Załącznik Nr 1 do Zarządzenia
Nr 14/2006 Starosty Buskiego
z dnia 21 lipca 2006 r.

Załącznik Nr 1 do Zarządzenia
Nr 18/99 Starosty Powiatu Buskiego

INSTRUKCJA

Określająca sposób zarządzania systemem informatycznym w Starostwie Powiatowym w Busku-Zdroju.

1.Za bezpieczeństwo danych osobowych w systemie informatycznym odpowiedzialny jest administrator bezpieczeństwa informacji. Jest on wyznaczony w formie pisemnej przez Administratora Danych.

2.Administrator bezpieczeństwa informacji prowadzi **REJESTR SYSTEMU INFORMATYCZNEGO,** w którym odnotowuje wszystkie fakty dotyczące informacji w systemie.

3.System informatyczny pracuje w sieci lokalnej. Do pracy w sieci każdy użytkownik musi posiadać unikalny identyfikator i hasło nadane przez Administratora bezpieczeństwa informacji. W sieci mogą pracować jedynie osoby upoważnione. Inne osoby mogą towarzyszyć pracownikom upoważnionym do pracy na zbiorach osobowych tylko za zgodą administratora danych lub osoby przez niego upoważnionej.

4.Rejestrowanie nowych użytkowników musi być poprzedzone szkoleniem w zakresie ochrony danych osobowych. Rejestracja jest związana z przydzieleniem użytkownikowi indywidualnej nazwy (identyfikator), hasła, praw dostępu do danych. Zarejestrowanie nowego użytkownika musi być odnotowane w Rejestrze systemu (nazwisko, imię, nazwa użytkownika, prawa dostępu do danych osobowych, data rejestracji, własnoręczny podpis).

5.Wyrejestrowanie użytkownika dokonuje się niezwłocznie po utracie jego uprawnień do danych osobowych. Wyrejestrowanie użytkownika musi być odnotowane w Rejestrze systemu (nazwisko, imię, nazwa użytkownika, aktualne prawa dostępu, data wy rejestrowania, własnoręczny podpis).

6. Rejestracji i wyrejestrowania użytkowników dokonuje Administrator bezpieczeństwa danych lub inna osoba wskazana przez Administratora danych osobowych.
7. System udostępnia dane wyłącznie upoważnionym osobom po podaniu identyfikatora i właściwego hasła.
8. Hasła użytkowników zmieniane są co miesiąc (w pierwszym tygodniu miesiąca).
9. Hasła użytkownika utrzymuje się w tajemnicy, również po upływie ich ważności.
10. Identyfikator użytkownika jest zmienny, a po wy rejestrowaniu użytkownika nie może być przydzielany innym osobom.
11. Czas pracy przy przetwarzaniu zbiorów danych osobowych pokrywa się z czasem pracy Starostwa (poniedziałek - piątek 7:30 - 15:30). Praca poza godzinami wymaga zgody Administratora danych. Fakt taki powinien być odnotowany w Rejestrze systemu. W trakcie przerw w przetwarzaniu danych użytkownicy muszą przerwać pracę w systemie i uniemożliwić innym osobom dostęp do danych osobowych.
12. Stanowiska pracy powinny być tak zorganizowane aby uniemożliwić wgląd lub dostęp do danych osobowych przez osoby nieupoważnione.
13. Stanowiska komputerowe gdzie przetwarza się dane osobowe w systemie informatycznym wyposażone są w oprogramowanie antywirusowe oraz antywłamaniowe którego celem jest zapobieganie nieuprawnionego dostępu do systemu informatycznego.
14. Kopie awaryjne tworzone są po zakończeniu pracy, nie rzadziej niż raz w tygodniu. Częstotliwość tworzenia kopii wynika z czasu dokonywania zmian w zbiorach danych. Kopie awaryjne tworzone są przy użyciu zewnętrznych nośników magnetycznych lub optycznych. Kopie tworzone są na przemian na jednym z pięciu nośników informacji zewnętrznych. Fakt wykonania archiwum odnotowywuje się w rejestrze systemu. Zapis taki powinien zawierać: nazwę archiwum, czas tworzenia, zakres danych. Kopie awaryjne należy sprawdzać pod kątem dalszej przydatności przynajmniej raz w miesiącu. Po okresie przydatności należy je bezzwłocznie usunąć

w sposób uniemożliwiający ich odtworzenie.

15. Nośniki informacji na których wykonuje się kopie awaryjne zastępuje się nowymi minimum jeden raz w okresie 12 miesięcy.
16. System komputerowy gdzie przetwarza się dane osobowe podlega okresowemu przeglądowi minimum jeden raz w okresie 12 miesięcy. W tym struktura nośników informacji podlega sprawdzeniu na wypadek wystąpień uszkodzeń logicznych oraz fizycznych.
17. Przed wykonaniem archiwum należy sprawdzić system pod kątem występowania wirusów przy wykorzystaniu specjalistycznego oprogramowania. W przypadku wykrycia wirusa należy podjąć próbę bezpiecznego usunięcia. Do usuwania należy wykorzystać odpowiednie oprogramowanie zapewniające bezpieczne usunięcie. Po usunięciu należy sprawdzić poprawność danych osobowych oraz ustalić sposób infekcji. W przypadku podejrzenia o uszkodzenie zbioru danych osobowych należy go odtworzyć z ostatniej kopii bezpieczeństwa. O takim fakcie należy powiadomić Administratora danych i zarejestrować to w Rejestrze Systemu.
18. Kopie i wydruki archiwalne przechowywane są w Archiwum Powiatowym.
19. Przeglądy systemu dokonywane są okresowo przynajmniej raz w tygodniu. W trakcie przeglądu analizowane są zbiory plików rejestrowych, odtwarzanie (w razie konieczności) zbiorów indeksów, wyszukiwanie wirusów komputerowych, porządkowanie zbiorów na dysku.
20. Urządzenie, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie.
21. Urządzenie, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do przekazania innemu podmiotowi, nieuprawnionemu do otrzymania danych osobowych, pozbawia się wcześniej zapisu tych danych.
22. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane dane osobowe przeznaczone do naprawy, pozbawia się wcześniej zapisu tych danych albo naprawia się pod nadzorem osoby upoważnionej przez

administratora danych.

23. Przy przekazywaniu danych osobowych konieczne jest zachowanie szczególnej ostrożności.
24. Rejestr wniosków o udostępnienie informacji ze zbioru danych osobowych prowadzony jest w każdym Wydziale przetwarzającym dane osobowe.
25. Stanowiska komputerowe gdzie przetwarza się dane osobowe w systemie informatycznym wyposażone są w zasilacze awaryjne oraz urządzenia eliminujące zakłócenia w sieci zasilającej (np. listwy zasilające z filtrem).