W przypadku niedostępności internetu awarię zgłaszać do TOYA pod numerem 42 633 38 88.
2. W przypadku dłuższej niedostępności internetu, dostęp do zasobów sieci internetowej mają tylko Burmistrz, Sekretarz, Skarbnik, Naczelnik Wydziału Organizacyjnego i Wydział Finansowy (kluczowe stanowiska Urzędu) z firmy Orange Polska S.A.

Instrukcja zarządzania SI - Wykaz zabezpieczeń na dzień: 11.05.2018

1. Regulamin Ochrony Danych Osobowych w Urzędzie Miejskim w Piszu dla pracowników i współpracowników
   - osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych (z Regulaminem ODO),
   - osoby zatrudnione przy przetwarzaniu podpisują stosowne „Oświadczenie o poufności".
2. Szkolenia personelu
   - szkolenia wewnętrzne.
3. Audyty
   - realizowana jest Procedura audytu.
4. Testy penetracyjne
   - realizowane są testy penetracyjne.
5. Procedury przywracania w razie incydentu
   - stosowana jest procedura „Plan ciągłości działania".
6. Polityka kluczy/polityka kontroli dostępu
   - stosowana jest procedura "Polityka kluczy",
   - stosowana jest procedura "Polityka kontroli dostępu",
   - kontrola kluczy zapasowych,
   - zakaz wstępu osób nieupoważnionych,
   - kontrola wydawania kluczy,
   - kontrola składowania kluczy.
7. Dostęp do pomieszczeń i sprzętu
   - ograniczenie dostępu do pomieszczeń, komputerów, drukarek, xero,
   - ograniczenie dostępu do pomieszczeń osobom nieupoważnionym,
   - dostęp w obecności osoby upoważnionej.
8. Zabezpieczenie dostępu do pomieszczeń (w tym biurowych)
   - drzwi zamykane na klucz,
   - drzwi ognioodporne,
   - drzwi antywłamaniowe.
9. Zabezpieczenie dostępu do serwerowni
   - drzwi zamykane na klucz.
10. Zabezpieczenie dostępu do archiwum
    - drzwi zamykane na klucz.
11. Zabezpieczenie dokumentacji w pomieszczeniach
    - zamknięte niemetalowe szafy,
    - zamknięte metalowe szafy,
    - sejf,
    - skrytki na klucze.
12. Systemy alarmowe/zabezpieczenia antywłamaniowe
    - system alarmowy,
    - kraty,
    - rolety.
13. Ochrona fizyczna obiektu / pomieszczeń
    - firma ochroniarska.
14. System ppoż.
    - system ppoż. w obiekcie,
    - system gaszenia serwerowni,
    - gaśnice.
15. Klimatyzacja
    - klimatyzacja w serwerowni.

16. Systemy UPS

- zastosowano UPS podtrzymujący zasilanie serwera,
- zastosowano UPS kluczowych elementów systemu IT.

17. Systemy antywirusowy i antyspamowy

- wersja serwerowa,
- system licencjonowany,
- system aktualizowany online,
- funkcja skanowania poczty,
- funkcja skanowania portów USB,
- wersja na komputery,
- wersja na smartfony,
- system antyspamowy.

18. Bramki filtrujące

- skanowanie niebezpiecznej zawartości,
- blokada dostępu do określonych stron.

19. Systemy firewall, UTM

- firewall/UTM do ochrony dostępu do sieci komputerowej,
- firewall sprzętowy,
- firewall programowy.

20. Active Directory

- system do ochrony dostępu do sieci komputerowej.

21. Monitorowanie zużycia

- stosowany jest systemy monitorujący stan usług i zasobów krytycznych (serwerów/ baz danych/ urządzeń sieciowych)

22. Systemy do inwentaryzacji

- stosowany jest system do inwentaryzacji sprzętu,

23. Szyfrowanie

- szyfrowanie poczty (SSL),
- szyfrowanie połączeń internetowych VPN
- szyfrowanie pendrive,
- szyfrowanie plików (7zip),

24. Hardening

- włączenie szyfrowania,
- zmiana domyślnych haseł,
- wyłączenie niepotrzebnych funkcji i usług.

25. Aktualizacje systemu

- zarządzanie aktualizacjami systemu operacyjnego,
- zarządzanie aktualizacjami aplikacji,
- zarządzanie aktualizacjami przeglądarek internetowych.

26. Backupy i archiwizacja

- stosowana jest "Procedura tworzenia kopii zapasowych",
- wykonywany jest backup serwerów, aplikacji, plików, licencji, haseł,
- niszczenie/czyszczenie nośników przed utylizacją.

27. Rozliczalność operacji

- program/aplikacja posiada mechanizm odnotowywania wykonywania operacji na danych osobowych. Odnotowane i logowane są: tworzenie rekordu/zmiana/usunięcie/wgląd w dane/identyfikator użytkownika dokonującego zmianę,
- każdy użytkownik posiada swój indywidualny login.

