Procedura zarządzania incydentami związanymi z bezpieczeństwem informacji w Państwowej Wyższej Szkole Filmowej, Telewizyjnej i Teatralnej im. L. Schillera w Łodzi

§ 1.
Cel procedury

Celem procedury zarządzania incydentami związanym z bezpieczeństwem informacji jest zapewnienie, że zdarzenia związane z bezpieczeństwem informacji świadczące o słabości systemów informatycznych są zgłoszone w sposób umożliwiający szybkie podjęcie działań korygujących. Ma ona również na celu zapewnienie ciągłości operacyjnej oraz ograniczenie wpływu przypadków naruszeń bezpieczeństwa zasobów informacyjnych, w tym bezpieczeństwa przetwarzania danych osobowych, na działalność Państwowej Wyższej Szkoły Filmowej, Telewizyjnej i Teatralnej im. L. Schillera w Łodzi zwanej dalej Uczelnią. Z niniejszej procedury wyłączone są informacje niejawne dla których stosowane są odrębne przepisy.

§ 2.
Zakres stosowania

Procedura zarządzania incydentami związanymi z bezpieczeństwem informacji obowiązuje we wszystkich jednostkach organizacyjnych Uczelni (na wszystkich Wydziałach i we wszystkich jednostkach administracyjnych Uczelni). Procedura obowiązuje również podmioty zewnętrzne, które dopuszczono do przetwarzania danych, w tym danych osobowych będącymi zasobami informacyjnymi Uczelni.

§ 3.
Odpowiedzialność

1. Odpowiedzialność za prawidłowe zgłoszenie incydentów dotyczących bezpieczeństwa infrastruktury teleinformatycznej w Uczelni spoczywa na pracownikach, użytkownikach i administratorach systemów oraz podmiotach zewnętrznych współpracujących z Uczelnią dokonujących zgłoszenia.
2. Osoby odpowiedzialne za rozwiązanie problemu lub zapobieżeniu incydentom w ramach swoich uprawnień działają zgodnie z niniejszą procedurą.

1. Administrator Danych (AD)

Administratorem Danych dalej zwanym AD jest Państwowa Wyższa Szkoła Filmowa, Telewizyjna i Teatralna im. Leona Schillera w Łodzi reprezentowana przez Rektora. Dotyczy to szczególnie danych osobowych w rozumieniu RODO oraz innych danych gromadzonych i zarządzanych w systemach informatycznych Uczelni.

AD, w ramach wykonywania swoich uprawnień, dokonuje następujących czynności:

a) zatwierdza procedurę zarządzania incydentami obowiązującą w Uczelni,
b) wyznacza osoby odpowiedzialne za proces zarządzania incydentami w Uczelni,
c) podejmuje decyzję w sprawie zgłoszenia incydentu organom uprawnionym w nadzorze cyberbezpieczeństwa i ochrony danych osobowych w Państwie,
d) podejmuje inicjatywy w zakresie rozwoju kultury bezpieczeństwa informacji w Uczelni.

2. Administrator Systemów Informatycznych (ASI).

Administratorem Systemów Informatycznych jest osoba zobowiązana do zarządzania systemami informatycznymi Uczelni wykorzystywanymi do przetwarzania danych osobowych. Jej podstawowym zadaniem jest bieżąca współpraca z Inspektorem Ochrony Danych mająca na celu ochronę przetwarzanych przez Uczelnię danych osobowych w zakresie zabezpieczeń teleinformatycznych. W ramach wykonywania swoich uprawnień, dokonuje następujących czynności:

a) usuwa na bieżąco skutki zgłoszonych incydentów,
b) sporządza kwartalny raport dotyczący ilości i kategorii zgłaszanych incydentów,
c) współpracuje z Inspektorem Ochrony Danych (IOD) w gromadzeniu materiału dowodowego w przypadku wystąpienia incydentów, w tym w szczególności związanych z bezpieczeństwem danych osobowych (zdarzenia większej wagi),
d) prowadzi rejestr incydentów bezpieczeństwa informacji w Uczelni.

