

**w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji
w Urzędzie Gminy w Nowym Korczynie**

Na podstawie art. 3 ust. 1 i art. 36 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity: Dz. U. z 2002 r. Nr 101 poz. 926, ze zm.) oraz 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), **w celu wytyczenia podstawowych zasad i wymagań bezpieczeństwa zasobów informacji, jako filaru bezpieczeństwa realizacji zadań gminy przez Urząd Gminy w Nowym Korczynie, zarządza się co następuje:**

§1

Powołuje się Administratora Bezpieczeństwa Informacji (ABI) którym jest Sekretarz Urzędu Gminy Nowy Korczyn, - osobą odpowiedzialną za ochronę i bezpieczeństwo przetwarzanych danych w tym w szczególności za przeciwdziałanie dostępowi do nich osób niepowołanych oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszenia zabezpieczeń.

§2

Na Administratora Systemów Informatycznych (ASI) wyznacza się Informatyka Urzędu Gminy w Nowym Korczynie odpowiedzialnego za funkcjonowania systemów informatycznych.

§3.

Do zadań Administratora Bezpieczeństwa Informacji należy:

- analiza ryzyka i zarządzanie nim,
- opracowanie planu wdrożenia zabezpieczeń,
- opracowanie treści programów szkoleniowych i prowadzenie szkoleń, prowadzenie działań uświadamiających w urzędzie,
- nadzór nad funkcjonowaniem mechanizmów kontroli dostępu do systemu i jego urządzeń,
- opracowanie planów reakcji na incydenty, planów awaryjnych, regulaminów,
- monitorowanie skuteczności zabezpieczeń, sprawdzanie osiągnięcia celów w zakresie bezpieczeństwa,
- opracowanie Planów Zabezpieczenia Systemów w Urzędzie Miasta i Gminy,
- aktualizacja dokumentów polityki, zwłaszcza wpływu nowelizacji ustaw, rozporządzeń i zawieranych umów na wymagania bezpieczeństwa określone w dokumentach polityki,
- doradztwo dla informatyka i kierownictwa urzędu,
- określanie niezbędnych zasobów (ludzkich, finansowych, wiedzy) potrzebnych do wdrożenia i utrzymania stanu bezpieczeństwa.

§4.

Do zadań Administratora Systemów Informatycznych należy eksploatacja systemów teleinformatycznych zgodnie z polityką bezpieczeństwa. Do szczegółowych zadań należy:

- pomoc przy analizie ryzyka i zarządzaniu ryzykiem,
- monitorowanie zmian środowiska, w tym pojawiania się nowych zagrożeń,
- właściwa konfiguracja mechanizmów kontroli dostępu do systemu i jego urządzeń,
- zarządzanie konfiguracją systemów i urządzeń,
- reagowanie na incydenty w zakresie bezpieczeństwa,
- odpowiedzialność za wdrażanie zabezpieczeń,
- planowanie szkoleń i działań uświadamiających wg ustalonych programów,
- analizowanie incydentów związanych z bezpieczeństwem,
- audyt zabezpieczeń i sprawozdawczość,

§5.

Szczegółowe określenie zadań, o których mowa w § 3 i § 4 zawierają dodatkowe przepisy wewnętrzne, instrukcje i procedury bezpiecznej eksploatacji stanowiące załączniki do niniejszego zarządzenia.

§6.

Administrator Bezpieczeństwa Informacji (ABI) może przekazać Administratorowi Systemów Informatycznych dodatkowe obowiązki w formie pisemnego upoważnienia.

§7.

1. Wszyscy pracownicy Urzędu i Gminy w Nowym Korczynie zobowiązani są do przestrzegania tajemnicy służbowej oraz innych tajemnic chronionych określonych w przepisach szczególnych, co potwierdzają własnoręcznym podpisem na oświadczeniu stanowiącym załącznik nr 1 do niniejszego zarządzenia.
2. Użytkownicy przed dopuszczeniem do pracy w systemach teleinformatycznych urzędu podpisują oświadczenie o zapoznaniu się z zasadami wykorzystania sprzętu teleinformatycznego.
3. Wzór oświadczenia, o którym mowa w pkt. 2 stanowi załącznik nr 2 do niniejszego zarządzenia.
4. Zasady wykorzystania sprzętu teleinformatycznego określa załącznik nr 3 do niniejszego zarządzenia.
5. Osoby z zewnątrz dopuszczone do informacji chronionych w Urzędzie Miasta i Gminy, podpisują zobowiązanie dotyczące zachowania poufności w trybie art. 266 § 1 KK. stanowiącym załącznik nr 4 do niniejszego zarządzenia.

