Brzozów, dnia 31.03.2020 r.

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH
przetwarzanych w ramach pracy zdalnej
w Specjalnym Ośrodku Szkolno-Wychowawczym w Brzozowie.

1. Wstęp.

1) Celem Polityki jest określenie sposobu przetwarzania informacji w tym ochrony danych osobowych i zasad ich przetwarzania podczas pracy zdalnej wykonywanej przez pracowników Specjalnego Ośrodka Szkolno-Wychowawczego w Brzozowie w związku z sytuacją epidemiologiczną;
2) Polityka została opracowana w związku z koniecznością realizacji zasad bezpieczeństwa wprowadzonych na obszarze Rzeczypospolitej Polskiej dotyczących zagrożenia pandemią koronawirusa;
3) W okresie sytuacji nadzwyczajnej, o której mowa w pkt 1 i 2 Polityka, staje się nadrzędną wobec innych regulacji wewnętrznych. Zatem w sytuacji, gdy zapisy Polityki stoją w sprzeczności z regulacjami zawartymi w innych dokumentach wewnętrznych, należy stosować zapisy niniejszej Polityki;
4) Wykonywanie pracy zdalnej nie zwalnia użytkownika z obowiązku przestrzegania postanowień innych regulacji, w szczególności Polityki bezpieczeństwa przetwarzanych danych osobowych wraz z dokumentami powiązanymi;
5) Zawarte w niniejszej Polityce odstępstwa od ogólnych zasad bezpieczeństwa i sposobu ochrony informacji przetwarzanych podczas sytuacji nadzwyczajnych wynikają z konieczności zapewnienia ciągłości działania, tym samym akceptowane są wyższe ryzyka dla bezpieczeństwa danych osobowych;
6) Wykonywanie pracy zdalnej nie może być jedyną przesłanką skutkującą przetwarzaniem danych osobowych. Sam fakt wykonywania pracy zdalnej nie skutkuje automatycznie uprawnieniami do przetwarzania określonej kategorii danych;
7) Nadzór nad wykonywaniem czynności w ramach pracy zdalnej oraz właściwe postepowanie z dokumentami, nośnikami oraz powierzonym sprzętem w tym zapewnienie rozliczalności ponosi bezpośredni przełożony.

2. Zakres pracy zdalnej oraz podstawowe wymagania.

1) Praca zdalna jest wykonywana na pisemne polecenie, które określa m.in. zakres zadań, czas ich realizacji oraz wskazuje obowiązujące zasady wykonywania pracy;
2) W pisemnym poleceniu wykonywania pracy zdalnej, każdorazowo należy zobowiązywać wyznaczoną osobę do zapewnienia bezpieczeństwa przetwarzanych danych;

3) Wnioskujący o zdalną pracę każdorazowo powinien dokonać stosownej analizy ryzyka proponując zakres tej pracy oraz formę i narzędzia do jej wykonania w taki sposób by zapewnione były wszystkie atrybuty bezpieczeństwa przetwarzania danych (poufności, integralności, niezaprzeczalności, dostępności);
4) Praca zdalna może być wykonywana z wykorzystaniem dokumentów i materiałów pracodawcy, jednak wymaga to zezwolenia przełożonego. Niezbędnym elementem jest zapewnienie podstawowych atrybutów bezpieczeństwa tj. integralności, poufności, niezaprzeczalności, dostępności oraz pełnej rozliczalności. Praca na dokumentach poza obiektem pracodawcy może być wykonywana (zlecana) wyłącznie po przeprowadzeniu stosownej analizy w wyniku, której osoba wyznaczona do pracy zdalnej oświadczy, że jest w stanie zapewnić szeroko rozumiane bezpieczeństwo a przełożony zaakceptuje powyższe;
5) Bezwzględnie zabronione jest wynoszenie poza siedzibę podmiotu dokumentów lub materiałów wobec, których został wprowadzony ustawowy obowiązek ich ochrony;
6) Dopuszcza się użycie podczas wykonywania pracy zdalnej sprzętu komputerowego będącego własnością pracownika wyłącznie do korzystania z dedykowanych narzędzi do pracy zdalnej w tym do prowadzenia korespondencji drogą elektroniczną (np. portal e-learningowy, poczta e-mail, media społecznościowe, strony www);
7) Po ustaniu przesłanek do wykonywania pracy zdalnej użytkownik prywatnego sprzętu komputerowego zobowiązany jest do skutecznego usunięcia z wszystkich prywatnych stanowisk komputerowych oraz informatycznych nośników przetwarzanych danych o charakterze służbowym;
8) Wykonywanie pracy zdalnej nie może obejmować przetwarzania danych osobowych na stanowiskach komputerowych będących własnością pracownika.

