ZARZĄDZENIE Nr 591/VII/2017
Burmistrza Gminy Chojna
z dnia 24 lutego 2017 r.

zmieniające zarządzenie dotyczące wdrożenia do stosowania w Urzędzie Miejskim w Chojnie „Polityki Bezpieczeństwa Informacji w Urzędzie Miejskim w Chojnie" i „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Chojnie".

Na podstawie art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r., poz. 992) i § 3, 4, 5 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024) **zarządzam, co następuje:**

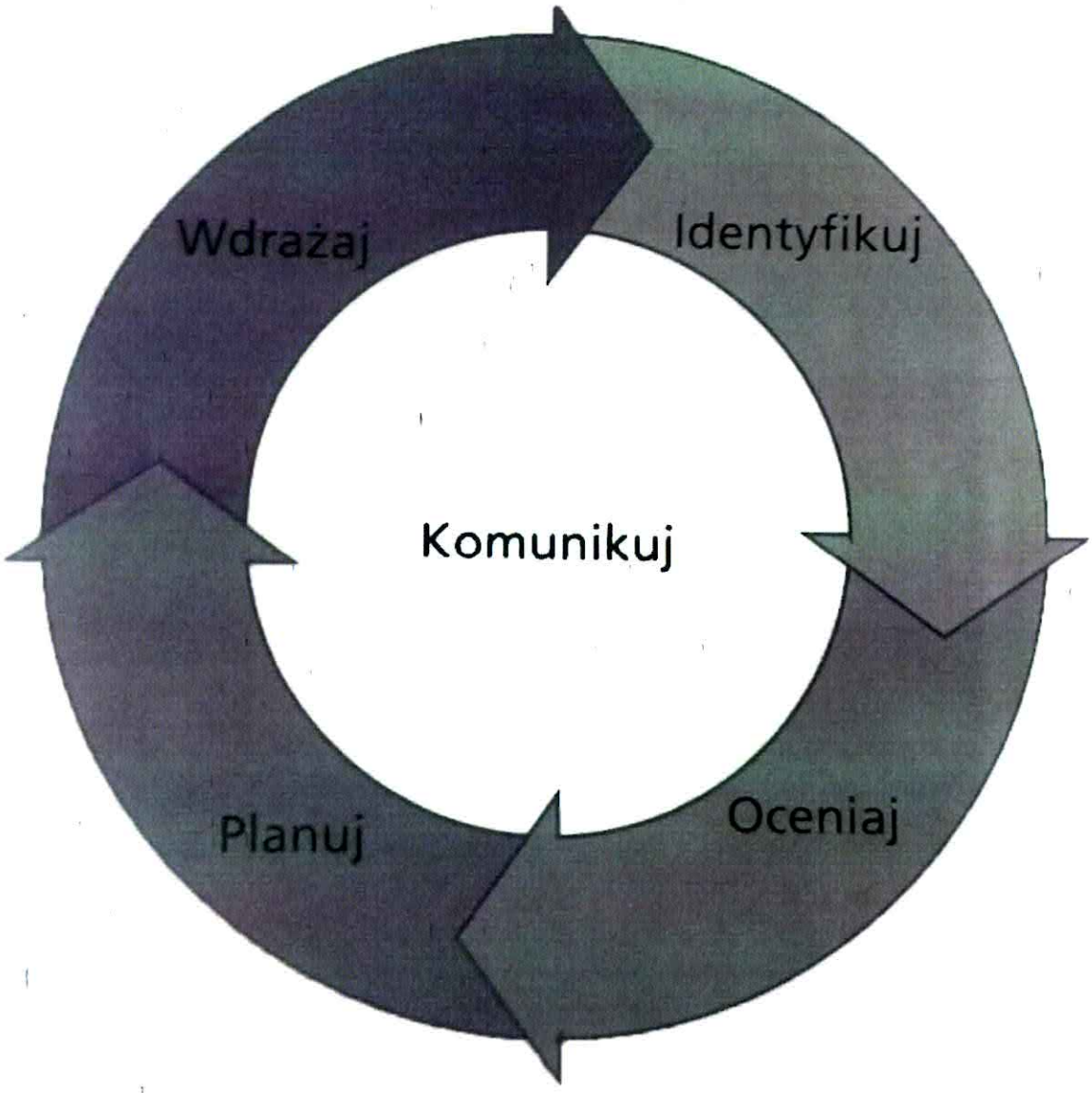
§ 1 W zarządzeniu Nr 1136/VII/2014 Burmistrza Gminy Chojna z dnia 19 września 2016 r. wprowadzą się następujące zmiany:
- § 4 zastępuje się zapisem „ Wykonanie zarządzenia powierzam Zastępcy Burmistrza".