3. Inspektor Ochrony Danych (IOD).

Inspektorem Ochrony Danych Osobowych jest osoba powoływana przez administratora do pomocy przy przestrzeganiu w Uczelni przepisów o ochronie danych osobowych. IOD pełni rolę pośrednika pomiędzy zainteresowanymi podmiotami (Urzędem Ochrony Danych Osobowych, podmiotem przetwarzającym dane oraz osobą, której dane są przetwarzane).

W ramach wykonywania swoich uprawnień, dokonuje następujących czynności:

a) prowadzi postępowanie wyjaśniające z Kanclerzem Uczelni dotyczące przyczyn incydentu oraz ustala ewentualnych sprawców jego wystąpienia,
b) przedstawia AD wnioski po zakończeniu postępowania wyjaśniającego w zakresie ustalenia przyczyn i okoliczności incydentu, a także wskazania osoby/osób odpowiedzialnych za incydent oraz sposobów przeciwdziałania wystąpienia podobnym incydentom w przyszłości,
c) sporządza półroczny raport ze zgłoszonych w tym okresie incydentów (zdarzenia większej wagi) z określeniem głównych przyczyn wstąpienia tych incydentów, zakresu szkód jakie z określeniem głównych przyczyn wstąpienia tych incydentów, zakresu szkód jakie wyrządziły oraz propozycji działań zaradczych w celu uniknięcia takich zdarzeń w przyszłości,
d) dokonuje zgłoszeń incydentów w instytucjach centralnych odpowiedzialnych za zarządzanie incydentami, a w zakresie incydentów dot. danych osobowych do Prezesa Urzędu Ochrony Danych Osobowych (PUODO),
e) opiniuje projekty procedur lub praktyk właściwego działania minimalizujące ryzyko wystąpienia incydentów bezpieczeństwa informacji w przyszłości,
f) ocenia istnienie potencjalnych zagrożeń w zakresie bezpieczeństwa informacji,
g) wnioskuje do Kanclerza Uczelni w sprawie podejmowania działań zmierzających do wzrostu świadomości w zakresie zapewnienia bezpieczeństwa informacji w Uczelni.

§ 4.
Klasyfikacja incydentów

1. Incydent bezpieczeństwa informacji to zdarzenie, którego skutkiem jest lub może być naruszenie bezpieczeństwa aktywów informacyjnych. Jego przyczyną może być:
   1) zdarzenie mniejszej wagi mające związek z nieprawidłowym działaniem infrastruktury technicznej (np. klimatyzacji, wentylacji, centralnego ogrzewania, urządzeń biurowych), informatycznej (sprzęt informatyczny) oraz systemów lub pojedynczych aplikacji nie mających wpływu na bezpośrednie naruszenie bezpieczeństwa informacji, a w szczególności danych osobowych. Zdarzenia te nie mają bezpośredniego wpływu na zachowanie informacyjnej ciągłości działania Uczelni;
   2) zdarzenie większej wagi mające bezpośredni wpływ na zachowanie informacyjnej ciągłości działania Uczelni, w tym stanowiące naruszenie ochrony danych osobowych skutkujące koniecznością powiadomienia Organu Nadzoru Ochrony Danych Osobowych (PUODO). W szczególności mogą to być:
      a) zdarzenie losowe zewnętrzne (np. klęski żywiołowe, pożary nagłe przerwy w zasilaniu), ich występowanie może prowadzić do utraty danych (np. trwała utrata danych, częściowa lub całkowita) także dokumentacji papierowej,
      b) zdarzenie losowe wewnętrzne (np. niezamierzone pomyłki pracowników, administratorów, awarie sprzętowe, błędy w oprogramowaniu) które mogą powodować zakłócenia ciągłości pracy systemów a także prowadzić do zniszczenia częściowego lub całkowitego danych,
      c) zdarzenie losowe wewnętrzne związane z informacjami przetwarzanymi w sposób tradycyjny (np. przypadkowe uszkodzenie, zagubienie, całkowite zniszczenie dokumentów papierowych zawierających dane osobowe lub dane ważne dla funkcjonowania Uczelni lub jej wizerunku),
      d) zdarzenie zamierzone, świadome i celowe mające na celu naruszenie poufności zasobów informacyjnych, w tym poufności danych osobowych:
         - nieuprawniony dostęp do danych z zewnątrz (włamania do systemów Uczelni),
         - nieuprawniony dostęp do danych z sieci wewnętrznej,
         - nieuprawnione transfery danych,
         - zainfekowanie sprzętu lub oprogramowania w celu uszkodzenia lub kradzieży danych (np. działanie złośliwego oprogramowania typu: malware, ransomware),
         - bezpośrednie zagrożenia materialnych elementów systemu (np. kradzież sprzętu),
         - celowa próba naruszenia integralności systemu lub bazy danych (sabotaż),
         - próba lub modyfikacja danych lub zmiana w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),
         - niedopuszczalna manipulacja danymi w systemie,
         - ujawnienie osobom nieupoważnionym danych osobowych lub objętych tajemnicą elementów systemu zabezpieczeń,
         - praca w systemie lub sieci komputerowej wykazuje odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony danych osobowych, np. praca w systemie lub sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym i nieautoryzowanym logowaniu się itp.,