3. Podstawowe wymagania w zakresie bezpieczeństwa fizycznego

1) Praca zdalna powinna odbywać się w sposób i miejscach zapewniających odpowiednie bezpieczeństwo przetwarzanych informacji, w tym ochronę przed utratą, zniszczeniem lub uszkodzeniem. Przed przystąpieniem do pracy, należy wydzielić odpowiednią przestrzeń, tak aby ewentualne osoby postronne, nie miały dostępu do dokumentów lub danych przetwarzanych w systemach TI;
2) Za ochronę sprzętu wykorzystywanego do pracy zdalnej oraz za zapewnienie bezpieczeństwa informacjom przetwarzanym w ramach pracy zdalnej odpowiada użytkownik. W szczególności, użytkownik odpowiada za ograniczenie dostępu do

sprzętu wykorzystywanego do pracy zdalnej domownikom oraz gościom domu;

3) Po zakończeniu pracy w systemie lub czasowej przerwie zabrania się pozostawiania stanowiska (programu) bez nadzoru. W takich przypadkach należy odpowiednio blokować urządzenie lub wylogować się z systemu.

4. Podstawowe wymagania w zakresie bezpieczeństwa teleinformatycznego

1) Urządzenia i oprogramowanie przekazane przez pracodawcę do pracy zdalnej służą wyłącznie do wykonywania obowiązków służbowych;
2) Komputery wykorzystywane do pracy zdalnej muszą spełniać poniższe wymagania:
   a) być zabezpieczone przed dostępem osób postronnych poprzez zastosowanie jednej z metod uwierzytelniania,
   b) zainstalowano na nich program antywirusowy, który jest uruchamiany wraz ze startem systemu operacyjnego,
3) W przypadku zakończenia pracy w systemie lub czasowej przerwy zabrania się pozostawiania stanowiska (programu, aplikacji) bez nadzoru. W takich przypadkach należy odpowiednio blokować urządzenie lub wylogować się z systemu;
4) Drukowanie i skanowanie dokumentów możliwe jest tylko na urządzeniach w siedzibie pracodawcy. Zabronione jest drukowanie i skanowanie dokumentów za pomocą urządzeń domowych;
5) W przypadkach wymagających zachowania poufności przesyłanym danym należy wykorzystywać narzędzia chociażby ogólnie dostępne do szyfrowania przesyłanych treści (np. 7 ZIP) pamiętając, że hasło do zaszyfrowanego pliku przekazujemy odrębnym kanałem (np. sms);
6) Należy używać przede wszystkim służbowych kont email. Jeśli pracuje się przetwarzając dane służbowe z wykorzystaniem prywatnego e-maila, należy upewnić się, że treść i załączniki są właściwie szyfrowane. Unikamy używania danych osobowych lub poufnych informacji w temacie wiadomości;
7) W przypadku, gdy aplikacja oferuje funkcjonalności kosza (np. kosz witryny Microsoft) zaleca się opróżnienie kosza po usunięciu pliku.

5. Podstawowe wymagania w zakresie bezpieczeństwa poczty elektronicznej.

1) Sprawdź nadawcę wiadomości;
   Jeśli otrzymana wiadomość, zawiera adres nadawcy niepowiązany z podmiotem na który wskazuje treść e-maila (np. bank z adresem nazwaWaszegoBanku@xytkawdk.com), to

może oznaczać, iż nieuprawniony podmiot podszywa się bank. Wątpliwości należy wyjaśnić kontaktując się telefonicznie z danym podmiotem.

2) Pisownia wiadomości;

Wiadomość, która zawiera rażące błędy ortograficzne lub stylistyczne może wskazywać że została napisana w innym języku, a później jedynie przetłumaczona za pomocą translatora może oznaczać, że mamy do czynienia z próbą oszustwa.

