„ZATWIERDZAM"

REKTOR

Zachodniopomorskiego Uniwersytetu Technologicznego

w Szczecinie

.....

dr hab. inż. Jacek Wróbel, prof. nadzw.

Zachodniopomorski
Uniwersytet
Technologiczny
w Szczecinie

Zatwierdzam i wprowadzam do użytku służbowego:

Wytyczne

w zakresie ochrony danych osobowych w Zachodniopomorskim Uniwersytecie Technologicznym w Szczecinie

Inspektor Ochrony Danych

INSPEKTOR OCHRONY DANYCH
w Zachodniopomorskim Uniwersytecie Technologicznym
w Szczecinie
mgr Artur Kurek

I. Postanowienia ogólne.

II. Kategorie naruszeń ochrony danych osobowych (incydentów).

III. Zakres obowiązywania procedury zarządzania incydentami związanymi z bezpieczeństwem danych osobowych.

IV. Zgłaszanie naruszenia ochrony danych osobowych.

V. Podejmowanie działań w związku ze zgłaszanymi incydentami naruszenia bezpieczeństwa przetwarzania danych osobowych .

VI. Załączniki.

I. Postanowienia ogólne.

Przez pojęcie ,,naruszenia ochrony danych osobowych" należy rozumieć naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych (art.4 pkt.12 RODO).

Aby zaistniało naruszenie muszą być spełnione łącznie trzy przesłanki:

1/ naruszenie dotyczy danych osobowych przesyłanych , przechowywanych lub w inny sposób przetwarzanych przez ZUT,

2/ skutkiem naruszenia musi być zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych,

3/ naruszenie jest skutkiem złamania zasad bezpieczeństwa ochrony danych.

Wyróżniamy trzy typy naruszenia ochrony danych osobowych:

1/ **naruszenie poufności**-polega na ujawnieniu danych osobowych nieuprawnionej osobie,

2/ **naruszenie dostępności**-polega na trwałej utracie lub zniszczeniu danych osobowych,

3/ **naruszenie integralności**-polega na zmianie treści danych osobowych w sposób nieautoryzowany.

II. Kategorie naruszeń ochrony danych osobowych (incydentów).

1. Rodzaje naruszeń ochrony danych osobowych:

   1/ zdarzenie losowe zewnętrzne (np. klęski żywiołowe, pożary, zakłócenia w dostawie energii elektrycznej itp.) którego wystąpienie może powodować zniszczenie lub uszkodzenie infrastruktury informatycznej albo dokumentacji papierowej,

   2/ zdarzenie losowe wewnętrzne (np. błędy w oprogramowaniu, awarie sprzętu itp.) które mogą powodować zakłócenia ciągłości pracy systemów a także prowadzić do zniszczenia lub utraty danych,

   3/ świadome i celowe działania mające na celu naruszenie poufności zasobów informacyjnych, w tym poufności danych osobowych,

2. Przyczyny naruszeń ochrony danych osobowych:

1/ niewłaściwe wykorzystywanie zasobów informatycznych lub niewłaściwe postępowanie z dokumentacją papierową ,

2/ działania szkodliwego oprogramowania,

3/ próby omijania systemów zabezpieczeń,

4/ nieautoryzowany dostępu do systemów, aplikacji i dokumentów,

5/ zniszczenia lub kradzież urządzeń wykorzystywanych do przetwarzania danych osobowych,

6/ zniszczenie lub kradzież nośników danych,

7/ próby wyłudzeń informacji o danych osobowych,

8/ ataków socjotechnicznych, ataków z wykorzystaniem technik zagrażających poufności, integralności lub dostępności informacji,

9/ nieprawidłowości w zakresie zabezpieczenia przechowywania danych osobowych,

10/ naruszenia zasad obowiązujących w ZUT dotyczących bezpieczeństwa danych osobowych (np. pozostawienie włączonego komputera lub nie wylogowanie się po zakończeniu pracy lub podczas przerwy w pracy, pozostawienie niezabezpieczonych dokumentów drukowanych zawierających dane osobowe itp.).

III. Zakres obowiązywania procedury zarządzania incydentami związanymi z bezpieczeństwem danych osobowych.

Procedura zarządzania incydentami związanymi z bezpieczeństwem danych osobowych obowiązuje we wszystkich jednostkach organizacyjnych ZUT. Procedura obowiązuje również podmioty zewnętrzne, które dopuszczono do przetwarzania danych osobowych będącymi zasobami informacyjnymi ZUT.

