Załącznik do Decyzji nr 8/2019 Prorektora ds. Ogólnych i Rozwoju
w sprawie wprowadzenia *Procedury postępowania z naruszeniami UKSW*
z dnia 20 listopada 2019 r.

PROCEDURA POSTEPOWANIA Z NARUSZENIAMI

w Uniwersytecie Kardynała Stefana Wyszyńskiego w Warszawie

SPIS TREŚCI:

I. ZGŁASZANIE NARUSZEŃ 3
II. POSTĘPOWANIE Z NARUSZENIAMI 4
III. OGRANICZANIE SKUTKÓW NARUSZENIA 5
IV. ODTWARZANIE SYSTEMU 6
V. DZIAŁANIA PO ZAKOŃCZENIU PROCEDURY NARUSZENIA 6
VI. REJESTROWANIE INFORMACJI O INCYDENTACH 6
VII. GROMADZENIE MATERIAŁU DOWODOWEGO 7
Załącznik nr 1 - Wzór raportu z naruszenia 8
Załącznik nr 2 – Instrukcja zabezpieczenia środków przetwarzania w sytuacji wystąpienia zdarzenia naruszenia ochrony danych 11
Załącznik nr 3 - Wzór protokołu zabezpieczenia materiału dowodowego 12

Procedura Zarządzania Naruszeniami w UKSW jest zgodna z:

1. *Rozporządzeniem 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 (w skrócie RODO);*
2. *Dyrektywą Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW;*
3. *Wytycznymi Grupy Roboczej (GDPR) ds. Ochrony danych 29 18/EN WP 250 rev.01 „dotyczące zgłaszania naruszenia ochrony danych" w rozumieniu rozporządzenia 2016/679.*
4. *Zarządzeniem Nr 40/2018 Rektora UKSW z dnia 21 września 2018 r. w sprawie wprowadzenia Polityki bezpieczeństwa informacji Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie (z późn. zm.)*

I. ZGŁASZANIE NARUSZEŃ

§ 1.

1. Pracownicy UKSW mają obowiązek niezwłocznego zgłaszania wszelkich zdarzeń, które naruszają lub mogą naruszyć przepisy prawa oraz polityki, regulaminy i procedury Uczelni w zakresie bezpieczeństwa danych osobowych.
2. Zgłoszenia należy kierować do Inspektora Ochrony Danych (IOD) za pomocą formularza dostępnego na stronie internetowej Uczelni w menu „ochrona danych osobowych", a tylko w wyjątkowych przypadkach, przy braku dostępności do ww. formularza, za pomocą „Raportu Stwierdzenia Naruszenia", o którym mowa *w załączniku nr 1* do niniejszej Procedury.
3. Po stwierdzeniu naruszenia ochrony danych osobowych administrator, o którym mowa w § 6 ust. 1 *załącznika Nr 1 do Polityki Bezpieczeństwa Informacji w UKSW (Zarządzenie Nr 40/2018 Rektora UKSW z dnia 21 września 2018 r. w sprawie wprowadzenia Polityki bezpieczeństwa informacji Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie (z późn. zm.))*, powinien zgłosić je organowi nadzorczemu bez zbędnej zwłoki, ale nie później niż w terminie 72 godzin po stwierdzeniu naruszenia, chyba że administrator jest w stanie wykazać zgodnie z zasadą rozliczalności, że jest mało prawdopodobne, by naruszenie to mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych. Jeżeli nie można dokonać zgłoszenia w terminie 72 godzin, zgłoszeniu powinno towarzyszyć wyjaśnienie przyczyn opóźnienia, a informacje mogą być przekazywane stopniowo, bez dalszej zbędnej zwłoki (art. 33 RODO.)
4. Wyróżniamy następujące rodzaje naruszeń (rodz. 1 art. 29 GDPR):
   1) „naruszenie poufności", które polega na ujawnieniu lub udostępnieniu danych osobie nieuprawnionej;
   2) „naruszenie integralności", które sprowadza się do zmiany treści danych osobowych, czyli ich modyfikowania, w sposób nieautoryzowany;
   3) „naruszenie dostępności", które wiąże się z trwałą utratą dostępu do danych lub ich zniszczeniem
5. W przypadku powierzenia obowiązków zarządzania systemami informatycznymi podmiotom zewnętrznym lub zawarcia umów w zakresie powierzenia przetwarzania danych osobowych, powiadamianie administratora o naruszeniu odbywa się na zasadach określonych w ww. umowach.

