Załącznik Nr 17 do Zarządzenia Nr 150/18

Prezydenta Miasta Szczecin

z dnia 6 kwietnia 2018 r.

Procedura tworzenia i przechowywania kopii bezpieczeństwa i archiwum danych w Urzędzie Miasta Szczecin

1. Osobą odpowiedzialną za tworzenie kopii bezpieczeństwa i kopii archiwalnych systemu informatycznego jest ASI lub osoba wyznaczona przez Dyrektora WInf.

2. Kopie bezpieczeństwa powinny być tworzone na dedykowanych, odpowiednio zabezpieczonych (poprzez nadmiarowość dysków, redundancję zasilania, itp.) przestrzeniach dyskowych (serwery z wydzielonymi zasobami macierzy dyskowej, dedykowane urządzenia do tworzenia/przechowywania kopii bezpieczeństwa, itp.). Kopie archiwalne powinny być tworzone na nośnikach taśmowych.

3. Kopie bezpieczeństwa wykonywane są z częstotliwością zależną od wielkości zbioru danych podlegających zabezpieczeniu oraz ich wagi krytyczności dla prawidłowego funkcjonowania systemu informatycznego. Do wykonywania kopii bezpieczeństwa wykorzystywane są dedykowane sprzętowe i/lub programowe rozwiązania w zakresie posiadanych przez Urząd licencji i możliwości technicznych.

4. Kopie archiwalne wykonywane są na dedykowanych nośnikach taśmowych, tworzonych w oparciu o dane zapisane w kopiach bezpieczeństwa przy wykorzystaniu rozwiązań programowo - sprzętowych oraz określonych licencji będących w posiadaniu Urzędu.

5. Kopie archiwalne są przechowywane w odpowiednio zabezpieczonym miejscu (szafa pancerna lub sejf) w pomieszczeniu innym niż serwerownia Urzędu. Dostęp do kopii posiadają: ABI, AS oraz osoba odpowiedzialna za wykonywanie kopii. Każde wydanie i przyjęcie kopii jest odnotowywane w rejestrze depozytów. Zabrania się przechowywania kopii zapasowych w pomieszczeniach przeznaczonych do przechowywania zbiorów danych pozostających w bieżącym użytkowaniu. Jednocześnie kopie zapasowe muszą być odpowiednio zabezpieczone fizycznie (sejf ognioodporny w zabezpieczonym pomieszczeniu). Kopie zapasowe mogą być przechowywane tylko w tych pomieszczeniach, w których jest zainstalowany system wykrywania pożaru.

6. Każdy nośnik zawierający kopie archiwalne powinien być opatrzony niepowtarzalnym numerem i etykietką informacyjną zawierającą następujące informacje:

1) zawartość,

2) data zapisu,

3) podpis osoby wykonującej zabezpieczenie.

7. Nośniki wykorzystywane do tworzenia kopii powinny być ewidencjonowane. Przed wykorzystaniem nośnika do innych celów niż kopia archiwalna należy go zainicjować i sprawdzić jego stan.

8. W celu zapewnienia poprawności wykonywanych kopii bezpieczeństwa należy co najmniej raz w tygodniu poddać testowi cyklicznie wybraną kopię. Próba polega na odtworzeniu danych w warunkach testowych i sprawdzeniu, czy jest możliwość odczytania danych.

9. Likwiduje się nośniki zawierające nieaktualne kopie danych, będące poza wykazem cyklicznych kopii. W przypadku nośników jednorazowych, takich jak płyty CD-R, DVD-R, likwidacja polega na ich fizycznym zniszczeniu w taki sposób, by nie można było odczytać ich zawartości. Nośniki wielorazowego użytku, takie jak dyski twarde, płyty CD-RW, DVD-RW, można wykorzystać ponownie do celów przechowywania kopii bezpieczeństwa po uprzednim usunięciu ich zawartości. Nośniki wielorazowego użytku nie nadające się do ponownego użycia należy zniszczyć fizycznie.