IV. Zgłaszanie naruszenia ochrony danych osobowych.

1. Naruszenie ochrony danych osobowych może być zgłaszane przez pracowników - użytkowników i administratorów systemów oraz podmioty zewnętrzne. Osoba zgłaszająca odpowiada za wyczerpujący opis incydentu odpowiednio do posiadanej wiedzy i umiejętności. Zgłoszenie incydentu musi być przekazane

Inspektorowi Ochrony Danych (IOD). Zgłoszenie musi być przekazane telefonicznie i potwierdzone w formie elektronicznej.

2. Zgłoszenie musi zawierać następujące informacje:

1) imię i nazwisko osoby zgłaszającej,

2) jednostka organizacyjna uczelni lub nazwa podmiotu zewnętrznego,

3) miejsce i datę wystąpienia incydentu,

4) opis incydentu w sposób adekwatny do posiadanej wiedzy i umiejętności zgłaszającego.

3. Brak umiejętności poprawnego rozpoznania incydentu przez osobę zgłaszającą nie może być przyczyną zaniechania zgłoszenia.

V. Podejmowanie działań w związku ze zgłaszanymi incydentami naruszenia bezpieczeństwa przetwarzania danych osobowych.

1. W przypadku naruszenia ochrony danych osobowych mają zastosowanie przepisy art. 33-34 rozporządzenia 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 – RODO) (Dz. Urz. UE L 119 z 5 kwietnia 2016 r.) .

2. Zgłoszenie naruszenia rejestrowanie jest przez IOD w rejestrze naruszeń ochrony danych osobowych.

Osoba zgłaszająca incydent powinna w miarę możliwości zabezpieczyć materiał dowodowy (np. zrzut ekranu monitora, zdjęcie niezabezpieczonych materiałów zawierających dane osobowe itp.). Działania związane z obsługą zgłoszenia w pierwszej kolejności dotyczą rozpoznania i kwalifikacji zgłoszenia. W przypadku, kiedy zgłoszenie zakwalifikowane zostało jako incydent naruszenia bezpieczeństwa przetwarzania danych osobowych, dokonywana jest ocena jego istotności.

3. Przy ocenie istotności incydentu pod uwagę brane są następujące czynniki:

1) charakter naruszenia ochrony danych osobowych,

2) kategorie i przybliżoną liczbę osób których dane dotyczą,

3) kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie,

4) możliwe konsekwencje naruszenia ochrony danych osobowych,

5) wpływ incydentu na ciągłość działania uczelni,
6) koszty usunięcia skutków incydentu,
7) szacowany czas naprawy skutków wywołanych incydentem.

4. Zakwalifikowanie zgłoszenia incydentu jako „fałszywy alarm” kończy postępowanie, o czym IOD informuje zgłaszającego.

5. W przypadku zakwalifikowania zdarzenia jako naruszenie ochrony danych osobowych, które skutkuje ryzykiem naruszenia praw lub wolności osób fizycznych, IOD bez zbędnej zwłoki zawiadamia Administratora o konieczności zgłoszenia naruszenia do organu nadzorczego nie później niż w terminie 72 godzin od stwierdzenia naruszenia i przygotowuje stosowne dokumenty.

6. IOD podejmuje również działania zabezpieczające i naprawcze zmierzające do zniwelowania skutków powstałych w wyniku incydentu, jak również działania zaradcze dla uniknięcia wystąpienia podobnych incydentów w przyszłości.

7. Jeżeli zgłoszony incydent naruszenia ochrony danych osobowych może powodować **wysokie ryzyko** naruszenia praw lub wolności osób fizycznych, a stosowane w uczelni techniczne i organizacyjne środki ochrony danych nie eliminują tego ryzyka, IOD bez zbędnej zwłoki informuje Administratora o konieczności zawiadomienia osób, których dane dotyczą, o takim naruszeniu .

8. Jeżeli zawiadomienie osób, których dane dotyczą wymagałoby niewspółmiernie dużego wysiłku, Administrator przygotowuje publiczny komunikat lub wybiera inny stosowny środek, za pomocą którego zawiadomienie zostanie tym osobom przekazane.

9. W przypadku stwierdzenia działań zamierzonych, przy jednoczesnym zidentyfikowaniu sprawcy incydentu dotyczącego naruszenia bezpieczeństwa przetwarzania danych osobowych Administrator podejmuje decyzję dotyczącą wyciągnięcia ewentualnych konsekwencji dyscyplinarnych wobec sprawcy incydentu. Jednocześnie, w zależności od wagi incydentu, mogą być zawiadomione organa ścigania.