§ 2 W załączniku Nr 1 do zarządzenia wprowadza się następujące zmiany:
- w § 1 uchyla się ust. 3,
- w § 8 ust. 2 w treści dotychczasowy zapis „Administrator, powołuje Administratora Bezpieczeństwa Informacji (ABI) oraz jego zastępcę który" zastępuje się zapisem „Administrator Danych "
- w § 8 uchyla się ust. 3,
- w § 8 ust. 7 w pkt c w treści uchyla się zapis „do ABI",
- w § 8 ust. 7 w pkt f uchyla się na końcu zdania zapis „przekazywanie ABI aktualnej ewidencji tych osób wraz z priorytetami im przydzielonymi",
- w § 8 dotychczasowy ust. 3-6 oznacza się jako 3-5.
-

§ 3 Dotychczasowy Rozdział V zastępuje się zapisem: „Zarządzenie ryzykiem"

„Rozdział V - Zarządzanie ryzykiem"
Ryzyko to niepewne zdarzenie lub zbiór zdarzeń, które w przypadku ich wystąpienia będą mieć wpływ na bezpieczeństwo informacji.
Zarządzanie ryzykiem odnosi się do systematycznego stosowania procedur dotyczących zadań identyfikowania i oceniania ryzyk, a następnie planowania i wdrażania reakcji na nie.

Procedura zarządzania ryzykiem
W Urzędzie stosuje się procedurę zarządzania ryzykiem zalecaną przez metodologię **PRINCE2** obejmującą pięć następujących kroków:
1. Identyfikuj
2. Oceniaj
3. Planuj
4. Wdrażaj
5. Komunikuj



Rys. Procedura zarządzania ryzykiem

Identyfikowanie ryzyk polega na możliwym rozpoznaniu zagrożeń, które mogą wpływać na bezpieczeństwo informacji. W tym celu przyjęto jako podstawową technikę mieszaną, będącą połączeniem technik „przeglądu doświadczeń" oraz „burzy mózgów".
Przegląd doświadczeń opiera się na wiedzy eksperckiej oraz analizie wcześniejszych incydentów związanych z naruszeniem bezpieczeństwa informacji.
Burza mózgów opiera się na myśleniu grupowym, które może być bardziej produktywne niż indywidualne oraz umożliwia zrozumienie poglądów innych interesariuszy na temat zidentyfikowanych ryzyk.
Ocenianie polega na oszacowaniu zagrożeń oraz możliwości ich zmaterializowania w przypadku nie podjęcia odpowiednich działań. Do tego celu wykorzystano „macierz prawdopodobieństwo/wpływ". Zawiera ona wartości niezbędne do sklasyfikowania zagrożeń w ujęciu jakościowym. Skale prawdopodobieństwa są miarami pochodzącymi z wartości procentowych, natomiast skale wpływu są wybrane w celu określenia miary oddziaływania na Urząd.
Planowanie polega na przygotowaniu określonych reakcji zarządczych w celu usunięcia lub zmniejszenia zagrożeń wynikających ze zmaterializowania się określonego ryzyka.

Wprowadza się następujące możliwe reakcje na ryzyko:

1. Unikanie (prewencja)- jeżeli to możliwe podjęcie stosownych reakcji zarządczych tak aby zagrożenie (przypisane do danego ryzyka) nie mogło wpłynąć na bezpieczeństwo informacji lub nie mogło zaistnieć.
2. Redukowanie- działania podjęte w celu zmniejszenia prawdopodobieństwa wystąpienia zdarzenia lub ograniczenia jego wpływu (redukcja jednego lub dwóch parametrów z macierzy prawdopodobieństwo/wpływ).
3. Plan rezerwowy- opracowanie działań, które zostaną podjęte w celu zredukowania skutków zagrożenia dla ryzyka, które się zmaterializowało.