- zmiana lub zniszczenie nośników z danymi bez odpowiedniego upoważnienia lub skopiowanie danych osobowych w niedozwolony sposób,
- zdarzenie związane z rażącym naruszeniem dyscypliny pracy (np. niewykonanie w ustalonym terminie kopii bezpieczeństwa, prace bez zgody na danych osobowych w celach prywatnych, itp.) mające wpływ na bezpieczeństwo informacji;
- celowe przełamanie tradycyjnych zabezpieczeń miejsc przechowywania danych, w tym także osobowych (np. nieuprawnione otwarcie szafy, regału, biurka, pomieszczenia);
- działania powodujące awarię sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, także niewłaściwe działanie systemu.

2. Incydentami bezpieczeństwa informacji w szczególności są:
   1) naruszenie poufności, to jest ujawnienie informacji niepowołanym osobom;
   2) naruszenie integralności, to jest zniszczenie, uszkodzenie lub przekłamanie informacji;
   3) naruszenie dostępności, to jest braku dostępu do danych przez uprawnionych użytkowników.
3. Przyczyny incydentów bezpieczeństwa informacji mogą dotyczyć:
   1) niewłaściwego wykorzystywania zasobów informatycznych lub niewłaściwe postępowanie z dokumentacją papierową;
   2) działania szkodliwego oprogramowania;
   3) próby omijania systemów zabezpieczeń;
   4) nieautoryzowanego dostępu do systemów, aplikacji i dokumentów;
   5) zniszczenia lub kradzieży urządzeń wykorzystywanych do przetwarzania i przechowywania informacji;
   6) zniszczenia lub kradzieży nośników danych;
   7) próby wyłudzeń informacji;
   8) ataków socjotechnicznych, ataków z wykorzystaniem technik zagrażających poufności, integralności lub dostępności informacji;
   9) nieprawidłowości w zakresie zabezpieczenia przechowywania danych, w tym danych osobowych;
   10) naruszenia zasad obowiązujących w Uczelni dotyczących bezpieczeństwa informacji, w tym danych osobowych (np. pozostawienie włączonego komputera, nie wylogowanie się po zakończeniu pracy lub podczas przerwy w pracy, pozostawienie niezabezpieczonych dokumentów drukowanych zawierających dane osobowe itp.).

§ 5.
Zgłaszanie incydentów

1. Pracownicy Uczelni mają obowiązek zgłaszania zauważonych przez siebie incydentów oraz notowania wszystkich szczegółów związanych z incydentem. Naruszenie bezpieczeństwa zasobów informacyjnych Uczelni, w tym bezpieczeństwa przetwarzania 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.

