

Załącznik Nr 26 do Zarządzenia Nr 150/18

Prezydenta Miasta Szczecin

z dnia 6 kwietnia 2018 r.

Procedura wymiany oraz udostępniania informacji z podmiotami zewnętrznym

§ 1. Ogólne zasady wymiany informacji

1. Przekazanie informacji sklasyfikowanej jako „Wewnętrzne” poza Urząd odbywa się za zgodą Prezydenta Miasta, Sekretarza Miasta oraz kierownika komórki organizacyjnej Urzędu właściwej dla danego rodzaju informacji. Informację wewnętrzną przekazuje pracownik upoważniony do tego przez kierownika komórki organizacyjnej.

2. Informacje wewnętrzne mogą być przekazywane podmiotom zewnętrznym w uzasadnionych przypadkach.

3. Za uzasadniony przypadek uważa się sytuację gdy:

- 1) przekazanie informacji jest niezbędne do realizacji zadań Urzędu, w tym gdy podmiot zewnętrzny świadczy usługi na rzecz Urzędu, a świadczenie tych usług jest uzależnione od dostępu do tych informacji,
- 2) jest to niezbędne do realizacji obowiązków wynikających z regulacji prawnych nałożonych na Urząd,
- 3) wynika to z prawa do dostępu do informacji publicznej zgodnie z Ustawą z dnia 6 września 2001 roku o dostępie do informacji publicznej,
- 4) o przekazanie informacji zwróciła się Policja, Prokuratura, Sąd, CERT lub inne organy w związku z prowadzonym postępowaniem

4. Przekazywanie informacji urzędowych wynika wyłącznie z realizacji obowiązków służbowych.

5. Przekazywane informacje podlegają ochronie w zakresie poufności, integralności oraz autentyczności w sposób adekwatny do przekazywanej informacji, zgodnie z zapisami niniejszej polityki. W szczególności w celu ochrony poufności przekazywanych informacji należy stosować odpowiednie metody kryptograficzne.

6. Osoba przekazująca informację jest zobowiązana do weryfikacji, czy odbiorca jest upoważniony do jej otrzymania. W szczególności obowiązek weryfikacji dotyczy informacji prawnie chronionych, w tym danych osobowych.

7. Urząd wdrożył i utrzymuje narzędzia zapewniające ochronę systemów informatycznych Urzędu służących wymianie informacji przed działaniem złośliwego oprogramowania.

8. Pracownicy Urzędu nie publikują za pośrednictwem serwisów społecznościowych, grup dyskusyjnych, serwisów udostępniających pliki lub komunikatorów informacji dotyczących działalności Urzędu, o ile nie wynika to z zakresu zadań realizowanych na rzecz Urzędu.

9. Preferowanym sposobem wymiany informacji wewnątrz Urzędu jest wykorzystanie systemów elektronicznej wymiany informacji.

10. Dopuszcza się stosowanie przenośnych nośników danych do wymiany informacji, wyłącznie w przypadku, gdy zastosowanie systemów elektronicznej wymiany informacji nie jest możliwe, w szczególności z uwagi na rozmiar danych lub możliwość ich zabezpieczenia. Po ustaniu konieczności korzystania z nośnika przenośnego dane podlegają obowiązkowemu usunięciu.

§ 2. 1. System poczty elektronicznej Urzędu wykorzystywany jest wyłącznie do realizacji obowiązków służbowych.

2. Do wymiany informacji o charakterze służbowym wykorzystywany jest wyłącznie system poczty elektronicznej Urzędu. Zabronione jest korzystanie w tym celu z kont w innych systemach poczty elektronicznej, w tym w systemach publicznie dostępnych.

3. W przypadku, gdy treść otrzymanej wiadomości budzi wątpliwości, użytkownik zobowiązany jest do weryfikacji jej wiarygodności.

4. W przypadku konieczności potwierdzenia faktu otrzymania wiadomości przez adresata stosuje się mechanizm potwierdzenia dostarczenia wiadomości oraz zawiera się w treści wiadomości klauzulę z prośbą o przesłanie potwierdzenia otrzymania wiadomości.

