PROCEDURA ZABEZPIECZANIA DANYCH OSOBOWYCH W POWIATOWYM INSPEKTORACIE WETERYNARII W GŁUBCZYCACH

1. Dla bezpieczeństwa przetwarzania danych stosuje się §20 Rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.

2. W siedzibie Powiatowego Inspektoratu Weterynarii wydzielono strefę bezpieczeństwa klasy I, w której dostęp do informacji zabezpieczony jest wewnętrznymi środkami kontroli.
Są to:
a) pomieszczenie Powiatowego Lekarza Weterynarii, w którym może przebywać wyłącznie PLW oraz inne osoby upoważnione do przetwarzania tylko w towarzystwie PLW, a osoby postronne w ogóle nie mają dostępu. Złożony w odpowiednim miejscu klucz jest zabezpieczony i opisany.
b) pomieszczenie księgowości/kasy z kasą pancerną, w którym mogą przebywać pracownicy księgowości, inni użytkownicy danych tylko w obecności pracowników księgowości, a osoby postronne w ogóle nie mają dostępu. Złożony w odpowiednim miejscu klucz jest zabezpieczony i opisany.

3. W strefie bezpieczeństwa klasy II do danych mają dostęp wszystkie osoby upoważnione do przetwarzania danych zgodnie z zakresami upoważnień do przetwarzania danych, a osoby postronne tylko w obecności pracownika upoważnionego do przetwarzania danych. Strefa ta obejmuje wszystkie pozostałe pomieszczenia zaliczone do obszaru przetwarzania danych w siedzibie Inspektoratu.

4. Wszystkie urządzenia systemu informatycznego są zasilane za pośrednictwem zasilaczy awaryjnych (tzw. UPS-ów).

5. Okablowanie sieciowe zostało zaprojektowane w ten sposób, że dostęp do linii teletransmisyjnych jest możliwy tylko z pomieszczeń zamykanych na klucz. Ponadto kable sieciowe nie krzyżują się z okablowaniem zasilającym, co zapobiega interferencjom.

6. Sieć lokalna podłączona do Internetu oddzielona jest sprzętowym firewallem – FortiGate.

7. Bieżąca konserwacja sprzętu prowadzona jest tylko przez Informatyka – Administratora Systemów Informatycznych (ASI). Natomiast, poważne naprawy wykonane przez personel zewnętrzny realizowane są w siedzibie Inspektoratu.

8. Wszystkie awarie, działania konserwacyjne i naprawy systemów informatycznych opisywane są w rejestrach napraw, prowadzonych przez ASI.

9. ASI dopuszcza konserwowanie i naprawę sprzętu poza siedzibą Inspektoratu jedynie po trwałym usunięciu danych. Zużyty sprzęt służący do przetwarzania danych może być zbywany dopiero po trwałym usunięciu danych, a urządzenia uszkodzone powinny być przekazywane właściwym podmiotom w celu ich utylizacji.

10. ASI wskazuje użytkownikom, jak postępować, aby zapewnić:
a) ochronę elektromagnetyczną nośników danych – dyskietek z danymi, a szczególnie nośników danych, na których przechowywane są kopie zapasowe (należy przechowywać je z dala od magnesów oraz urządzeń wytwarzających pole magnetyczne, a więc nie wprost na urządzeniach komputerowych);
b) prawidłową lokalizację komputerów.

11. Dla bezpieczeństwa danych osobowych każda osoba upoważniona do przetwarzania danych jest zobowiązana do:

a) kasowania danych na dyskach przenośnych po ich wykorzystaniu;

b) pilnego strzeżenia akt, dyskietek, pamięci przenośnych i komputerów przenośnych;

c) stawiania ekranów komputerowych tak, aby osoby nie powołane nie mogły oglądać ich zawartości, a zwłaszcza nie naprzeciwko wejścia do pomieszczenia;

d) nie zapisywania hasła wymaganego do uwierzytelnienia się w systemie na papierze oraz pozostawiania hasła w miejscu ogólnie dostępnym (klawiaturze lub monitorze) lub innym nośniku;

e) nie podłączania do listew podtrzymujących napięcie, przeznaczonych dla sprzętu komputerowego innych urządzeń, szczególnie tych łatwo powodujących spięcia (np. grzejników, czajników, wentylatorów);

f) dbania o prawidłową wentylację komputerów (nie można zasłaniać im kratek wentylatorów meblami, zasłonami lub stawiać tuż przy ścianie);

g) powstrzymywania się od samodzielnej integracji w oprogramowanie i konfiguracje powierzonego sprzętu (szczególnie komputerów przenośnych), nawet gdy z pozoru mogłoby to usprawnić pracę lub podnieść poziom bezpieczeństwa danych;

h) przestrzegania swoich uprawnień w systemie, tj. właściwego korzystania z baz danych, używania tylko własnego identyfikatora i hasła oraz stosowania się do zaleceń Powiatowego Lekarza Weterynarii lub ASI;