10. Powyższe działania raportowane są w rejestrze naruszeń związanych z bezpieczeństwem przetwarzania danych osobowych.

Załącznik nr 1

Zgłoszenie wstępne z naruszenia ochrony danych osobowych

1. Data …….…… Godzina ……

2. Osoba powiadamiająca o naruszeniu oraz inne osoby zaangażowane lub odpytane w związku z naruszeniem (imię, nazwisko, stanowisko służbowe,):

……

3. Lokalizacja zdarzenia (nr. pokoju, nazwa pomieszczenia, określenie komputerowego stanowiska roboczego, nazwa programu lub aplikacji itp.):

……

4. Rodzaj naruszenia i określenie okoliczności towarzyszących naruszeniu:

……

5. Podjęte działania:

……

6. Wstępna ocena przyczyn wystąpienia naruszenia:

……

7. Postępowanie wyjaśniające i naprawcze:

……

…….. ……

(podpis zgłaszającego) (data i podpis IOD)

Załącznik nr 2- Wykaz przykładowych incydentów

<table>
<tr><th>FORMY NARUSZEŃ</th><th>SPOSOBY POSTĘPOWANIA</th></tr>
<tr><td colspan="2">W ZAKRESIE WIEDZY</td></tr>
<tr><td>Ujawnianie sposobu działania aplikacji i systemu oraz jej zabezpieczeń osobom niepowołanym.</td><td rowspan="3">Natychmiast przerwać rozmowę lub inną czynność prowadzącą do ujawnienia informacji. Bezzwłocznie powiadomić inspektora ochrony danych osobowych (IOD).</td></tr>
<tr><td>Ujawnianie informacji o sprzęcie i pozostałej infrastrukturze informatycznej.</td></tr>
<tr><td>Dopuszczanie i stwarzanie warunków, aby ktokolwiek taką wiedzę mógł pozyskać np. z obserwacji lub dokumentacji.</td></tr>
<tr><td colspan="2">W ZAKRESIE SPRZĘTU I OPROGRAMOWANIA</td></tr>
<tr><td>Opuszczenie stanowiska pracy i pozostawienie aktywnej aplikacji umożliwiającej dostęp do bazy danych osobowych.</td><td>Niezwłocznie zakończyć działanie aplikacji.</td></tr>
<tr><td>Dopuszczenie do korzystania z aplikacji umożliwiającej dostęp do bazy danych osobowych przez jakiekolwiek inne osoby niż osoba, której identyfikator został przydzielony.</td><td>Wezwać osobę bezprawnie korzystającą z aplikacji do opuszczenia stanowiska przy komputerze.</td></tr>
<tr><td>Pozostawienie w jakimkolwiek niezabezpieczonym, a w szczególności w miejscu widocznym, zapisanego hasła dostępu do bazy danych osobowych lub sieci.</td><td>Natychmiast zabezpieczyć notatkę z hasłami w sposób uniemożliwiający odczytanie.</td></tr>
<tr><td>Dopuszczenie do użytkowania sprzętu komputerowego i oprogramowania umożliwiającego dostęp do bazy danych osobowych osobom nieuprawnionym.</td><td>Wezwać osobę nieuprawnioną do opuszczenia stanowiska. Ustalić, jakie czynności zostały przez osoby nieuprawnione wykonane. Przerwać działające programy.</td></tr>
<tr><td>Samodzielne instalowanie jakiegokolwiek oprogramowania.</td><td>Pouczyć osobę popełniającą wymienioną czynność, aby jej zaniechała. Wezwać służby informatyczne w celu odinstalowania programów. Bezzwłocznie powiadomić administratora systemu informatycznego (ASI).</td></tr>
<tr><td>Modyfikowanie parametrów systemu i aplikacji.</td><td>Wezwać osobę popełniającą wymieniona czynność, aby jej zaniechała. Bezzwłocznie powiadomić administratora systemu informatycznego (ASI).</td></tr>
</table>

