ZARZĄDZENIE NR 119/2024
BURMISTRZA SOŚNICOWIC

z dnia 10 lipca 2024 r.

w sprawie wprowadzenia instrukcji tworzenia kopii zapasowych zbiorów danych, oprogramowania oraz systemów służących do przetwarzania danych w Urzędzie Miejskim w Sośnicowicach

Na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04. 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. UE. L. Nr 119, s. 1 ze zm.) zarządzam, co następuje:

§ 1. Instrukcję tworzenia kopii zapasowych zbiorów danych danych, oprogramowania oraz systemów służących do przetwarzania danych w Urzędzie Miejskim w Sośnicowicach określa Załącznik 1 do niniejszego Zarządzenia.

§ 2. Wykonanie zarządzenia powierza się Sekretarzowi Gminy.

§ 3. Zarządzenie wchodzi w życie z dniem podpisania.

Burmistrz Sośnicowic

Bernard Wilczek

Załącznik do zarządzenia Nr 119/2024
Burmistrza Sośnicowic
z dnia 10 lipca 2024 r.

Instrukcja tworzenia kopii zapasowych zbiorów danych danych, oprogramowania oraz systemów służących do przetwarzania danych w Urzędzie Miejskim w Sośnicowicach

1. **Wykonywanie kopii zapasowych.**

1) Zbiory danych w systemie informatycznym są zabezpieczone przed utratą lub uszkodzeniem za pomocą:

   a) urządzeń zabezpieczających przed awarią zasilania lub zakłóceniami w sieci zasilającej,

   b) sporządzania kopii zapasowych zbiorów danych (kopie pełne);

2) Za tworzenie kopii bezpieczeństwa systemu informatycznego odpowiedzialny jest Administrator Systemu Informatycznego lub osoba wyznaczona przez niego;

3) Kopie zapasowe bazy danych wykonywane są mechanizmami bazy, a następnie archiwizowane w oparciu o specjalizowane oprogramowanie. Pełne kopie zapasowe zbiorów danych są tworzone codziennie.

4) Kopie dokumentów z serwerów wykonywane są za pomocą specjalizowanego oprogramowania. Kopie całościowe wykonywane są co tydzień, kopie przyrostowe codziennie.

5) Kopie wykonywane są na dyskach w serwerach backupowych w serwerowni zapasowej.

6) W szczególnych przypadkach – przed aktualizacją lub zmianą w systemie należy bezwarunkowo wykonać pełną kopię zapasową systemu;

7) Kopie zapasowe zbiorów danych należy okresowo sprawdzać pod kątem ich przydatności do odtworzenia w przypadku awarii systemu. Za przeprowadzanie tej procedury odpowiedzialny jest Administrator Systemu Informatycznego lub inna wyznaczona przez niego osoba;

8) Nośniki danych po ustaniu ich użyteczności należy pozbawić danych, zniszczyć w sposób uniemożliwiający odczyt danych, lub przechowywać w bezpiecznym miejscu zabezpieczonym przed dostępem do niego osób niepowołanych;

9) W przypadku komputerów stacjonarnych i przenośnych nie będących własnością Jednostki, użytkownik systemu ma obowiązek sporządzania kopii zapasowych jak również ochrony nośników informacji. Wymaga się

od użytkownika stosowania zasad dotyczących ochrony danych osobowych przed dostępem osób nieuprawnionych;

10) Istnieją kopie programów, które może wykonywać sam użytkownik (z powodu braku automatycznego mechanizmu kopiującego) – wedle zaleceń ASI;

2. **Przechowywanie kopii zapasowych oraz elektronicznych nośników informacji zawierających dane osobowe.**

1) Okresowe kopie zapasowe wykonywane są na macierz NAS. Kopie powinny być przechowywane w innych pomieszczeniach niż te, w których przechowywane są zbiory danych osobowych wykorzystywane na bieżąco. Kopie zapasowe przechowuje się w sposób uniemożliwiający nieuprawnione przejęcie, modyfikacje, uszkodzenie lub zniszczenie;

2) Każdy z egzemplarzy kopii zapasowej powinien być przechowywany w innej lokalizacji, w bezpiecznej odległości od serwerów systemu;

3) Dostęp do nośników z kopiami zapasowymi systemu oraz kopiami danych osobowych ma Administrator Systemów Informatycznych;

4) Kopie zapasowe muszą być opisane w sposób umożliwiający szybką identyfikację.

5) Po upływie okresu ich użyteczności lub przechowywania, dane osobowe powinny zostać skasowane lub zniszczone tak, aby nie było możliwe ich odczytanie.

6) Kopie przechowywane są przez 30 dni (kopie dzienne)

7) W przypadku likwidacji nośników informatycznych zawierających dane osobowe lub kopie zapasowe systemów informatycznych służących do przetwarzania danych osobowych należy przed ich likwidacją usunąć dane osobowe lub uszkodzić je w sposób uniemożliwiający odczyt danych osobowych.

8) Usunięcie danych z systemu powinno zostać zrealizowane przy pomocy oprogramowania przeznaczonego do bezpiecznego usuwania danych z nośnika informacji;

9) W przypadku nośników informacji, przez ich zniszczenie rozumie się ich trwałe i nieodwracalne zniszczenie fizyczne do stanu nie dającego możliwości ich rekonstrukcji i odzyskania danych;

10) W przypadku braku możliwości zrealizowania procedury wewnętrznego zniszczenia nośników informacji, fakt ten należy zgłosić Administratorowi Danych Osobowych; po przekazaniu nośników zostaną one zniszczone w ramach środków technicznych Jednostki bądź poddane procedurze utylizacji

nośników informacji realizowanej przez firmę zewnętrzną, zakończonej sporządzeniem odpowiedniego protokołu utylizacji/zniszczenia.