i) nie pozostawiania osób postronnych w pomieszczeniu, w którym przetwarzane są dane, bez obecności osoby upoważnionej do przetwarzania danych;

j) opuszczania stanowiska pracy dopiero po aktywizowaniu wygaszacza ekranu lub po zablokowaniu stacji roboczej w inny sposób;

k) kopiowania tylko jednostkowych danych (pojedynczych plików), obowiązuje zakaz robienia kopii całych zbiorów danych lub takich ich części, które nie są konieczne do wykonania obowiązków przez pracownika; jednostkowe dane mogą być kopiowane na nośniki magnetyczne, optyczne i inne po ich zaszyfrowaniu i przechowywane w zamkniętych na klucz szafach. Po ustaniu przydatności tych kopii dane należy trwale skasować lub fizycznie zniszczyć nośniki, na których są przechowywane;

l) udostępniania danych pocztą elektroniczną tylko w postaci zaszyfrowanej;

m) nie wynoszenia na jakichkolwiek nośnikach całych zbiorów danych oraz szerokich z nich wypisów, bez uprzedniego zaszyfrowania;

n) wykonania kopii roboczych danych tak często, aby zapobiec ich utracie;

o) kończenia pracy na stacji roboczej po wprowadzeniu danych przetwarzanych tego dnia w odpowiednie obszary serwera, a następnie prawidłowego wylogowania się i wyłączenia komputera oraz odcięcia napięcia w UPS i listwie;

p) chowania do zamykanych na klucz szaf wszelkich akt zawierających dane, przed opuszczeniem miejsca pracy po zakończeniu dnia pracy;

r) zamykania okien w razie opadów lub innych zjawisk atmosferycznych, które mogą zagrozić bezpieczeństwu danych;

s) zamykania okien w razie opuszczania pomieszczenia, w tym zwłaszcza po zakończeniu dnia pracy;

t) zamykania drzwi na klucz po zakończeniu pracy w danym dniu.

u) umieszczania kluczy do szaf w ustalonym, przeznaczonym do tego miejscu po zakończeniu dnia pracy;

12. Jeśli niemożliwe jest umieszczenie wszystkich dokumentów zawierających dane w zamykanych szafach, to należy powiadomić o tym Powiatowego Lekarza Weterynarii, który zgłasza pracownikom sprzątającym jednorazową rezygnację z wykonania sprzątania pomieszczenia.

13. Osoby upoważnione do przetwarzania danych powinny mieć również na uwadze, że:

a) dane z nośników po wprowadzeniu ich do systemu informatycznego powinny być trwale usuwane z tych nośników przez fizyczne zniszczenie (np. płyty CD, DVD, pendrive) lub skasowanie danych programem usuwającym trwale pliki. Jeżeli istnieje uzasadniona konieczność, to dane pojedynczych osób (a nie całe zbiory czy obszerne wypisy ze zbiorów) mogą być przechowywane na specjalnie oznaczonych nośnikach, nośniki te muszą być przechowywane w zamkniętych na klucz szafach, nie mogą być udostępniane osobom postronnym. Po ustaniu przydatności tych danych nośniki powinny być trwale kasowane lub niszczone;

b) uszkodzone nośniki przed ich wyrzuceniem należy zniszczyć fizycznie (przeciąć, przełamać);
c) po wykorzystaniu wydruki zawierające dane osobowe należy codziennie przed zakończeniem pracy zniszczyć w niszczarce. Nie należy przechowywać takich wydruków na biurku ani wynosić poza siedzibę Inspektoratu;
d) zabrania się powtórnego używania do sporządzania brudnopisów pism jednostronnie zadrukowanych kart, jeśli zawierają one chronione dane; zaleca się natomiast dwustronne drukowanie brudnopisów pism i sporządzanie dwustronnych dokumentów.

14. Bezpieczeństwo danych, a w szczególności ich integralność i dostępność w dużym stopniu zależy od zdyscyplinowanego, codziennego umieszczania danych w wyznaczonych zasobach serwera. Pozwala to przynajmniej w pewnym stopniu uniknąć wielokrotnego wprowadzania tych samych danych do systemu informatycznego.

15. Pocztą elektroniczną można przesyłać tylko jednostkowe dane, a nie całe bazy lub obszerne z nich wypisy i tylko w postaci zaszyfrowanej. Chroni to przesłane dane przed ,,przesłuchami" na liniach teletransmisyjnych oraz przed przypadkowym rozproszeniem ich w Internecie.

16. Przed atakami z sieci zewnętrznej wszystkie komputery (w tym także przenośne) chronione są środkami dobranymi przez ASI w porozumieniu z Powiatowym Lekarzem Weterynarii. Ważne jest, aby użytkownicy zwracali uwagę na to, czy urządzenie, na którym pracują, domaga się aktualizacji tych zabezpieczeń. O wszystkich takich przypadkach należy informować ASI oraz umożliwić mu monitorowanie oraz aktualizację środków (urządzeń, programów) bezpieczeństwa.