W ZAKRESIE DOKUMENTÓW I OBRAZÓW ZAWIERAJĄCYCH DANE OSOBOWE	
Pozostawienie dokumentów w otwartych pomieszczeniach bez nadzoru.	Zabezpieczyć dokumenty.
Przechowywanie dokumentów niewłaściwie zabezpieczonych przed dostępem osób niepowołanych.	Powiadomić przełożonych. Spowodować poprawienie zabezpieczeń.
Wyrzucanie dokumentów w stopniu zniszczenia umożliwiającym ich odczytanie.	Zabezpieczyć niewłaściwie zniszczone dokumenty. **Bezzwłocznie powiadomić inspektora ochrony danych osobowych (IOD).**
Dopuszczanie do kopiowania dokumentów i utraty kontroli nad kopią.	Zaprzestać kopiowania. Odzyskać i zabezpieczyć wykonaną kopię. Powiadomić przełożonych.
Dopuszczanie, aby inne osoby odczytywały zawartość ekranu monitora, na którym wyświetlane są dane osobowe.	Wezwać nieuprawnioną osobę odczytującą dane do zaprzestania czynności, wyłączyć monitor.
Sporządzanie kopii danych na nośnikach danych w sytuacjach nie przewidzianych procedurą.	Spowodować zaprzestanie kopiowania. Podjąć próbę odzyskania oraz zabezpieczyć wykonaną kopię. **Bezzwłocznie powiadomić (ASI).**
Utrata kontroli nad kopią danych osobowych.	Podjąć próbę odzyskania kopii. **Bezzwłocznie powiadomić (ASI).**
W ZAKRESIE POMIESZCZEŃ I INFRASTRUKTURY SŁUŻĄCYCH DO PRZETWARZANIA DANYCH OSOBOWYCH	
Opuszczanie i pozostawianie bez dozoru nie zamkniętego pomieszczenia, w którym zlokalizowany jest sprzęt komputerowy używany do przetwarzania danych osobowych, co stwarza ryzyko dokonania na sprzęcie lub oprogramowaniu modyfikacji zagrażających bezpieczeństwu danych osobowych.	Zabezpieczyć pomieszczenie.
Wpuszczanie do pomieszczeń osób nieznanych i dopuszczanie do ich kontaktu ze sprzętem komputerowym.	Wezwać osoby bezprawnie przebywające w pomieszczeniach do ich opuszczenia, próbować ustalić ich tożsamość.
Dopuszczanie, aby osoby spoza służb informatycznych i telekomunikacyjnych podłączały jakiekolwiek urządzenia do sieci komputerowej, demontowały elementy obudów gniazd i torów kablowych lub dokonywały jakichkolwiek manipulacji.	Wezwać osoby dokonujące zakazanych czynność do ich zaprzestania. Postarać się ustalić ich tożsamość. **Powiadomić (ASI).**

W ZAKRESIE POMIESZCZEŃ, W KTÓRYCH ZNAJDUJĄ SIĘ KOMPUTERY CENTRALNE I URZĄDZENIA SIECI	
Dopuszczenie lub ignorowanie faktu, że osoby spoza służb informatycznych i telekomunikacyjnych dokonują jakichkolwiek manipulacji przy urządzeniach lub okablowaniu sieci komputerowej w miejscach publicznych (hole, korytarze, itp.).	Wezwać osoby dokonujące zakazanych czynność do ich zaprzestania i ew. opuszczenia pomieszczeń. Postarać się ustalić ich tożsamość. **Bezzwłocznie powiadomić inspektora ochrony danych osobowych (IOD).**
Dopuszczanie do znalezienia się w pomieszczeniach komputerów centralnych lub węzłów sieci komputerowej osób spoza służb informatycznych i telekomunikacyjnych.	Wezwać osoby dokonujące zakazanych czynność do ich zaprzestania i opuszczenia chronionych pomieszczeń. Postarać się ustalić ich tożsamość. **Bezzwłocznie powiadomić inspektora ochrony danych osobowych (IOD).**

TABELA PRZYKŁADOWYCH ZJAWISK ŚWIADCZĄCYCH O MOŻLIWOŚCI NARUSZENIA OCHRONY DANYCH OSOBOWYCH	
FORMY NARUSZEŃ	SPOSOBY POSTĘPOWANIA
Ślady manipulacji przy układach sieci komputerowej lub komputerach.	Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. **Bezzwłocznie powiadomić (ASI).**
Obecność nowych kabli o nieznanym przeznaczeniu i pochodzeniu.	Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji.
Niezapowiedziane zmiany w wyglądzie lub zachowaniu aplikacji służącej do przetwarzania danych osobowych.	
Nieoczekiwane, nie dające się wyjaśnić, zmiany zawartości bazy danych.	
Obecność nowych programów w komputerze lub inne zmiany w konfiguracji oprogramowania.	
Ślady włamania do pomieszczeń, w których przetwarzane są dane osobowe.	**Postępować zgodnie z właściwymi przepisami. Bezzwłocznie powiadomić inspektora ochrony danych osobowych (IOD).**