28. Postępowanie z nośnikami

- stosowana jest "Procedura postępowania z nośnikami i sprzętem poza Urzędem Miejskim w Piszu",
- stosowany jest "Regulamin korzystania z komputerów przenośnych",
- ograniczono możliwość kopiowania danych na pendrive,
- zastosowano blokadę portów USB do korzystania z pendrive,
- wymuszono użycie szyfrowanych firmowych pendirve.

29. Zabezpieczenie pracy użytkowników

- stosowana jest "Procedura korzystania z internetu",
- stosowana jest "Procedura korzystania z poczty elektronicznej",
- zahasłowane wygaszacze ekranu aktywowane w przypadku nieaktywności użytkownika,
- poufne ustawienie monitorów,
- filtry polaryzacyjne,

30. Wirtualizacja

- stosowana jest wirtualizacja serwerów.

31. Niszczenie nośników

- stosowana jest "Procedura niszczenia nośników",
- niszczarki ścinkowe,
- niszczarki o podwyższonym standardzie,
- niszczenie/czyszczenie nośników przed utylizacją,
- firma niszcząca dokumenty.

32. Zarządzanie uprawnieniami

- stosowana jest "Procedura zarządzania uprawnieniami",
- minimalizacja uprawnień,
- separacja obowiązków,
- zarządzanie uprawnieniami,
- konta firmowe oddzielone od prywatnych.

33. Uwierzytelnianie

- stosowana jest „Polityka haseł"
- długość hasła – co najmniej 8 - znakowe z dużymi i małymi literami i znakami specjalnymi,
- częstotliwość zmiany haseł ustalono na 30 dni,
- wymuszenie zmiany hasła,
- uwierzytelnianie za pomocą kodu PIN,
- hasło na BIOS,
- zapewniono uwierzytelnianie do aplikacji, stacji roboczych, dysków sieciowych, sieci, poczty.

34. Umowy serwisowe

- stosowane są umowy powierzenia
- w umowach stosuje się SLA (Service Level Agreement),
- w umowach stosuje się kary umowne za niewywiązywanie się z realizacji umów.

35. Procedury napraw w serwisach zewnętrznych

- stosowana jest "Procedura napraw w serwisach zewnętrznych".

36. Outsourcing

- korzystanie z ISP (dostawca usług internetowych),
- korzystanie z hostingu poczty, serwera.

Załącznik nr 2
do Zarządzenia Nr 92.18
Burmistrza Pisza
z dnia 23 maja 2018 r.

Instrukcja zarządzania Systemami Informatycznymi – wykaz zabezpieczeń RODO w Urzędzie Miejskim w Piszu

I. Wstęp

Instrukcja stanowi wykaz procedur oraz stosowanych środków technicznych i organizacyjnych mających na celu, zgodnie z 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), zabezpieczyć przetwarzane dane osobowe przed: przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych oraz nieuprawnionym dostępem do danych osobowych.

II. Zabezpieczenia fizyczne

1. Zabezpieczono dostęp do kluczowej infrastruktury w postaci budynków/pomieszczeń biurowych/archiwów/serwerowni, miejsc przechowywania kopii bezpieczeństwa.
2. Wdrożono zasadę dostępu osób nieupoważnionych do miejsc przetwarzania danych wyłącznie w obecności osoby upoważnionej (praca personelu sprzątającego w godzinach pracy i w obecności osób upoważnionych).
3. Rozmieszczenie komputerów, drukarek, xero ogranicza dostęp osób nieupoważnionych.
4. Ograniczenie fizycznego dostępu do miejsc, gdzie znajdują się nienadzorowane gniazdka sieciowe (np. sale konferencyjne, korytarze).
5. Krytyczne elementy infrastruktury zabezpieczono w zamykanych na klucz szafach serwerowych.
6. Rozdzielnie elektryczne zabezpieczono w szafach zamykanych na klucz.
7. Dostęp do pomieszczeń (w tym biurowych) zabezpieczono drzwiami zamykanymi na klucz, drzwiami ognioodpornymi i antywłamaniowymi w serwerowni.
8. Dostęp do serwerowni zabezpieczono drzwiami zamykanymi na klucz zamkami podklamkowymi.
9. Dostęp do archiwum zabezpieczono drzwiami zamykanymi na klucz.
10. Dostęp do dokumentacji, danych w pomieszczeniach zabezpieczono w zamkniętych niemetalowych szafach lub zamkniętych metalowych szafach.
11. Budynki/pomieszczenia chronione są przez system alarmowy, kraty, rolety przeciwwłamaniowe.
12. Zapewniono ochronę obiektu - firma ochroniarska.
13. Wdrożono system kontroli dostępu, kontroli dostępu do pomieszczeń, serwerowni i punktów dystrybucyjnych sieci.
14. Stosowana jest Polityka kluczy, która stanowi **Załącznik nr 1 do** niniejszej **Instrukcji**

III. Zabezpieczenia techniczne

1. Redundantna linia zasilania internetu.
2. Zastosowano UPS podtrzymujący zasilanie serwera, UPS dla kluczowych elementów systemu IT.
3. Serwerownia wyposażona w system gaszenia gazami technicznymi (gaśnica).
4. Klimatyzacja w serwerowni
5. Archiwum - składowanie dokumentacji papierowej na podwyższeniu

IV. Procedura nadawania uprawnień do przetwarzania danych osobowych

Celem procedury jest minimalizacja ryzyka przetwarzania danych przez osoby nieupoważnione.