II. POSTĘPOWANIE Z NARUSZENIAMI

§ 2.

1. O możliwości zaistnienia przypadku naruszenia bezpieczeństwa danych osobowych, z uwzględnieniem Tabeli form naruszeń zasad ochrony danych osobowych zawartej w załączniku Nr 2 do Polityki Bezpieczeństwa Informacji w UKSW *(Zarządzenie Nr 40/2018 Rektora UKSW z dnia 21 września 2018 r. w sprawie wprowadzenia Polityki bezpieczeństwa informacji Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie (z późn. zm.)),* mogą świadczyć:
   1) nadmierne w stosunku do wykonywanych zadań (zakresu upoważnienia), uprawnienia użytkownika do zasobów danych,
   2) niestabilna praca systemu teleinformatycznego,
   3) korzystanie z zasobów danych poza miejscem przetwarzania/godzinami pracy (bez zgody przełożonego),
   4) nowe „podejrzane" (nieznane) konta użytkowników w systemie,
   5) wysoka aktywność kont, które długo pozostawały niewykorzystane,
   6) zanotowanie w krótkim czasie dużej liczby nieudanych prób logowania,
   7) anomalie w pracy systemu lub programu (świadczące np. o obecności wirusa komputerowego),
   8) naruszenie lub wadliwe funkcjonowanie zabezpieczeń fizycznych w pomieszczeniach, w których następuje przetwarzanie danych osobowych (uszkodzone zamki, okna, drzwi, naruszone plomby, itp.)
2. Lokalny Administrator (LA) dokonuje wstępnej identyfikacji zaistniałego zdarzenia i na podstawie dostępnych informacji oraz analizy okoliczności kwalifikuje zdarzenie (lub serię zdarzeń) jako:
   1) zdarzenie nie mające cech naruszenia bezpieczeństwa, np. zaplanowana przerwa technologiczna,
   2) błąd w działaniu elementu systemu teleinformatycznego, infrastruktury teleinformatycznej lub infrastruktury biurowej,
   3) awaria techniczna czasowo blokująca dostępność informacji,
   4) zdarzenie niskiej kategorii - związane z naruszeniem bezpieczeństwa ochrony danych, a szczególnie jej integralności i poufności, nie generujące kar finansowych, jednak powodujący pośrednio lub bezpośrednio utrudnienia w realizacji jakiegokolwiek procesu głównego Uczelni,
   5) zdarzenie średniej kategorii - związane z naruszeniem bezpieczeństwa ochrony danych skutkujące pośrednio lub bezpośrednio zatrzymaniem realizacji jakiegokolwiek procesu ustawowego i/lub stratami finansowymi oraz możliwością konsekwencji prawnych i/lub utraty wizerunku,
   6) zdarzenie wysokiej kategorii - związane z naruszeniem bezpieczeństwa ochrony danych, którego skutkiem jest destrukcja (zniszczenie, utrata) kluczowych zasobów i przerwanie funkcjonowania procesów Uczelni.
3. O zdarzeniu noszącym znamiona naruszenia - osoba, która stwierdziła jego wystąpienie powiadamia niezwłocznie IOD, zgodnie z zasadą opisaną w § 1 ust. 2. IOD przeprowadza analizę i dokonuje ostatecznej klasyfikacji zdarzenia na potrzeby realizacji zadań administratora, o których mowa w § 1 ust. 3.
4. Analiza naruszenia, o której mowa w ust. 3 niniejszego paragrafu, uwzględnia następujące kryteria:
   1) charakter zdarzenia i jego znaczenie związane z naruszeniem bezpieczeństwa ochrony danych osobowych,
   2) miejsce wystąpienia zdarzenia - identyfikacja punktu, w którym nastąpiło zdarzenie (lokalizacja

pomieszczenia, serwer, stacja robocza itp.),

3) liczba jednostek organizacyjnych Uczelni, identyfikacja osób „związanych” ze zdarzeniem, zakres zasobów dotkniętych naruszeniem,
4) identyfikację zasobów potrzebnych przy dalszych działaniach w ramach postępowania ze zdarzeniem związanym z naruszeniem bezpieczeństwa ochrony danych,
5) możliwości rozszerzania się naruszenia i sposoby jego ograniczania,
6) rodzaj ujawnionej informacji (jeśli ma zastosowanie - np. dane osobowe),
7) szacunkowy czas, po którym skutki naruszenia zostaną zlikwidowane, jeżeli nie ma możliwości natychmiastowego usunięcia stanu naruszenia bezpieczeństwa ochrony danych,
8) skutki organizacyjne i prawne (wstępny szacunek).