3) Linki wewnątrz wiadomości;

Co do zasady nie klikamy na linki, adresy wpisujemy ręcznie w przeglądarce. Możemy najechać myszką na link i sprawdzić czy link napisany w treści jest taki sam jak pokazuje się nam na podglądzie. Gdy zauważymy różnicę absolutnie nie klikamy na niego.

4) Spakowane załączniki;

Jeśli niczego nie zamawialiśmy a otrzymujemy spakowane załączniki (np. faktury) upewniamy się, czy to wiadomość do nas. Sprawdzamy linki w mailu, jeśli wyglądają bardzo dziwnie i różnią się od tego co jest napisane w treści to znaczy, że to próba ataku.

5) Różne hasła;

Stosujemy zasadę, że do serwisów, kont pocztowych używamy odrębnych haseł.

6) Udostępnianie wrażliwych danych;

Nigdy w żadnej wiadomości nie podajemy haseł, numerów kart płatniczych, czy jakichkolwiek informacji wrażliwych. Żadna strona ani żaden bank nigdy nie poprosi o takie informacje drogą elektroniczną.

7) Szyfrowanie wiadomości;

Do szyfrowania wiadomości poleca się darmowy program 7-Zip, który potrafi w taki sposób zakodować dane, że ich odczytanie będzie możliwe tylko i wyłącznie w przypadku posiadania odpowiedniego klucza deszyfrującego. Samo hasło powinno być przekazane odbiorcy innym (bezpiecznym) kanałem komunikacji, tak aby zminimalizować ryzyko jego przejęcia zgodnie z wdrożoną Polityką szyfrowania danych. Decyzje o szyfrowaniu wiadomości zawsze podejmuje nadawca w oparciu o analizę elementów wpływających na bezpieczeństwo danych, takich jak: charakter, zakres, kontekst i cele, jakim ma służyć przekazywana informacja oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia.

8) Rozpoznawanie zagrożeń;

Bezpieczne korzystanie z poczty e-mail to nie tylko rozpoznawanie zagrożeń wychwyconych przez filtr antyspamowy czy też program antywirusowy, ale również

umiejętność samodzielnego ich rozpoznawania. W przypadkach wątpliwości próbujemy odpowiedzieć na klika pytań pomocnych w identyfikacji niebezpiecznych wiadomości e-mail:

a) Czy znasz nadawcę wiadomości?

b) Czy otrzymywałeś już inne wiadomości od tego nadawcy?

c) Czy spodziewałeś się otrzymać tę wiadomość?

d) Czy tytuł wiadomości i nazwa załącznika mają sens?

e) Czy wiadomość nie zawiera złośliwego oprogramowania – jaki jest wynik skanowania antywirusowego?

Pozytywne odpowiedzi na powyższe pytania zwiększą prawdopodobieństwo, że dana wiadomość nie będzie stanowiła zagrożenia.

Negatywna odpowiedź na przynajmniej jedno z pytań powinna skutkować podjęciem przez odbiorcę działań, takich jak:

a) rezygnacja z odpowiedzi na wiadomość,

b) nieklikanie w odnośniki umieszczone w e-mailu,

c) skasowanie wiadomości bez jej otwierania.

9) Przed wysłaniem wiadomości e-mail należy sprawdzić, że wysyłamy ją do właściwego adresata;

10) Zaleca się przesyłanie informacji w sposób umożliwiający zachowanie integralności tzn. w wersji nieedytowalnej.

6. Wykorzystanie służbowej poczty elektronicznej.

Służbowy adres poczty elektronicznej wykorzystuje się wyłącznie w celu prowadzenia korespondencji związanej z działalnością placówki. Zabrania się wykorzystywania służbowej poczty elektronicznej do celów prywatnych.

7. Postanowienia końcowe.

1) Niniejsza Polityka obowiązuje przez okres obowiązywania art. 3 ustawy z dnia 2 marca 2020r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID – 19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych (Dz. U. 2020 poz. 374);

2) Postanowienia pkt. 5 zachowują moc do odwołania.

INSPEKTOR
OCHRONY DANYCH
Marek Broda