1. Dostęp do systemu informatycznego (np. stacji roboczej, dysku sieciowego, programu lub aplikacji, poczty elektronicznej) nadawany jest każdemu użytkownikowi w formie indywidualnego identyfikatora (loginu)
2. Każdemu użytkownikowi uprzywilejowanemu (administratorowi) nadawane jest indywidualne konto administracyjne.
3. Nadawanie, zmiana, odbieranie uprawnień użytkownika do zasobów i aplikacji odbywa się na polecenie przełożonych (lub innych osób upoważnionych).
4. Za wykonanie czynności nadawania, zmiany, odbierania uprawnień użytkownikowi odpowiada administrator systemów informatycznych (ASI)/informatyk.
5. Powyższą procedurę wykonuje się:
   1) zgodnie z **Załącznikiem nr 2 do** niniejszej **Instrukcji**,
   2) z użyciem profili użytkowników.
6. Obowiązuje zasada minimalizacji uprawnień.
7. Identyfikator użytkownika po wyrejestrowaniu z systemu informatycznego nie może być przydzielany innej osobie.
8. Użytkowników obowiązuje zasada pracy na własnym koncie. Zabronione jest umożliwianie innym osobom pracy na koncie innego użytkownika. Zasada ta obowiązuje również administratorów systemów.
9. W przypadku pracy z uprawnieniami użytkownika uprzywilejowanego, każdy administrator systemu zobowiązany jest do bieżącej pracy na koncie roboczym. Użycie tzw. konta administracyjnego (np. "root" lub "admin") dopuszczalne jest jedynie w sytuacjach awaryjnych lub podczas poważnych zmian wprowadzanych w administrowanym systemie.
10. Stosowany jest system uwierzytelniania do aplikacji z wykorzystaniem certyfikatu kwalifikowanego lub indywidualnego loginu i hasła.

V. Metody i środki uwierzytelnienia (polityka haseł)

Celem procedury jest zapewnienie, że do systemów informatycznych przetwarzających dane osobowe mają dostęp jedynie osoby do tego upoważnione.

1. Pierwsze (pierwotne) hasło użytkownika nadawane jest przez ASI/informatyka i przekazywane mu w poufny sposób.
2. Użytkownik systemu zobowiązany jest do niezwłocznej zmiany tego hasła.
3. Użytkownik systemu w trakcie pracy w aplikacji może zmienić swoje hasło.
4. W przypadku, gdy użytkownik zapomni hasła, ASI/informatyk nadaje je ponownie, w trybie pierwszego (pierwotnego) ustawienia.
5. Hasła nie mogą być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów.
6. Użytkownik zobowiązuje się do zachowania hasła w poufności, nawet po utracie przez nie ważności.
7. Zabronione jest zapisywanie haseł w sposób jawny oraz przekazywanie ich innym osobom.
8. Standard hasła: hasło co najmniej 8 – znakowe zawierające duże i małe litery, cyfry oraz znaki specjalne, zmieniane co 30 dni. Zmiana hasła jest wymuszana przez system.
9. Zastosowano mechanizm blokady dostępu po 3 próbach nieudanego logowania się.
10. Hasła administracyjne zdeponowane są w opieczętowanej kopercie w zamkniętej skrzynce w serwerowni.
11. W przypadku utraty uprawnień przez osobę administrującą systemem należy niezwłocznie zmienić hasła, do których miała dostęp.
12. W przypadkach awaryjnych (np. nieobecność administratora) hasło może być przekazane decyzją Burmistrza Pisza lub Sekretarza Gminy Pisz osobie zastępującej administratora.
13. Po ustaniu sytuacji awaryjnej, administrator jest zobowiązany do zmiany haseł.

VI. Procedura tworzenia kopii zapasowych

1. Tworzenie kopii bezpieczeństwa zintegrowanego systemu informatycznego

1) Kopie zapasowe danych osobowych tworzone są przez ASI w bibliotekach taśmowych firmy HP z wykorzystaniem oprogramowania HP Data Protektor.
2) Kopie tworzone są z wykorzystaniem urządzenia HP StorageWorks MSL2024 Tape Library zamontowanego w szafie rakowej serwerowni.
3) Kopie danych sporządzane są jako całościowe raz dziennie na koniec dnia pracy.
4) Kopie sporządzane na nośnikach taśmowych przechowywane są maksymalnie przez 30 dni w kasecie urządzenia zamontowanego w szafie serwerowni.
5) Każda taśma opatrzona jest znakiem kodowym umożliwiającym odczyt danych z określonego backupu.
6) Dostęp do kopii ma ASI.
7) Kopie przechowywane są w serwerowni.
8) ASI sprawuje nadzór nad wykonywaniem kopii zapasowych oraz weryfikuje ich poprawność.
9) Niszczenie streamera odbywa się poprzez jego rozmontowanie i zniszczenie taśmy poprzez jej pocięcie.