5. W przypadku, gdy zasięg i szacunkowy czas trwania powoduje zakwalifikowanie naruszenia do wysokiej kategorii, administrator powiadamia niezwłocznie Prezesa Urzędu Ochrony Danych Osobowych (PUODO), a następnie przeprowadza dochodzenie wyjaśniające.
6. W przypadku, gdy rodzaj i zasięg incydentu, zidentyfikowany na którymkolwiek z etapów postępowania, uzasadnia potrzebę powiadomienia organów ścigania, to decyzję o sposobie i terminie powiadomienia podejmuje administrator.

III. OGRANICZANIE SKUTKÓW NARUSZENIA

§ 3.

1. Dokumentacja naruszenia podlega rygorom ochrony przez tworzenie autoryzowanych kopii tych elementów, które mają zastosowanie przy postępowaniu z naruszeniem, w tym: rejestry urządzeń, systemów operacyjnych i aplikacji, kopie zapasowe, pliki konfiguracyjne i systemowe (zgodnie z rygorami tworzenia materiału dowodowego), bezpieczne przechowywanie tych kopii, przyjęcia dokumentacji oraz jej wszystkich części.
2. IOD przeprowadza bieżące działania zmierzające do ograniczenia skutków naruszenia i zidentyfikowania jego źródła. W tym celu może spowodować zablokowanie części systemu lub dostępnych usług.
3. W przypadku, gdy działania opisane w ust. 2 obejmują wyłączenie lub ograniczenie funkcjonowania zasobów niezbędnych do realizowania celów ustawowych bądź statutowych Uczelni, IOD przedstawia decyzję do akceptacji ADO, wraz z rekomendacją Centralnego Administratora Systemu Informatycznego (CASI).
4. Rekomendacja CASI uwzględnia:
   1) uzależnienie Uczelni od systemu teleinformatycznego (jak długo Uczelnia może funkcjonować przy całkowitym lub częściowym wyłączeniu systemu),
   2) stopień narażenia informacji przetwarzanych w systemach teleinformatycznych Uczelni na ujawnienie w przypadku utrzymywania się stanu naruszenia zabezpieczenia,
   3) stopień uświadomienia użytkowników (jaka może być reakcja użytkowników na anormalne zachowanie się systemu - np. niemożność zarejestrowania się, wyłączenie niektórych funkcji, itp.),
   4) konieczność schwytania i ewentualnego ukarania sprawcy (przy założeniu, że istnieją okoliczności umożliwiające takie działanie),
   5) konieczność angażowania zasobów systemu informatycznego (jaka część i jak długo),
   6) aspekt finansowy, organizacyjny i ludzki podejmowanych działań (jak długo działanie ma trwać, w

jakim stopniu zakłóca normalne funkcjonowanie Uczelni, jakie są tego koszty).

5. Przy ograniczaniu skutków incydentu ADO może korzystać z konsultantów zewnętrznych, jeśli Uczelnia wcześniej zawarła w umowach z tymi podmiotami stosowne zapisy o przekazywaniu i ochronie informacji Uczelni.

IV. ODTWARZANIE SYSTEMU

§ 4.

1. Z zastrzeżeniem ust. 4 niniejszego paragrafu, CASI przystępuje do odtworzenia systemu po zidentyfikowaniu i usunięciu lub zablokowaniu źródła naruszenia.
2. Odtwarzanie systemu odnosi się do punktu odtworzenia, co do którego CASI ma uzasadnioną pewność, że nie zawiera źródła naruszenia.
3. Zasoby w postaci oprogramowania oraz danych są odtwarzane z oryginalnych źródeł dystrybucji oprogramowania oraz kopii zapasowych.
4. ADO, po zasięgnięciu opinii IOD, może podjąć decyzję o podjęciu przetwarzania danych mimo braku pewności usunięcia źródła naruszenia, jeśli szacowane negatywne skutki braku przetwarzania przewyższają potencjalne ryzyko podjęcia działania.

V. DZIAŁANIA PO ZAKOŃCZENIU PROCEDURY NARUSZENIA

§ 5.