17. ASI w porozumieniu z Powiatowym Lekarzem Weterynarii dobiera elektronicznie środki ochrony przed atakami z sieci stosownie do pojawiania się nowych zagrożeń (nowe wirusy, robaki, trojany, inne możliwości wdarcia się do systemu), a także stosownie do rozbudowy systemu informatycznego i powiększania bazy danych. Jednocześnie należy zwracać uwagę czy rozwijający się system zabezpieczeń sam nie powoduje nowych zagrożeń.

18. Poszczególnym osobom upoważnionym do przetwarzania danych przydziela się konta opatrzone niepowtarzalnym identyfikatorem umożliwiające dostęp do danych, zgodnie z zakresem upoważnienia do przetwarzania danych. ASI, po uprzednim przedłożeniu upoważnienia do przetwarzania danych, przydziela pracownikowi upoważnionemu do przetwarzania danych konto w systemie informatycznym dostępne po wprowadzeniu prawidłowego identyfikatora i uwierzytelnieniu hasłem.

19. W razie potrzeby, po uzyskaniu uprzedniej akceptacji Powiatowego Lekarza Weterynarii, ASI może przydzielić konto opatrzone identyfikatorem osobie upoważnionej do przetwarzania danych osobowych nie mającej statusu pracownika.

20. Do zagwarantowania poufności i integralności danych konieczne jest przestrzeganie przez użytkowników swoich uprawnień w systemie, tj. właściwego korzystania z baz danych, używania tylko własnego identyfikatora i hasła oraz stosowanie się do zaleceń Powiatowego Lekarza Weterynarii i ASI.

21. ASI w celu zapewnienia bezpieczeństwa przetwarzania danych na każdym komputerze stacjonarnym lub przenośnym ustawia tak wygaszacz ekranu, że po upływie ….. minut automatycznie wygaszacz zostaje uruchomiony. W celu ponownego uruchomienia funkcjonalności komputera użytkownik musi wprowadzić identyfikator oraz hasło do systemu.

22. Urządzenia przenośne oraz nośniki danych wynoszone z siedziby Inspektoratu nie powinny być pozostawiane bez nadzoru w miejscach publicznych. Komputery przenośne należy przewozić w służbowych torbach.

23. W domu natomiast, niedozwolone jest udostępnianie domownikom komputera przenośnego. Użytkownik powinien zachować w tajemnicy wobec domowników identyfikator i hasło, których podanie jest koniecznie do rozpoczęcia pracy na komputerze przenośnym.

24. ASI w razie potrzeby wskazuje w dokumencie powierzenia komputera przenośnego osobie upoważnionej do przetwarzania danych na konieczność i częstotliwość sporządzania kopii zapasowych danych przetwarzanych na komputerze przenośnym administratora danych oraz określa zasady:

a) postępowania w razie nieobecności w pracy dłużej niż 14 dni. Jeśli komputer przenośny nie może być zwrócony przed okresem nieobecności, to użytkownik tego komputera powinien niezwłocznie powiadomić o tym osobę wykonującą zadania administratora danych i uzgodnić z nim zwrot komputera przenośnego;
b) zwrotu sprzętu w razie ustania stosunku pracy.

25. System informatyczny, stacje robocze umożliwiają zapisywanie zdarzeń dzienników systemowych na potrzeby audytu i przechowywanie informacji o nich przez określony czas dwóch lat.

26. Zapisy takie obejmują:

a) identyfikator użytkownika;
b) datę i czas zalogowania i wylogowania się systemu;
c) tożsamość stacji roboczej;
d) zapisy udanych i nieudanych prób dostępu do systemu;
e) zapisy udanych i nieudanych prób dostępu do danych i innych zasobów systemowych.

27. Powiatowy Lekarz Weterynarii przeprowadza co najmniej raz na rok przegląd przetwarzanych danych pod kątem celowości ich dalszego przetwarzania. Osoby upoważnione do przetwarzania danych są zobowiązane współpracować z IOD w tym zakresie przez wypełnienie kwestionariuszy przeglądu i w razie potrzeby udzielenie innych koniecznych informacji.

28. Inne wymogi bezpieczeństwa systemowego określają instrukcje obsługi producentów sprzętu i używanych programów oraz ,,Instrukcja zarządzania systemem informatycznym w Powiatowym Inspektoracie Weterynarii w Głubczycach".

29. Inspektor Ochrony Danych analizuje, czy Polityka Bezpieczeństwa Informacji i pozostała dokumentacja jest adekwatna do:

a) zmian w budowie systemu informatycznego,
b) zmian organizacyjnych, w tym również zmian statusu osób upoważnionych do przetwarzania danych,
c) zmian w obowiązującym prawie.

Andrzej Pawłowicz
IOD – PIW Głubczyce
20.10.2020