Wdrażanie polega na zapewnieniu, aby planowane reakcje na ryzyko zostały zrealizowane oraz aby podjęte zostały działania korygujące w przypadku gdyby reakcje te nie spełniły związanych z nimi oczekiwań. Istotnym elementem ról i obowiązków w zarządzaniu ryzykiem. Wprowadza się następujące role:

1. Właściciela ryzyka – wskazane stanowisko lub osoba odpowiedzialna zarządzanie, monitorowanie i kontrolowanie wszystkich aspektów przypisanego jej ryzyka łącznie z wdrożeniem wybranych reakcji na zagrożenie.
2. Wykonawca reakcji na ryzyko- stanowisko lub osoba wyznaczona do wykonywania działań związanych z reakcją na konkretne ryzyko. Wykonawca reakcji wspiera właściciela ryzyka i otrzymuje od niego polecenia.

Komunikacja polega na zapewnieniu, aby wszystkie informacje o zagrożeniach docierały do wszystkich zainteresowanych. Jako podstawową formę komunikacji wprowadza się w Urzędzie drogę elektroniczną poprzez pocztę email.

Analiza ryzyka

Identyfikowanie ryzyka

W Urzędzie zidentyfikowano następujące ryzyka:

- włamanie do sieci Urzędu z zewnątrz,
- włamanie do sieci Urzędu z wewnątrz,
- błędy przesyłania, adresowania danych,
- zawodność infrastruktury technicznej,
- podsłuch,
- błędy w oprogramowaniu,
- pogorszenie jakości sprzętu i oprogramowania,
- niepożądany ruch w sieci,
- kopiowanie, podmiana lub niszczenie plików,
- nieświadome udostępnienie informacji,
- świadome udostępnienie informacji,
- klęski żywiołowe.

Prawdopodobieństwo							
	0,9	B. wysokie 71-90%	0.045	0.09	0.18	0.36	0.72
	0,7	Wysokie 51-70%	0.035	0.07	0.14	0.28	0.56 ID:2
	0,5	Średnie 31-50%	0.025	0.05	0.10 ID:7,10	0.20	0.40
	0,3	Niskie 11-30%	0.015	0.03 ID:6	0.06 ID:3	0.12	0.24 ID:1,4,12
	0,1	B. niskie <10%	0.005	0.01 ID:5	0.02 ID:8,9,11	0.04	0.08
			B. mały	Mały	Średni	Duży	B. duży
			0.05	0.1	0.2	0.4	0.8
			Wpływ				

Kolorem czerwonym oznaczono ryzyka:

- włamanie do sieci Urzędu z zewnątrz,
- włamanie do sieci Urzędu z wewnątrz,
- zawodność infrastruktury technicznej,
- pogorszenie jakości sprzętu i oprogramowania,
- nieświadome udostępnienie informacji,
- klęski żywiołowe.

Kolorem zielonym oznaczono ryzyka:

- podsłuch,
- błędy w oprogramowaniu.

Kolorem fioletowym oznaczono ryzyka:

- błędy przesyłania, adresowania danych,
- niepożądany ruch w sieci,
- kopiowanie, podmiana lub niszczenie plików,
- świadome udostępnienie informacji.