1. IOD, sporządza raport z naruszenia, zgodnie ze wzorem zamieszczonym w **załączniku nr 1** do niniejszej Procedury i przedstawia go ADO.
2. Jeśli zachodzi taka potrzeba, to CASI sporządza dodatkowy raport techniczny, stanowiący załącznik do raportu wskazanego w ust. 1 i zawierający co najmniej:
   1) rejestr incydentu, zawierający szczegółowe zapisy chronologiczne dotyczące kolejnych zdarzeń i podejmowanych działań,
   2) opis incydentu w aspekcie technicznym (zakres incydentu, części systemów dotknięte skutkami incydentu, rozmiar bezpośrednich szkód),
   3) kopie dzienników (logów zdarzeń, logów audytu) urządzeń, systemów operacyjnych i aplikacji w części systemów, która była dotknięta skutkami incydentu,
   4) kopię dziennika pracy systemu z okresu trwania incydentu,
   5) informacje o oryginalnych źródłach dystrybucji oprogramowania oraz kopiach zapasowych wykorzystanych do odtworzenia systemu,
   6) zakres informacji technicznych przekazanych Podmiotom zewnętrznym uczestniczącym w działaniach związanych z ograniczaniem skutków incydentu.

VI. REJESTROWANIE INFORMACJI O INCYDENTACH

§ 6.

1. IOD prowadzi rejestr naruszeń zawierający, w szczególności:
   1) źródło zgłoszenia;
   2) opis naruszenia,
   3) datę i godzinę stwierdzenia naruszenia,

4) datę i godzinę zgłoszenia do IOD;
5) dane identyfikujące osobę zgłaszającą,
6) liczbę osób, których dotyczy naruszenie,
7) dane identyfikujące osobę rejestrującą incydent,
8) informacje o zgromadzonych materiałach dowodowych,
9) informacje dotyczące sposobu postępowania z naruszeniem.

2. IOD zapewnia właściwe wykorzystanie informacji o naruszeniach związanych z ochroną danych dla doskonalenia systemu zarządzania bezpieczeństwem ochrony danych.

VII. GROMADZENIE MATERIAŁU DOWODOWEGO

§ 7.

1. Na każdym etapie postępowania z naruszeniem, IOD nadzoruje prawidłowość gromadzenia materiału dowodowego.
2. Każdy element materiału dowodowego - dokument papierowy, dokument elektroniczny, kopia zapasowa bazy danych lub plików systemowych i konfiguracyjnych, obraz dysku, dzienników (logów) zdarzeń, dzienników audytu - jest gromadzony i przechowywany w sposób gwarantujący jego poufność, integralność i kompletność.
3. Każdy element materiału dowodowego jest utrwalany z zachowaniem integralności całego procesu przetwarzania, od utworzenia do ewentualnego przedstawienia jako dowodu w postępowaniu sądowym:
   1) dla dokumentów papierowych - oryginał jest bezpiecznie przechowywany wraz z informacją o źródle, czasie i okolicznościach utrwalenia dokumentu,
   2) dla zapisów utrwalanych na nośnikach komputerowych - sporządzenie kopii zapasowej lub obrazu dysku wraz z udokumentowaniem procesu kopiowania oraz bezpieczne ich przechowanie (np. poza siedzibą Uczelni).
4. Zabezpieczenie środków przetwarzania danych jest przeprowadzane zgodnie z instrukcją zamieszczoną **w załączniku nr 2** do niniejszego regulaminu.
5. Protokół ze sporządzenia elementu materiału dowodowego lub zabezpieczenia środków przetwarzania danych jest sporządzany zgodnie ze wzorem zamieszczonym **w załączniku nr 3** do niniejszej procedury.
6. Wszelkie działania w systemie teleinformatycznym, związane z postępowaniem z naruszeniem, mogą być prowadzone wyłącznie z wykorzystaniem kopii zapasowych, obrazów dysków, kopii plików konfiguracyjnych i systemowych, rejestrów systemowych i aplikacji, plików dokumentów, identycznych ze sporządzonymi uprzednio kopiami przechowywanymi jako materiał dowodowy.

Załącznik nr 1 - Wzór raportu z naruszenia

Miejscowość, data ……..

RAPORT

(stwierdzenie wystąpienia naruszenia)

A. ZGŁOSZENIE Naruszenia (wypełnia osoba zgłaszająca)
DANE OSOBY ZGŁASZAJĄCEJ

Imię i nazwisko ..... Stanowisko służbowe .....

Adres .....

Nr telefonu ..... e-mail .....

OPIS NARUSZENIA:

Komu zgłoszono: ……..

Data i godzina zgłoszenia: ……..