2. Tworzenie kopii bezpieczeństwa dokumentacji serwera

1) Kopie zapasowe dokumentacji serwera tworzone są w sposób zautomatyzowany w oparciu o procedurę tworzenia kopii bezpieczeństwa ZSI.
2) Kopie bezpieczeństwa sporządzane są także dla dokumentacji gromadzonej na dysku serwera użytkowników.
3) Kopie całościowe sporządzane są raz dziennie na streamerze.
4) Kopie przechowywane są w sejfie w pomieszczeniu serwerowni.
5) Dostęp do kopii ma ASI.
6) ASI sprawuje nadzór nad wykonywaniem kopii zapasowych oraz weryfikuje ich poprawność.

VII. Utylizacja elektronicznych nośników i wydruków oraz czyszczenie danych

1. Podlegające likwidacji uszkodzone lub przestarzałe nośniki, a w szczególności twarde dyski z danymi osobowymi ze stacji roboczych i laptopów, pendrive, pamięci flash, dyski SSD, płyty DVD, telefony komórkowe, smartfony są niszczone w sposób fizyczny zgodnie z Protokołem zniszczenia uszkodzonych nośników komputerowych, którego wzór stanowi **Załącznik nr 5 do** niniejszej **Instrukcji**. Stosowana metoda niszczenia, to fizyczne niszczenie (pocięcie, nawiercenie, młotkowanie) wymontowanych nośników, użycie degaussera, zmielenie w specjalistycznej firmie potwierdzone protokołem zniszczenia lub certyfikatem bezpieczeństwa firmy utylizacyjnej lub nagraniem z procesu transportu
i utylizacji.
2. Nośniki informacji zamontowane w sprzęcie IT, a w szczególności twarde dyski muszą być wyczyszczone specjalistycznym oprogramowaniem zanim zostaną przekazane poza obszar Urzędu Miejskiego w Piszu zwanego dalej Urzędem (np. sprzedaż lub darowizna komputerów stacjonarnych, laptopów, smartfonów).
3. Dokumentacja papierowa niszczona jest w niszczarkach paskowych oraz tam, gdzie to wymagane w niszczarkach o podwyższonym standardzie (cięcie ścinkowe, niszczenie płyt DVD) zgodnie z protokołem usunięcia danych osobowych, którego wzór stanowi **Załącznik nr 6 do** niniejszej **Instrukcji**.
4. Dokumentacja papierowa niszczona jest za pośrednictwem firmy niszczącej dokumenty. Firma zobowiązana jest do wykazania się bezpieczną procedurą utylizacji (np. powinna posiadać certyfikat ISO27001), nagraniem z procesu transportu i utylizacji

VIII. Procedura zabezpieczenia systemu informatycznego

1. Bezpieczeństwo przetwarzania danych poza Urzędem

1) Użytkownicy komputerów przenośnych wynoszonych poza obszar Urzędu, na których są przetwarzane dane osobowe są zobowiązani do przestrzegania zasad bezpieczeństwa i potwierdzenia, że zapoznali się z Regulaminem użytkowania komputerów przenośnych, który stanowi **Załącznik nr 3 do** niniejszej **Instrukcji**.
2) Stosuje się szyfrowanie dysków komputerów przenośnych zawierających dane osobowe, jeśli wynoszone są poza obszar Urzędu.
3) Dane osobowe na komputerach przenośnych wynoszonych poza obszar Urzędu muszą być przechowywane na zaszyfrowanych partycjach.
4) Dyski przenośne, pendrive wynoszone poza Urząd muszą być zaszyfrowane.
5) Sprzęt mobilny (smartfony/tablety) zabezpieczono mechanizmem uwierzytelniania.
6) Sprzęt mobilny wyposażony jest w oprogramowanie umożliwiające jego nadzór, blokowanie dostępu, czyszczenie zawartości.
7) W przypadku użycia komputerów przenośnych lub sprzętu mobilnego do zdalnego dostępu do zasobów wewnętrznej sieci przez Internet, stosuje się szyfrowanie tego połączenia z użyciem VPN.
8) W przypadku użycia komputerów przenośnych lub sprzętu mobilnego do zdalnego dostępu do zasobów wewnętrznej sieci przez Internet uwierzytelnienia dokonuje się z użyciem loginu i podania.

2. Ochrona przed nieautoryzowanym dostępem do sieci lokalnej

Stosowane zabezpieczenia mają na celu zabezpieczenie systemów informatycznych przed nieautoryzowanym dostępem do sieci lokalnej np. przez programy szpiegujące, hackerów.