5. System poczty elektronicznej konfiguruje się w sposób zapewniający ograniczenie wielkości przesyłanych wiadomości.

§ 3. W celu dostarczania przez klientów Urzędu dokumentów w postaci elektronicznej, dopuszcza się zastosowanie poniższych kanałów komunikacji:

- 1) poczta elektroniczna.
- 2) forma papierowa.
- 3) nośniki elektroniczne.

2. Nośniki elektroniczne dostarczane przez klientów Urzędu podlegają skanowaniu antywirusowemu.

3. Dokumenty dostarczane za pośrednictwem poczty elektronicznej, platformy ePUAP oraz nośników elektronicznych podlegają automatycznemu skanowaniu przez mechanizmy ochrony antywirusowej.

§ 4. 1. Przekazywanie informacji podmiotom zewnętrznym może wystąpić jedynie w przypadkach, gdy wynika to z potrzeb Urzędu lub z konieczności spełnienia obowiązujących przepisów prawa.

2. W przypadku, gdy wymiana informacji związana jest ze świadczeniem usług na rzecz Urzędu, wymagane jest zapewnienie, poprzez umowę zawartą z podmiotem świadczącym usługi, ochrony poufności przekazanych informacji przed podmiot zewnętrznym oraz należytego ich zabezpieczenia.

3. Wymiana danych osobowych pomiędzy Urzędem, a podmiotem zewnętrznym odbywa się zgodnie z wymaganiami wynikającymi z Ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych. W celu ochrony poufności przekazywanych danych osobowych należy stosować zabezpieczenie hasłem skompresowanego pliku i przekazanie hasła innym kanałem komunikacyjnym.

4. WInf prowadzi ewidencję systemów informatycznych, które realizują wymianę informacji z systemami informatycznymi podmiotów zewnętrznych, wraz ze wskazaniem celu wymiany informacji.

5. W przypadku wymiany informacji z Policją, Prokuraturą, Sądem, CERT i innymi organami wszelkie dane przekazywane są na wniosek ww. organów przekazane za wiedzą i zgodą Prezydenta Miasta lub osoby upoważnionej do wydawania takich decyzji.

6. Przekazywanie informacji w formie papierowej musi odbywać się z zachowaniem rozliczalności oraz poufności przekazywanych informacji. Przekazanie informacji odbywa się protokolarnie (za potwierdzeniem odbioru).

7. Przekazywanie informacji w formie elektronicznej (poczta elektroniczna, elektroniczny nośnik danych) odbywa się z zachowaniem zasad poufności (szyfrowanie danych) oraz rozliczalności.

8. Przekazanie hasła odbywa się innym kanałem komunikacji niż przekazanie ww. informacji.

Z ww. czynności osoba bezpośrednio przekazująca informacje sporządza notatkę/raport i przekazuje Prezydentowi Miasta lub osobie upoważnionej do wydania zgody na przekazanie informacji w jego imieniu.

§ 5. 1. W przypadku konieczności przekazania właściwym organom sprzętu informatycznego WInf:

- 1) zabezpiecza sprzęt przed dostępem osób nieuprawnionych
- 2) wykonuje backup nośnika danych sprzętu podlegającemu przekazaniu zgodnie z obowiązującymi procedurami .
- 3) zabezpiecza nośniki danych z zachowaniem cech poufności, integralności danych zawartych na nośnikach.
- 4) weryfikuje konfiguracje sprzętu na zgodność z kartą sprzętu.
- 5) protokolarnie przekazuje sprzęt (za potwierdzeniem przekazania);
- 6) z przeprowadzonych czynności Dyrektor WInf sporządza lub zleca wykonanie notatki/raportu i przekazuje go Prezydentowi Miasta lub osobie upoważnionej do wydania zgodny na wydanie sprzętu w jego imieniu.

Dokument podpisany bezpiecznym podpisem elektronicznym

Podpis: Signature-1512419735

Imię: PIOTR

Nazwisko: KRZYTEK

Instytucja: URZĄD MIASTA SZCZECIN

Województwo: zachodniopomorskie

Miejscowość: Szczecin

Data podpisu: 6 kwietnia 2018 r.

Zakres podpisu: Cały dokument