Podpis osoby zgłaszającej ……..

B. DZIAŁANIA PO ZAISTNIENIU NARUSZENIA

(wypełnia osoba rozpatrująca zgłoszenie naruszenia)

DANE OSOBY, KTÓRA DOKONAŁĄ ZGŁOSZENIE NARUSZENIA

Imię i nazwisko..... Stanowisko .....

Adres .....

Nr telefonu.....e-mail .....

INFORMACJE O NARUSZENIU

Data i czas zaistnienia naruszenia.....

Data i czas wykrycia naruszenia.....

Data i czas zgłoszenia naruszenia .....

Czy incydent jest zakończony? TAK □ NIE □

Jeśli tak, to jak długo trwał (dni/godziny/minuty)? .....

Jeśli nie, należy określić jak długo już trwa? .....

Kogo powiadomiono z KIEROWNICTWA? .....

OPIS WSTĘPNY / PODJĘTE DZIAŁANIA / ZABEZPIECZENIE MATERIAŁU DOWODOWEGO

Załączniki (materiał dowodowy): 1.....

2 .....

3 .....

OPIS ROZWIĄZANIA PROBLEMU / KOSZTY ODTWORZENIA

Imię i Nazwisko

Data .....

Podpis .....

C. POSTĘPOWANIE WYJAŚNIAJĄCE/ ZAKOŃCZENIE NARUSZENIA

(wypełnia osoba prowadząca postępowanie wyjaśniające)

Data rozpoczęcia postępowania ws. naruszenia .....

Data zakończenia naruszenia (jeśli jest zakończony).....

Data zamknięcia skutków naruszenia .....

Data zakończenia postępowania ws. naruszenia .....

Data przedstawienia naruszenia Administratorowi.....

USTALENIA - OPIS POSTĘPOWANIA - SPRAWCY NARUSZENIA

(w tym opis postępowania dyscyplinarnego, jeśli takie ma miejsce)

WNIOSKI I REKOMENDACJE

(w tym zalecenia dotyczące zmian)

WYKAZ DOŁĄCZONYCH DOKUMENTÓW

DANE OSÓB PROWADZĄCYCH POSTĘPOWANIE WYJAŚNIAJĄCE

Imię i Nazwisko …….. Imię i Nazwisko…….

Stanowisko …….. Stanowisko ……..

Data …….. Data ……..

Podpis…….. Podpis ……..

Załącznik nr 2 – Instrukcja zabezpieczenia środków przetwarzania w sytuacji wystąpienia zdarzenia naruszenia ochrony danych

1. Odsunąć w sposób zdecydowany, ale taktowny całą obsługę od miejsca zdarzenia.
2. Na czas zabezpieczenia należy zabronić korzystania z pomieszczenia, w którym są przetwarzane dane osobowe/urządzeń komputerowych/łączności.
3. Jeśli urządzenie jest wyłączone, NIE WŁĄCZAĆ GO.
4. Jeśli urządzenie jest włączone, NIE próbować zamykać programów ani wyłączać komputera. Nie przerywać drukowania, zabezpieczyć, jeśli to możliwe, wykonane wydruki. Zanotować dokładnie wszystkie wiadomości, jakie pojawiają się na ekranie. Zanotować w miarę możliwości wszystkie parametry połączeń komputera:
   a) w przypadku połączenia modemowego, zanotować numer telefoniczny, adres IP komputera, adresy bramki wychodzącej oraz serwera DNS,
   b) w przypadku połączenia po sieci kablowej, zanotować typ połączenia, adres IP komputera, adresy bramki wychodzącej oraz serwera DNS,
   c) w przypadku połączenia po sieci bezprzewodowej, zanotować ustawienia zabezpieczenia sieci adres IP komputera, adresy bramki wychodzącej oraz serwera DNS.
5. Przed zabezpieczeniem zanotować, stan pomieszczenia/w jaki sposób poszczególne części stanowiska komputerowego są ze sobą połączone. Zrobić zdjęcia, wykonać opis połączeń wraz z opisem wyposażenia. Oznaczyć odpowiednio wszystkie przewody i połączenia.
6. Następnie ODŁĄCZYĆ WSZYSTIE KABLE ZEWNĘTRZNE KOMPUTERA. Zanotować czas odłączenia kabli.
7. Zabezpieczyć jednostkę centralną (komputer) oraz inne urządzenia z zainstalowaną na stałe pamięcią masową. WYPEŁNIĆ METRYCZKĘ, która powinna zawierać typ, numer seryjny urządzenia i numer inwentarzowy nadany przez Uczelnię albo opis jego indywidualnych cech. Wpisać do PROTOKOŁU wykonane czynności (załącznik nr 3 do niniejszej Procedury).
8. Zabezpieczyć wszystkie wymienne nośniki komputerowe: pamięci flash, taśmy streamera, płyty CD, DVD oraz niezamontowane dyski twarde (także uszkodzone). Grupy nośników zabezpieczyć zbiorczo (dyskietki, płyty CD itp). Jeśli urządzenia są spakowane to NUMERUJ poszczególne paczki, ZAPLOMBOWAĆ I OPISAĆ W PROTOKOLE. Wpisać do PROTOKOŁU wykonane czynności.
9. Wskazać osobę upoważnioną, która zarządza licencjami i oryginalnymi nośnikami oprogramowania i miejsce ich przechowywania. Oznaczenia licencji i nośników należy wpisać do protokołu, a następnie zabezpieczyć jako materiał porównawczy.
10. Zabezpiecz jako materiał porównawczy instrukcje programów pisanych na zamówienie lub programów nietypowych (np. FK). Wpisać do protokołu wykonane czynności.
11. Zabezpieczyć parametry dostępu do BIOS-u, systemu operacyjnego i oprogramowania (kont, haseł, identyfikatorów, itp.) za pomocą bezpiecznej koperty. Wpisać czynność przejęcia parametrów dostępu do protokołu.
12. Przechowywać zabezpieczone materiały (nośniki i sprzęt) w miejscach suchych i chłodnych z daleka od urządzeń emitujących pole elektromagnetyczne.