1) Dokonuje się aktualizacji oprogramowania (firmware, sterowniki) urządzeń sieciowych oraz innych (np. w urządzeniach jak: routery, switche, access pointy, firewalle, dyski NAS, drukarki, skanery).
2) Dokonywana jest konfiguracja urządzeń sieciowych oraz innych (routery, switche, access pointy, firewalle, dyski NAS, drukarki, skanery) w celu zabezpieczenia przed nieuprawnionym dostępem do nich (np. zmiana domyślnych haseł na urządzeniach, zmiana domyślnych nazw kont administratora w urządzeniach, konfiguracja portów na routerze).
3) Dokonuje się aktualizacji oprogramowania systemów i aplikacji (systemy operacyjne na stacjach roboczych, systemy operacyjne serwerów, przeglądarki www, Adobe, Flash, Java). Aktualizacja dokonywana jest zgodnie z zaleceniami producentów oraz opinią rynkową co do bezpieczeństwa i stabilności nowych wersji (np. aktualizacje, service pack-i, łatki)
4) Przeprowadza się monitoring usług sieciowych, (np. DHCP, DNS, SSH, http, telnet, FTP, SMTP), utrzymuje się niezbędne usługi oraz dezaktywuje pozostałe.
5) Zastosowano system antywirusowy na serwerze i na stacjach roboczych.
6) Zastosowano filtr antyspamowy.
7) Stosowany jest Firewall programowy na serwerze, na stacjach roboczych i na wirtualnym serwerze.
8) Zastosowano mechanizmy kontroli dostępu do sieci w technologii NAT.
9) Zastosowano blokadę dostępu do określonych stron internetowych.
10) Sieć bezprzewodową zabezpieczono technologią WPA.
11) Separacja sieci wewnętrznej od sieci przeznaczonej dla gości (dla wifi) np. w salach konferencyjnych.
12) Zabezpieczenie baz i katalogów webowych przed indeksacją wyszukiwarek.
13) Zastosowano systemy DLP - Ochrona przed wyciekami informacji.

3. Zabezpieczenia infrastruktury IT

1) Zapewniono redundantne łącze internetowe.
2) Serwer wyposażono w macierz dyskową w celu ochrony danych osobowych przed skutkami awarii pamięci dyskowej.
3) Zastosowano wirtualizację serwera.
4) Zastosowano redundantny serwer.
5) Zastosowano blokadę portów na urządzeniach sieciowych i stacjach roboczych.
6) Zabezpieczono dostęp do portów fizycznych (gniazd - np. szeregowych, USB, Ethernet) celem uniemożliwienia zmian konfiguracji przez osoby nieupoważnione.
7) Dokonano dezaktywacji nieużywanych gniazd sieciowych (np. przez wypięcie przewodów lub wyłączenie portów na switchu).
8) Dopuszczono do użycia wyłącznie zakwalifikowane pendrive wraz z blokadą dopuszczenia pozostałych.
9) Na stacjach roboczych zastosowano „zahasłowane wygaszacze ekranu", aktywowane po 15 minutach nieaktywności użytkownika
10) Ustawienie monitorów uniemożliwiające wgląd w dane przez osoby postronne.
11) Zabezpieczenie monitorów filtrami polaryzacyjnymi.

4. Zabezpieczenia aplikacji

1) Zapewniono rozliczalność operacji dla pracy w kluczowych aplikacjach, bazach, serwerach plików.
2) W ramach rozliczalności logowane są operacje tworzenia, zmiany (historii zmian), usuwania rekordu, eksportu danych do plików.
3) Kluczowe aplikacje/bazy z danymi osobowym zabezpieczono przed eksportem danych do plików (np. txt, .csv, .xls).
4) Zabezpieczono interfejsy programistyczne poprzez zmianę domyślnych loginów i haseł, wyłączenie dostępu zdalnego, gdy nie jest wymagany.
5) Zabezpieczenie testowych wersji aplikacji poprzez zmianę domyślnych loginów i haseł, wyłączenie dostępu zdalnego, gdy nie jest wymagany.
6) Stosuje się szyfrowanie poczty wychodzącej(SSL).
7) Dla aplikacji webowych stosowane jest szyfrowanie połączeń internetowych z użyciem protokołu SSL.
8) Formularze kontaktowe na stronach www zabezpieczono protokołem SSL.