Rejestr ryzyk

LP.	Zdarzenie	Skutek	P	W	Reakcja	Działanie	Właściciel ryzyka
1	Nieuprawniony dostęp do systemów IT Urzędu	Utrata integralności, poufności, dostępności informacji	0,3	0,8	Unikanie	Zapewnienie przez ADO środków finansowych niezbędnych do: odpowiedniego zabezpieczenia systemów IT, szkoleń pracowników.	ASI
2	Błędne zaadresowanie informacji	Możliwy dostęp do informacji osób nieuprawnionych	0,3	0,2	Redukowanie	Podniesienie świadomości pracowników.	ADO, ASI, Kierownik wydziału, pracownik
3	Możliwy brak ciągłości pracy systemów IT	Utrudnienia pracy Urzędu i obsługi petentów	0,3	0,8	Redukowanie	Zapewnienie przez ADO odpowiednich środków finansowych, prowadzenie systematycznych przeglądów infrastruktury technicznej.	ADO, ASI
4	Nieuprawniony dostęp do informacji	Utrata poufności informacji	0,1	0,1	Unikanie	Powiadomienie właściwych służb o możliwym zaistnieniu zdarzenia.	ADO, ASI, Kierownik wydziału, pracownik
5	Możliwe wprowadzenie do sieci potencjalnie niebezpiecznych kodów lub aplikacji	Utrata, zniszczenie lub udostępnienie lub części. Niewłaściwa praca systemów.	0,1	0,2	Redukowanie, Unikanie	Monitorowanie ruchu sieciowego	ASI, Kierownik wydziału, pracownik
6	Nieuprawnione udostępnienie lub zniszczenie informacji	Utrata, zniszczenie lub udostępnienie informacji w całości lub części.	0,1	0,2	Redukowanie	Podnoszenie świadomości pracowników	ADO, ASI, Kierownik wydziału, pracownik

7	Przypadkowe udostępnienie informacji	Nieuprawniony dostęp do informacji	0,5	0,2	Redukowanie	Podnoszenie świadomości pracowników	ADO, ASI, Kierownik wydziału, pracownik
8	Celowe udostępnienie informacji	Nieuprawniony dostęp do informacji	0,1	0,2	Unikanie	Podnoszenie świadomości pracowników	ADO, ASI, Kierownik wydziału, pracownik
9	Pożar, powódź, uderzenie pioruna	Zniszczenie infrastruktury, utraty informacji	0,3	0,8	Redukowanie	Opracowanie procedur reagowania, oraz zabezpieczenie budynku Urzędu oraz jego aktywów	ADO, Kierownik jednostki.

P – Prawdopodobieństwo
W – Wpływ

§ 4 Rozdział VI zastępuje się zapisem:
„Rozdział VI – Postępowanie sprawdzające"
W fazie sprawdzania realizowany jest pomiar lub szacowanie wykonania procedur i wymogów polityki bezpieczeństwa. Działania sprawdzające mają poświadczyć, że wdrożone zabezpieczenia funkcjonują efektywnie i zgodnie z zamierzeniami. Jeśli mechanizmy zabezpieczające okażą się nieodpowiednie, należy podjąć działania naprawcze. Celem czynności korygujących jest utrzymanie spójności dokumentacji PBI i niedopuszczenie do narażania instytucji na nieakceptowane ryzyko.
Procedury powinny być wykonywane regularnie w ramach procesu, który pozwali wykryć nieprawidłowości będące wynikiem przetwarzania danych.

§ 5 Dotychczasowy „Rozdał V" i „Rozdział VI" oznacza się jako „Rozdział VII" i „Rozdział VIII".

§ 6 W załączniku nr 2 do zarządzenia wprowadza się następujące zmiany:
- § 5 ust. 1 w treści dotychczasowy zapis „Sekretarz Gminy" zastępuje się zapisem „Zastępca Burmistrza",
- § 5 ust. 1.a i 1.b w treści dotychczasowy zapis „Sekretarz Gminy" zastępuje się zapisem „Zastępca Burmistrza",
- § 5 ust. 5 w treści dotychczasowy zapis „Sekretarz Gminy" zastępuje się zapisem „Zastępca Burmistrza".

§ 7 W załączniku nr 3 do Polityki Bezpieczeństwa Informacji wprowadza się następujące zmiany:
- w § 1 ust. 1 dotychczasowy zapis zastępuje się zapisem „1. Właściciel ZDO tworzy nowy zbiór danych osobowych",
- w § 1 ust. 2 w treści dotychczasowy zapis „ABI" zastępuje się zapisem „Właściciel ZDO",
- w § 1 ust. 3 uchyla się zapis „w uzgodnieniu z ABI",
- w § 1 ust. 4 dotychczasowy zapis zastępuje się zapisem „ASI dokonuje zgłoszenia zbioru danych osobowych do rejestracji GIODO, a ADO podpisuje go podpisem elektronicznym",
- w § 1 uchyla się ust 5., ust. 6 i ust.7,
- w § 1 ust 11. w treści dotychczasowy zapis „ABI przygotowuje" zastępuje się zapisem „Naczelnicy Wydziałów, Kierownicy Referatów, pracownicy na samodzielnych stanowiskach przygotowują",
- w § 1 uchyla się ust 13.
- w § 1 ust. 14 w treści dotychczasowy zapis „Sekretarz Gminy" zastępuje się zapisem „Naczelnik Wydziału, Kierownik Referatu, pracownicy na samodzielnych stanowiskach",
- w § 1 dotychczasowy ust. 5 - 14 oznacza się jako ust. 5 -10.
-