PAMIĘTAJ:

NIE PRÓBUJ SAMODZIELNIE BADAĆ KOMPUTERA, ANI ZAWARTOŚCI NOŚNIKÓW DANYCH.

KAŻDE TWOJE WŁĄCZENIE KOMPUTERA PO ZAKOŃCZENIU ZABEZPIECZENIA WYWOŁUJE POWSTANIE ŚLADÓW WSKAZUJĄCYCH NA NARUSZENIE INTEGRALNOŚCI MATERIAŁU BADAWCZEGO.

Załącznik nr 3 - Wzór protokołu zabezpieczenia materiału dowodowego

PROTOKÓŁ ZABEZPIECZENIA MATERIAŁU DOWODOWEGO

Wykonano w dniu.....o godzinie..... w obecności:

Świadek 1: <imię i nazwisko, stanowisko, komórka organizacyjna Uczelni>
Świadek 2: <imię i nazwisko, stanowisko, komórka organizacyjna Uczelni>
Świadek 3: <imię i nazwisko, niezależny ekspert>

I. Rodzaj materiału dowodowego

(zaznaczyć właściwe kwadraty i wpisać odpowiednie nazwy i oznaczenia)

Zaznacz właściwy kwadrat		*Rodzaj/Nazwa/Wersja/Oznaczenie nośnika*
	Dokument papierowy	
	Dokument elektroniczny	
	Kopia zapasowa	
	System operacyjny	
	Aplikacja	
	Baza danych	
	Obraz dysku	
	Lokalizacja dysku (adres IP/IPX):	
	Typ i nr seryjny dysku:	
	Pliki konfiguracyjne i/lub systemowe	
	System operacyjny	
	Aplikacja	
	Baza danych	
	Baza danych	
	Kopie zawartości dzienników (logów) zdarzeń	
	System operacyjny	
	Aplikacja	
	Baza danych	
	Nazwa(y) Pliku(ów)	
	Kopia zawartości skrzynki pocztowej	
	Zewnętrzna: zakres od:	
	Wewnętrzna: zakres od:	

II. Opis czynności
(opisać kolejne czynności z zaznaczeniem Wykonawcy(ów))

III. Wytworzony materiał dowodowy

Wykonano kopie materiału dowodowego w 2 egzemplarzach, którym nadano etykiety:

„....., Egzemplarz nr 1”

„....., Egzemplarz nr 2”
(wprowadzić krótkie oznaczenie zabezpieczonego materiału dowodowego, zgodnie z kategorią wskazaną w pkt. I, datą i godziną wykonania)

IV. Zabezpieczenie materiału dowodowego
(opisać sposób zabezpieczenia jednego z egzemplarzy)

Protokół sporządził:

Podpisano:

Świadek 1 ……..

Świadek 2 ……..

Świadek 3 ……