§8

1. Kadra kierownicza urzędu oraz pracownicy, którzy wykonują dodatkowe obowiązki związane z organizacją i kontrolą przestrzegania zasad bezpieczeństwa informacji, powinni prezentować wysoki poziom etyki zawodowej i są zobowiązani do szczególnej staranności w wykonywaniu zadań.
2. Pracownicy mający dostęp do danych osobowych lub informacji niejawnych, powinni być dopuszczeni do nich na zasadach określonych w odpowiednich ustawach i rozporządzeniach wykonawczych.

§9

Użytkownicy uzyskują dostęp do systemów informatycznych po:

- zdobyciu formalnych uprawnień od właściwych przełożonych,
- odbyciu przeszkolenia,
- utworzeniu konta i przyporządkowaniu hasła.

§10

Pracownicy urzędu zobowiązani są do przestrzegania zasad ochrony fizycznej dokumentów i materiałów zawierających informacje chronione w Urzędzie Gminy, polegających na:

- przechowywaniu ich w pomieszczeniach i szafach odpornych na włamania lub zniszczenie na skutek awarii bądź klęsk żywiołowych,
- opracowywaniu ich w strefach bezpieczeństwa,
- obowiązkowego udziału w okresowo organizowanych szkoleniach.

§11

Pracownicy niezaangażowani bezpośrednio w procesy przetwarzania danych chronionych zaliczeni zostają do grupy podwyższonego ryzyka i nie powinni być dopuszczeni do pomieszczeń oraz systemów mających związek z procesami przetwarzania, bez asysty osoby wyznaczonej przez Administratora Bezpieczeństwa Informacji.

§12

1. W celu zapobieżenia nadużyciom, kradzieżom informacji, nośników i innych zasobów, po zakończeniu pracy należy uporządkować swoje stanowisko i zabezpieczyć nośniki oraz dokumenty w specjalnie do tego przeznaczonych szafkach - zasada „czystego biurka”.
2. Ekran monitorów należy usytuować w ten sposób, aby uniemożliwić podgląd osobom trzecim, należy stosować wygaszacze ekranu.
3. Zabrania się wynoszenia sprzętu na zewnątrz bez pozwolenia przełożonego i jego szczegółowej kontroli.

§13

W celu monitorowania incydentów i niesprawności, minimalizacji szkód z nich wynikających i wyciągnięcia wniosków na przyszłość, wprowadza się:

- obowiązek raportowania Administratorowi Bezpieczeństwa Informacji naruszeń (incydentów), zauważonych podatności i innych słabych punktów oraz przypadków błędnego działania sprzętu i oprogramowania,
- obowiązek analizowania przez Administratora Bezpieczeństwa Informacji incydentów i popełnionych błędów, wnioskowanie w powyższych sprawach do Wójta o wyciągnięcie wniosków służbowych.

§14

Wprowadza się „Instrukcję realizacji polityki bezpieczeństwa w zakresie ochrony danych oraz zasady postępowania w sytuacji ich naruszenia w Urzędzie Gminy w Nowym Korczynie” stanowiącą załącznik nr 5 do niniejszego zarządzenia

§15

Wprowadza się „Instrukcję przetwarzania danych osobowych w Urzędzie Gminy w Nowym Korczynie” stanowiącą załącznik nr 6 do niniejszego zarządzenia.

§16

Zobowiązuje się pracowników Urzędu Gminy do zapoznania się z treścią zarządzenia i załączników oraz ich stosowania.

§17

Wykonanie Zarządzenia i nadzór nad wykonaniem zarządzenia powierza się Sekretarzowi Gminy.

§18

Zarządzenie wchodzi w życie z dniem podpisania

WÓJT
inż. Wiktor Kwęś