Lublin, dnia 27.01.2023

SPRAWOZDANIE

z przeprowadzenia audytu wewnętrznego w zakresie bezpieczeństwa informacji i sieci informatycznej w Zespole Szkół Specjalnych przy Uniwersyteckim Szpitalu Dziecięcym w Lublinie za rok 2022

Zgodnie z § 4 ust. 14 *REGULAMINU POLITYKI ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI* w Zespole Szkół Specjalnych przy Uniwersyteckim Szpitalu Dziecięcym w dniu 27.01.2023 roku przeprowadzono audyt wewnętrzny w zakresie bezpieczeństwa informacji.

Audyt przeprowadziła Komisja w składzie:

Krzysztof Baran - dyrektor

Lidia Sobolewska-Gąszczyk – sekretarz szkoły

Krzysztof Król – informatyk

Audyt przeprowadzono w oparciu o następujące dyrektywy:

1) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 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).
2) Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2012 r. poz. 526).
3) Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych.(Dz. U. z 2018 r. poz. 1000 ze zm.).
4) Polityka Ochrony Danych Osobowych w Zespole Szkół Specjalnych przy Uniwersyteckim Szpitalu Dziecięcym w Lublinie.

I. USTALENIA AUDYTU WEWNĘTRZNEGO

A. Kryteria oceny

W zakresie ochrony informacji w Zespole Szkół Specjalnych przy Uniwersyteckim Szpitalu Dziecięcym w Lublinie obowiązują następujące zasady, na podstawie których kształtuje się mechanizmy techniczne i organizacyjne bezpieczeństwa informacji:

a) Zasada uprawnionego dostępu – każdy pracownik przeszedł szkolenie z zasad ochrony informacji, spełnia kryteria dopuszczenia do informacji i podpisał stosowne oświadczenie o zachowaniu poufności.

b) Zasada przywilejów koniecznych – każdy pracownik posiada prawa dostępu do informacji, ograniczone wyłącznie do tych, które są konieczne do wykonywania powierzonych mu zadań.

c) Zasada wiedzy koniecznej – każdy pracownik posiada wiedzę o systemie, do którego ma dostęp, ograniczoną wyłącznie do zagadnień, które są konieczne do realizacji powierzonych mu zadań.

d) Zasada usług koniecznych – udostępniane powinny być tylko takie usługi jakie są konieczne do realizacji zadań statutowych.

e) Zasada asekuracji – każdy mechanizm zabezpieczający musi być ubezpieczony drugim, innym (podobnym). W przypadkach szczególnych może być stosowane dodatkowe (trzecie) niezależne zabezpieczenie.

f) Zasada świadomości zbiorowej – wszyscy pracownicy są świadomi konieczności ochrony zasobów informacyjnych i aktywnie uczestniczą w tym procesie.

g) Zasada indywidualnej odpowiedzialności – za bezpieczeństwo poszczególnych elementów odpowiadają konkretne osoby.

h) Zasada obecności koniecznej – prawo przebywania w określonych miejscach mają tylko osoby upoważnione.

i) Zasada stałej gotowości – system jest przygotowany na wszelkie zagrożenia. Niedopuszczalne jest tymczasowe wyłączanie mechanizmów zabezpieczających.

j) Zasada najsłabszego ogniwa – poziom bezpieczeństwa wyznacza najsłabszy (najmniej zabezpieczony) element.

k) Zasada kompletności – skuteczne zabezpieczenie jest tylko wtedy, gdy stosuje się podejście kompleksowe, uwzględniające wszystkie stopnie i ogniwa ogólnie pojętego procesu przetwarzania informacji.

l) Zasada ewolucji – każdy system musi ciągle dostosowywać mechanizmy wewnętrzne do zmieniających się warunków zewnętrznych.

m) Zasada odpowiedniości – używane środki techniczne i organizacyjne muszą być adekwatne do sytuacji.

n) Zasada świadomej konwersacji – nie zawsze i wszędzie trzeba mówić, co się wie, ale zawsze i wszędzie trzeba wiedzieć co, gdzie i do kogo się mówi.