IX. Procedura wykonywania przeglądów i konserwacji

1. Stosowane jest oprogramowanie do inwentaryzacji infrastruktury IT zainstalowanego oprogramowania na stacjach roboczych (serwerach) oraz do kontroli procesu aktualizacji (patche, łatki).
2. Stosowany jest system do monitoringu aktywności użytkowników.
3. ASI/informatyk jest odpowiedzialny za monitoring/przegląd logów aktywności aplikacji/baz.
4. ASI/informatyk jest odpowiedzialny za monitoring/przegląd logów aktywności oraz uprawnień użytkowników i administratorów.
5. ASI/informatyk odpowiada za optymalizację zasobów serwerowych, wielkości pamięci i dysków, optymalizację baz danych.
6. ASI/informatyk odpowiada za sprawdzanie poprawności działania systemu IT, w tym: stacji roboczych, serwerów, drukarek, baz danych, aplikacji, poczty email.
7. ASI/informatyk odpowiada za identyfikację i przyjmowanie zgłoszeń o nieprawidłowościach w działaniu systemu informatycznego oraz oprogramowania celem ich niezwłocznego usunięcia.
8. W przypadku napraw dokonywanych na zewnątrz należy zastosować się do procedury napraw w serwisach zewnętrznych, która stanowi **Załącznik nr 4 do** niniejszej **Instrukcji**.
9. W przypadku naprawy sprzętu z danymi osobowymi na nośniku - rekomendowane jest zawarcie specjalnego zapisu w umowie serwisowej, gwarantującego bezpieczną naprawę (należy na to zwrócić uwagę przy zakupach sprzętu).
10. W przypadku naprawy sprzętu z danymi osobowymi na nośniku - rekomendowane jest przekazywanie do naprawy uszkodzonego sprzętu z danymi zaszyfrowanymi na dysku/karcie pamięci. Sprzęt przekazywany jest do serwisu bez podania hasła.
11. Rekomendowane jest korzystanie z serwisu, który dokonuje napraw u klienta (umowy gwarancyjne on-site).
12. Czynności konserwacyjne i naprawcze wykonywane przez osoby nieposiadające upoważnień do przetwarzania danych (np. specjalistów z firm zewnętrznych) muszą być wykonywane pod nadzorem osób upoważnionych.
13. Wszelkie prace konserwacyjne i naprawcze sprzętu komputerowego oraz uaktualnienia systemu informatycznego wykonywane przez podmiot zewnętrzny, powinny odbywać się na zasadach określonych w szczegółowej umowie z uwzględnieniem klauzuli dotyczącej ochrony danych.

Polityka kluczy

1. Polityka kluczy obejmuje budynki i pomieszczenia w Urzędzie Miejskim w Piszu przy ul. Gustawa Gizewiusza 5 i Placu Daszyńskiego 7.
2. Obowiązuje pięciodniowy tydzień pracy, od poniedziałku do piątku, w godzinach 06:00 – 22:00.
3. Upoważnienia do pobierania kluczy do pomieszczeń wydziałów lub komórek organizacyjnych mają wyłącznie osoby upoważnione przez Naczelników wydziałów zwanych dalej Naczelnikami lub Koordynatorów, upoważnienie wymaga wprowadzenia osoby do ewidencji, prowadzonej w Wydziale Organizacyjnym, której wzór stanowi **Załącznik do Polityki kluczy**.
4. Klucze do pomieszczeń w godzinach pracy pozostają pod osobistym nadzorem osób upoważnionych i pobierane są z sekretariatu lub Wydziału Organizacyjnego.
5. Klucze do pomieszczeń pobierane i zdawane są z depozytora typu SAIK KEY w sekretariacie. Każdorazowe pobranie i zdanie kluczy odnotowane jest w oprogramowaniu dostarczonym wraz z depozytorem. Dostęp do oprogramowania depozytora posiada Wydział Organizacyjny.
6. Burmistrz, Zastępca Burmistrza i Sekretarz Gminy, mają dostęp do wszystkich kluczy pomieszczeń. Naczelnicy i Koordynatorzy mają dostęp do kluczy podległych im pomieszczeń.
7. Uprawnienia do kluczy nadaje Wydział Organizacyjny na wniosek Burmistrza Naczelnikowi, Sekretarzowi Gminy lub Koordynatorowi, a pracownikom Naczelnik lub Koordynator.
8. Klucze do pomieszczeń szczególnie chronionych jak serwerowni, Wydziału Spraw Obywatelskich, Promocji i Turystyki, Urzędu Stanu Cywilnego przy Placu Daszyńskiego 7 pozostają pod osobistym nadzorem osób upoważnionych. Dostęp osób trzecich do tych pomieszczeń odbywa się pod ścisłym nadzorem osób upoważnionych.
9. Klucze zapasowe przechowywane są w Wydziale Organizacyjnym. Wydawanie kluczy zapasowych upoważnionym pracownikom może odbywać się tylko w uzasadnionych sytuacjach oraz w przypadkach awaryjnych za zgodą osób uprawnionych. Klucze zapasowe po ich wykorzystaniu należy niezwłocznie zwrócić do depozytu.
10. Klucze służące do zabezpieczenia biurek i szaf muszą być jednoznacznie opisane.
11. W godzinach pracy klucze pozostają pod nadzorem pracowników, którzy ponoszą pełną odpowiedzialność za ich należyte zabezpieczenie.
12. Zabrania się pozostawiania kluczy w drzwiach, biurkach i szafach podczas chwilowej nieobecności osób upoważnionych w pomieszczeniu.
13. Po zakończeniu pracy, klucze służące do zabezpieczenia biurek i szaf muszą być przechowywane w zabezpieczonym miejscu.
14. Po zakończeniu pracy, pracownicy są zobowiązani do zabezpieczenia pomieszczeń, a w szczególności wyłączenia i zabezpieczenia urządzeń elektronicznych oraz elektrycznych, wyłączenia oświetlenia, zabezpieczenia i zamknięcia okien, drzwi.
15. Naruszenie zasad polityki kluczy może spowodować wyciągnięcie konsekwencji wynikających z art. 52 ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. z 2018 r. poz. 108 z późn. zm.).

