Zespół Obsługi Placówek Oświaty
w Okonku, ul. Leśna 46
64-965 OKONEK
NIP 767-15-70-923 REGON 572106468
tel. 067 266 91 45

Załącznik nr 2

I N S T R U K C J A
POSTĘPOWANIA W SYTUACJI NARUSZENIA OCHRONY DANYCH OSOBOWYCH W ZESPOLE OBSŁUGI PLACÓWEK OŚWIATY W OKONKU

INSTRUKCJA

postępowania w sytuacji naruszenia ochrony danych osobowych

§ 1

Instrukcja jest przeznaczona dla osób zatrudnionych przy przetwarzaniu danych osobowych w systemie informatycznym w Zespole Obsługi Placówek Oświaty w Okonku.

§ 2

Instrukcja określa tryb postępowania w przypadku, gdy:

1. stwierdzono naruszanie zabezpieczenia systemu informatycznego,
2. stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie zabezpieczeń tych danych.

§ 3

Każda osoba zatrudniona w Zespole Obsługi Placówek Oświaty w Okonku, która stwierdzi lub podejrzewa naruszenie zabezpieczenia ochrony danych osobowych w systemie informatycznym, powinna niezwłocznie poinformować o tym administratora bezpieczeństwa informacji lub osobę przez niego upoważnioną.

§ 4

Osoba zatrudniona przy przetwarzaniu danych osobowych, która uzyskała informację lub sama stwierdziła naruszenie zabezpieczenia bazy danych osobowych w systemie informatycznym, zobowiązana jest niezwłocznie powiadomić o tym administratora bezpieczeństwa informacji lub upoważnioną przez niego osobę, a w przypadku ich nieobecności – bezpośrednio administratora danych osobowych.

§ 5

Administrator bezpieczeństwa informacji lub osoba przez niego upoważniona powinna w pierwszej kolejności:

1. Zapisać wszelkie informacje związane z zaistniałym zdarzeniem, a szczególnie: dokładny czas uzyskania informacji o naruszeniu zabezpieczenia danych osobowych i czas samodzielnego wykrycia tego faktu.
2. Na bieżąco wygenerować i wydrukować (jeżeli pozwala na to system) wszystkie możliwe dokumenty i raporty, które mogą pomóc w ustaleniu okoliczności zdarzenia, opatrzeć je datą i podpisem.
3. Przystąpić do zidentyfikowania rodzaju zaistniałego zdarzenia, zwłaszcza do określenia skali zniszczeń i metody dostępu do danych osobowych osoby niepowołanej.

§ 6

Niezwłocznie należy podjąć odpowiednie kroki w celu powstrzymania lub ograniczenia dostępu do danych osoby niepowołanej, zminimalizowania szkód i zabezpieczenia przed usunięciem śladu jej ingerencji, szczególnie przez:

a) fizyczne odłączenie urządzeń i segmentów sieci, które mogły umożliwić dostęp do bazy danych osoby nieupoważnionej
b) wylogowanie użytkownika podejrzanego o naruszenie ochrony danych
c) zmianę hasła na konto administratora i użytkownika, poprzez które uzyskano nielegalny dostęp w celu uniknięcia ponownej próby włamania

§ 7

Po wyeliminowaniu bezpośredniego zagrożenia należy przeprowadzić wstępną analizę stanu systemu informatycznego w celu potwierdzenia lub wykluczenia faktu naruszenia ochrony danych osobowych systemu.

§ 8

Administrator bezpieczeństwa informacji lub osoba przez niego upoważniona powinna sprawdzić:

a) stan urządzeń wykorzystywanych do przetwarzania danych osobowych
b) zawartość zbioru danych osobowych
c) sposób działania programu
d) jakość komunikacji w sieci telekomunikacyjnej
e) wykluczyć możliwość obecności wirusów komputerowych

§ 9

Po dokonaniu powyższych czynności administrator bezpieczeństwa informacji powinien przeprowadzić szczegółową analizę systemu informatycznego obejmującego identyfikację:

a) rodzaje zaistniałego zdarzenia,
b) metody dostępu do danych osoby nieupoważnionej,
c) skali zniszczeń.

§ 10

Niezwłocznie należy przywrócić prawidłowy stan działania systemu, przy czym, jeżeli nastąpiło uszkodzenie bazy danych osobowych, niezbędne jest odtworzenie jej z ostatniej kopii awaryjnej z zachowaniem wszelkich środków ostrożności, mających na celu uniknięcie ponownego uzyskania dostępu tą samą drogą przez osobę niepowołaną.

§ 11

Po przywróceniu prawidłowego stanu bazy danych osobowych należy przeprowadzić szczegółową analizę w celu określenia przyczyny naruszenia ochrony danych osobowych oraz przedsięwziąć kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.

1. Jeżeli przyczyną zdarzenia był błąd osoby zatrudnionej przy przetwarzaniu danych osobowych w systemie informatycznym należy przeprowadzić dodatkowe szkolenie wszystkich osób biorących udział przy przetwarzaniu danych.

2. Jeżeli przyczyną zdarzenia było uaktywnienie wirusa, należy ustalić źródło jego pochodzenia oraz wykonać zabezpieczenia antywirusowe.
3. Jeżeli przyczyną zdarzenia było niewłaściwe postępowanie ze strony osoby zatrudnionej przy przetwarzaniu danych osobowych, należy wyciągnąć konsekwencje regulowane ustawą.
4. Jeżeli przyczyną zdarzenia było włamanie w celu pozyskania danych osobowych, należy dokonać szczegółowej analizy wdrożonych środków zabezpieczających w celu zapewnienia skuteczniejszej ochrony bazy danych.
5. Jeżeli przyczyną zdarzenia był zły stan urządzenia lub sposób działania programu, należy wówczas niezwłocznie przeprowadzić kontrolne czynności serwisowo – programowe.

§ 12

Administrator bezpieczeństwa informacji przygotowuje szczegółowy raport o przyczynach, przebiegu i wnioskach ze zdarzenia (dołączając ewentualne kopie dowodów dokumentujących to zdarzenie) oraz w określonym terminie od daty zaistnienia zdarzenia przekazuje go administratorowi danych osobowych.

DYREKTOR
Zespołu Obsługi Placówek Oświaty
w Okonku
mgr Renata Mejnartowicz