o) Zasada segregacji zadań – zadania i uprawnienia powinny być tak podzielone, aby jedna osoba nie mogła zdobyć pełni władzy nad całym systemem.

p) Zasada czystego biurka – dokumenty papierowe i nośniki komputerowe, kiedy nie są używane przechowuje się w specjalnych segregatorach, teczkach, szafach,

„korytkach” na półkach, wózkach rozliczeniowych, szczególnie poza godzinami pracy, pracownik zobowiązany jest do przechowywania wszystkich dokumentów zgodnie z przyjętymi wymaganiami.

q) Zasada czystego ekranu – w przypadku opuszczania stanowiska pracy, należy zablokować stację roboczą. Monitor stacji powinien być ustawiony w taki sposób, by osoby postronne nie miały możliwości wglądu do przetwarzanych aktualnie informacji; wygaszacze ekranu w stacjach roboczych zostały ustawione na nie więcej niż 5 minut.

r) Zasada odbioru wydruków z drukarki – wszelkie wydruki zawierające dane chronione zabierane są przez uprawnioną osobę natychmiast z drukarki po zakończeniu drukowania.

s) Zasada zamykania pomieszczeń – ostatni pracownik opuszczający pomieszczenie zobowiązany jest do zamknięcia okien oraz drzwi zewnętrznych na klucz. Bezwzględnie zakazuje się pozostawiania klucza w zamku, pomimo obecności pracownika w pomieszczeniu.

t) Zasada nadzorowania Klientów / gości – Klienci przyjmowani są w pomieszczeniach pracy tylko i wyłącznie pod nadzorem pracowników Zespołu Szkół Specjalnych przy Uniwersyteckim Szpitalu Dziecięcym w Lublinie. Pracownik opiekujący się osobą trzecią zobowiązany jest do nie pozostawiania jej bez nadzoru w przypadku, gdy istnieje możliwość spowodowania przez nią incydentu bezpieczeństwa (np. nieuprawnionego dostępu do informacji).

Kierownictwo Zespołu Szkół Specjalnych przy Uniwersyteckim Szpitalu Dziecięcym w Lublinie zapewnia optymalne warunki umożliwiające realizację i egzekwowanie następujących działań:

1) zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia;

2) utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację;

3) przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy;

4) podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji;

5) bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób zaangażowanych w proces przetwarzania informacji,

6) zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak:
a) zagrożenia bezpieczeństwa informacji,
b) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna,
c) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich;
7) zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez:
a) monitorowanie dostępu do informacji,
b) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,
c) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji;
8) ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość;
9) zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie;
10) zawierania w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji;
11) ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych;
12) zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności
na:

- dbałości o aktualizację oprogramowania,
- minimalizowaniu ryzyka utraty informacji w wyniku awarii,
- ochronie przed błędami, utratą, nieuprawnioną modyfikacją,
- stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa,
- zapewnieniu bezpieczeństwa plików systemowych,
- redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych,

- niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa,
- kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa;

13) bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących;

B. Ocena stanu faktycznego, zalecenia i opinie

Na podstawie przeprowadzonego oglądu funkcjonowania placówki w zakresie bezpieczeństwa informacji, przeprowadzonych rozmów z pracownikami, analizie stosownej dokumentacji należy stwierdzić, iż wymagania dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych w Zespole Szkół Specjalnych przy Uniwersyteckim Szpitalu Dziecięcym w Lublinie spełnione są przynajmniej w stopniu minimalnym.
W celu udoskonalenia funkcjonowania placówki w zakresie bezpieczeństwa informacji należałoby kontynuować proces modernizacji sprzętu komputerowego i sieci komputerowej oraz regularnie prowadzić indywidualne szkolenia pracowników w zakresie bezpieczeństwa informatycznego i obsługi urządzeń komputerowych.

Przygotował

Krzysztof Król