Załącznik do Polityki kluczy

Ewidencja dostępu do pomieszczeń

L.p.	Nazwisko i imię pracownika	Budynek-nr pomieszczenia	Limity czasowe (w godz. od – do)	Data przyznania pozwolenia	Data anulowania pozwolenia	Podpis Naczelnika Wydziału
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
16						
17						
18						
19						
20						

Zatwierdził na podstawie upoważnień uzyskanych od kierownictwa: .....

Procedura nadawania uprawnień do przetwarzania danych osobowych.

Celem procedury jest minimalizacja ryzyka przetwarzania danych przez osoby nieupoważnione.

1. Dostęp do systemu informatycznego (np. stacji roboczej, dysku sieciowego, programu lub aplikacji, poczty elektronicznej) nadawany jest każdemu użytkownikowi w formie indywidualnego identyfikatora (loginu).
2. Każdemu użytkownikowi uprzywilejowanemu (administratorowi) nadawane jest indywidualne konto administracyjne.
3. Nadawanie, zmiana, odbieranie uprawnień użytkownika do zasobów i aplikacji odbywa się na polecenie przełożonych (lub innych osób upoważnionych).
4. Za wykonanie czynności nadawania, zmiany, odbierania uprawnień użytkownikowi odpowiada ASI/informatyk.
5. Powyższą procedurę wykonuje się:
   a) zgodnie z **Załącznikiem do Procedury**,
   b) z użyciem profili użytkowników.
6. Obowiązuje zasada minimalizacji uprawnień.
7. Identyfikator użytkownika po wyrejestrowaniu z systemu informatycznego nie może być przydzielany innej osobie.
8. Użytkowników obowiązuje zasada pracy na własnym koncie. Zabronione jest umożliwianie innym osobom pracy na koncie innego użytkownika. Zasada ta obowiązuje również administratorów systemów.
9. W przypadku pracy z uprawnieniami użytkownika uprzywilejowanego, każdy administrator systemu zobowiązany jest do bieżącej pracy na koncie roboczym. Użycie tzw. konta administracyjnego (np. "root" lub "admin") dopuszczalne jest jedynie w sytuacjach awaryjnych lub podczas poważnych zmian wprowadzanych w administrowanym systemie
10. Stosowany jest system uwierzytelniania do aplikacji wewnętrznych takich jak PUMA, Legislator, Płatnik, JPK i zewnętrznych Źródło, CEIDG, GUS, UOKIK, SRPP, PFRON, ePUAP, US, z wykorzystaniem certyfikatu kwalifikowanego lub indywidualnego loginu i hasła.

Załącznik do Procedury

ZLECENIE
NADANIA, MODYFIKACJI, ANULOWANIA ZAKRESU UPRAWNIEŃ

☐ **Nowy użytkownik**	☐ **Modyfikacja uprawnień**	☐ **Anulowanie uprawnień w systemie informatycznym**

Imię i nazwisko użytkownika	**Wydział/samodzielne stanowisko**

Opis zakresu uprawnień użytkownika w systemie informatycznym

P – przeglądanie/drukowanie; **Z** – zmiana; **D** – dopisanie; **U** – usuwanie; **N** – zakładanie nowych kont/aktualizacja Planu Kont; **O/Z** – otwarcie/zamknięcie miesiąca/roku; **A** – archiwizowanie

*) zakreślić odpowiednio krzyżykiem

Uprawnienia	**P**	**Z**	**D**	**U**	**N**	**O/Z**	**A**

Data wystawienia:	**Podpis bezpośredniego przełożonego użytkownika systemu:**
	Akceptacja ASI/informatyk

Regulamin użytkowania komputerów przenośnych

1. Każdy Użytkownik komputera przenośnego winien zapoznać się z Regulaminem użytkowania komputerów przenośnych oraz pisemnie zobowiązać się do jego przestrzegania.
2. W przypadku przechowywania na komputerze przenośnym danych osobowych lub stanowiących tajemnicę Pracodawcy, Użytkownik zobowiązany jest do ich przechowywania na dysku szyfrowanym, zabezpieczonym co najmniej 8 - znakowym hasłem (duże, małe litery, znaki specjalne lub cyfry).
3. Na komputerach przenośnych przeznaczonych do zewnętrznych prezentacji multimedialnych nie powinny, o ile jest to możliwe, znajdować się dane osobowe lub stanowiące tajemnicę Pracodawcy.
4. W przypadku kradzieży lub zgubienia komputera przenośnego, Użytkownik powinien natychmiast powiadomić o tym Administratora/Inspektora Ochrony Danych, zaznaczając jednocześnie, jakiego rodzaju dane były na tym urządzeniu przechowywane.
5. Użytkownik zobowiązany jest do zabezpieczenia komputera przenośnego w czasie transportu, a w szczególności:
   a) zaleca się przenoszenie go w specjalnym futerale,
   b) zabrania się pozostawiania komputera przenośnego w samochodzie podczas postoju w miejscu publicznym bez nadzoru,
   c) podczas jazdy samochodem zaleca się przechowywanie komputera zgodnie z wytycznymi wskazanymi w ubezpieczeniu firmy ubezpieczającej sprzęt komputerowy.
6. W przypadku, gdy komputer przenośny pozostawiony jest w miejscu dostępnym dla osób nieupoważnionych, Użytkownik jest zobowiązany do stosowania kabla zabezpieczającego. W szczególności dotyczy to zabezpieczenia komputera na stanowisku pracy, podczas konferencji, prezentacji, szkoleń, targów itp..
7. W przypadku pozostawiania komputerów przenośnych w biurze zaleca się umieszczanie ich po zakończeniu pracy w zamykanych szafkach.
8. Użytkownik komputera przenośnego jest zobowiązany do regularnego tworzenia kopii bezpieczeństwa danych na serwerze lub na określonych nośnikach (pendrive, CD, DVD). Nośniki z takimi kopiami powinny być przechowywane w bezpiecznym miejscu, z uwzględnieniem ochrony przed dostępem osób niepowołanych.
9. Pracując na komputerze przenośnym w miejscach publicznych i środkach transportu, Użytkownik zobowiązany jest chronić wyświetlane na monitorze informacje przed wglądem osób nieupoważnionych.