§ 8 W załączniku nr 4 do Polityki Bezpieczeństwa Informacji wprowadza się następujące zmiany:
- w § 1 ust. 1 w treści dotychczasowy zapis „Sekretarz Gminy" zastępuje się zapisem „Zastępca Burmistrza",
- w § 1 ust. 2 w treści dotychczasowy zapis „Sekretarz Gminy" zastępuje się zapisem „Zastępca Burmistrza",

- w § 1 ust. 7 w treści dotychczasowy zapis „Sekretarz Gminy" zastępuje się zapisem „Zastępca Burmistrza",
- w § 3 ust. 1 w treści dotychczasowy zapis „Sekretarz Gminy" zastępuje się zapisem „Zastępca Burmistrza".
- dodaje się § 4 w brzmieniu:

„ § 4 Kryptograficzne zabezpieczenie danych

W przypadku konieczności przeniesienia danych osobowych (np. przy użyciu urządzeń typu Pendrive) w celach ich przetwarzania poza Urzędem, dane należy zaszyfrować.

1. Służbowe telefony komórkowe z systemami Android, iOS, Windows Phone na których możliwie jest przenoszenie lub przetwarzanie danych osobowych, powinny być zaszyfrowane i zabezpieczone hasłem lub numerem PIN.
2. Służbowe laptopy, na których przetwarzane są dane osobowe, powinny mieć zaszyfrowane dyski twarde, odblokowywane przy pomocy hasła podawanego podczas startu systemu,
3. Użytkownicy, wykorzystujący prywatne urządzenia do przenoszenia i przetwarzania danych osobowych powinni zadbać o wydzielenie, lub zaszyfrowanie urządzeń,
4. Wszystkie powyższe działania mają na celu uniknięcie utraty danych na skutek np. zgubienia urządzenia, lub też jego kradzieży.
5. Do szyfrowania wiadomości email należy wykorzystać program GPG, lub w przypadku braku możliwości jego wykorzystania, dane należy spakować jako załącznik zabezpieczony hasłem.
6. Konieczność przeprowadzenia szyfrowania oraz odbycie szkolenia z obsługi programu szyfrującego należy zgłosić ASI".

§ 9 W załączniku nr 5 do Polityki Bezpieczeństwa Informacji wprowadza się następujące zmiany:

- w pkt 6.b w treści dotychczasowy zapis „Sekretarzem Gminy" zstępuje się zapisem „z Zastępcą Burmistrza"
- dodaje się pkt 10 w brzmieniu:

„10) Procedura eksploatacji sprzętu komputerowego

a) ASI prowadzi rejestr wszystkich napraw i wymiany sprzętu komputerowego,
b) w przypadku zużycia sprzętu komputerowego, ASI oznacza go, jako uszkodzony oraz składuje w miejscu niedostępnym dla osób postronnych,
c) w przypadku awarii dysków twardych i pamięci przenośnych, ASI demontuje urządzenie, opisuje je oraz składuje w miejscu niedostępnym dla osób postronnych,
d) w przypadku konieczności utylizacji dysków twardych i innych nośników danych, ASI postępuje zgodnie z Procedurą Utylizacji sprzętu komputerowego, z tą różnicą, że do likwidacji należy wybrać specjalistyczną firmę, zajmującą się utylizacją nośników danych".

§ 9 Wykonanie zarządzenia powierza się Zastępcy Burmistrza.

§ 10 Zarządzenie wchodzi w życie z dniem podpisania

BURMISTRZ

mgr Adam Fedorowicz