Zapoznałem\am się z treścią Regulaminu użytkowania komputerów przenośnych i zobowiązuję się do przestrzegania zasad w nim zawartych.

Czytelny podpis Użytkownika

.....

Procedura napraw w serwisach zewnętrznych

1. ASI/informatyk odpowiada za sprawdzanie poprawności działania systemu IT, w tym: stacji roboczych, serwerów, drukarek, baz danych, aplikacji, poczty email
2. ASI/informatyk odpowiada za identyfikację i przyjmowanie zgłoszeń o nieprawidłowościach w działaniu systemu informatycznego oraz oprogramowania celem ich niezwłocznego usunięcia.
3. W przypadku napraw dokonywanych na zewnątrz z komputerów należy uprzednio wymontować wszelkie nośniki z urządzeń mobilnych karty pamięci, usunąć dane z nośnika z użyciem specjalistycznego oprogramowania.
4. W przypadku naprawy sprzętu z danymi osobowymi na nośniku - rekomendowane jest zawarcie specjalnego zapisu w umowie serwisowej, gwarantującego bezpieczną naprawę (należy na to zwrócić uwagę przy zakupach sprzętu).
5. W przypadku naprawy sprzętu z danymi osobowymi na nośniku - rekomendowane jest przekazywanie do naprawy uszkodzonego sprzętu z danymi zaszyfrowanymi na dysku, karcie pamięci. Sprzęt przekazywany jest do serwisu bez podania hasła.
6. Rekomendowane jest korzystanie z serwisu, który dokonuje napraw u klienta (umowy gwarancyjne on-site).
7. Czynności konserwacyjne i naprawcze wykonywane przez osoby nieposiadające upoważnień do przetwarzania danych (np. specjalistów z firm zewnętrznych) muszą być wykonywane pod nadzorem osób upoważnionych
8. Wszelkie prace konserwacyjne i naprawcze sprzętu komputerowego oraz uaktualnienia systemu informatycznego wykonywane przez podmiot zewnętrzny, powinny odbywać się na zasadach określonych w szczegółowej umowie z uwzględnieniem klauzuli dotyczącej ochrony danych.

Załącznik nr 5 do Instrukcji

Protokół zniszczenia uszkodzonych nośników komputerowych

..... Pisz. dnia .....r.
(akcept powołującego komisję)

Protokół nr .....
zniszczenia uszkodzonych nośników komputerowych

.....
(Wydział Urzędu Miejskiego w Piszu)

Dnia ..... komisja powołana **Zarządzeniem Nr**..... Burmistrza Pisza z dnia .....

w składzie:
1. Przewodniczący - .....
2. Członek - .....
3. Członek - .....

dokonała trwałego zniszczenia nośników komputerowych:

L.p.	Nazwa	Nr ewidencyjny	Sposób zniszczenia	Uwagi

Dokonanie w/w czynności zostaje potwierdzone własnoręcznymi podpisami komisji:

1. .....
2. .....
3. .....

ADMINISTRATOR SYSTEMÓW INFORMATYCZNYCH

.....

komórka organizacyjna

Załącznik nr 6 do Instrukcji

Protokół usunięcia danych osobowych

Dnia ..... komisja powołana **Zarządzeniem Nr**..... Burmistrza Pisza z dnia .....

w składzie:

1. Przewodniczący - .....
2. Członek - .....
3. Członek - .....

dokonała trwałego zniszczenia zbioru danych osobowych o nazwie *(nazwa zbioru)*.

Zniszczenie obejmuje:

- wersję papierową zbioru. Zniszczenia dokonano poprzez *(opisać sposób zniszczenia)*
- bazę danych. Zniszczenia dokonano poprzez *(opisać sposób zniszczenia)*
- kopie bezpieczeństwa. Zniszczenia dokonano poprzez *(opisać sposób zniszczenia)*

Dokonanie w/w czynności zostaje potwierdzone własnoręcznymi podpisami komisji:

1. .....
2. .....
3. .....