2. Zgłoszenie musi zawierać:
   1) imię nazwisko zgłaszającego,
   2) jednostka organizacyjna Uczelni lub nazwa podmiotu zewnętrznego,
   3) miejsce i datę wystąpienia incydentu,
   4) opis zdarzenia w sposób adekwatny do posiadanej wiedzy i umiejętności zgłaszającego.
3. Brak umiejętności poprawnego rozpoznania incydentu przez osobę zgłaszającą nie może być przyczyną zaniechania zgłoszenia.
4. Zdarzenia mniejszej wagi winny być zgłaszane za pośrednictwem poczty elektronicznej na adres **incydent@filmschool.lodz.pl**. W przypadku niedostępności systemu pocztowego zgłoszenia należy dokonać telefonicznie lub osobiście ASI. Po przywróceniu dostępności systemów zgłaszający zobowiązany jest do uzupełnienia zgłoszenia za pośrednictwem poczty elektronicznej.
5. Zdarzenia większej wagi winny być zgłaszane za pośrednictwem poczty elektronicznej na adres **incydent@ filmschool.lodz.pl.**
6. Zgłoszenia należy dokonać na formularzu zgłoszenia stanowiącym załącznik nr 1 do niniejszej procedury wraz z posiadanymi dowodami zaistniałego zdarzenia. Dotyczy to zwłaszcza naruszenia ochrony danych osobowych.
7. IOD w uzgodnieniu z AD bez zbędnej zwłoki w terminie 72 godzin po stwierdzeniu naruszenia, jest zobowiązany zgłosić takie naruszenie organowi nadzorczemu – Prezesowi Urzędu Ochrony Danych Osobowych (PUODO), chyba że jest mało prawdopodobne, by takie naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.
8. Zgłaszający incydent nie powinien podejmować żadnych działań na własną rękę jednak w miarę możliwości powinien zabezpieczyć materiał dowodowy, np. w postaci zdjęć ekranu komputera co do którego zaistniało podejrzenie, że jego działanie odbiega od normy.

§ 6.
Postępowanie z incydentami

1. Obsługę incydentu rozpoczyna się od jego dokładnego rozpoznania - ustalenia oznak naruszenia bezpieczeństwa, identyfikacji rodzaju incydentów, identyfikacji zabezpieczania dowodów oraz poinformowania o zdarzeniu odpowiednich osób. Osoba zgłaszająca incydent powinna w miarę możliwości zabezpieczyć materiał dowodowy (np. zrzut ekranu monitora, zdjęcie niezabezpieczonych materiałów zawierających dane osobowe itp.).
2. ASI który otrzymuje zgłoszenie mniejszej wagi zgodnie z nadanym mu priorytetem w najszybszym możliwym terminie usuwa skutki zaistniałego incydentu.
3. W przypadku, jeżeli otrzymane przez niego zgłoszenie wyczerpuje opis zdarzenia większej wagi, dokonuje na jego podstawie zgłoszenia zgodnie z ścieżką działania dla tego typu zdarzeń, opisaną w § 5.
4. Po usunięciu skutków incydentu Kanclerz Uczelni zamyka zgłoszenie, o czym jest informowany zgłaszający.
5. W przypadku zgłoszenia incydentu większej wagi, ASI przekazuje zgłoszenie także do Kanclerza Uczelni oraz IOD.
6. ASI odpowiada za zabezpieczenie materiału dowodowego. Zawiadamia o zgłoszeniu IOD i przesyła mu drogą elektroniczną, w postaci zaszyfrowanej, zgromadzone materiały

dotyczące zaistniałego incydentu dotyczącego danych osobowych, w szczególności formularz zgłoszenia. W dalszej kolejności odnotowuje zgłoszony incydent w rejestrze incydentów stanowiącym załącznik nr 2 do procedury.

7. IOD dokonuje analizy materiału dowodowego i podejmuje decyzje o sposobie dalszego postępowania, w szczególności dalszego prowadzenia postępowania, w tym gromadzenia materiału dowodowego.
8. IOD dokonuje oceny istotności incydentu. W przypadku incydentu o znacznym zagrożeniu bezpieczeństwa informacji, szczególnie danych osobowych, zawiadamia AD o zaistnieniu incydentu oraz poziomie zagrożenia bezpieczeństwa informacji. Oceniając poziom istotności incydentu IOD kieruje się m.in. następującymi kryteriami:
   1) wpływ incydentu na ciągłość działania Uczelni oraz realizację zadań;
   2) krytyczność systemów dotkniętych skutkami incydentu bezpieczeństwa;
   3) wrażliwość informacji, których poufność integralność i dostępność naruszono (np. czy naruszono bezpieczeństwo informacji prawnie chronionej – np.: danych osobowych, informacji niejawnych);
   4) rozległość wpływu incydentu na działanie systemów;
   5) rozmiar szkód powstałych wskutek incydentu;
   6) koszty usunięcia i naprawy skutków incydentu bezpieczeństwa;
   7) szacowany czas przywrócenia ciągłości działania dotkniętego incydentem systemu;
   8) bezpieczeństwo systemu;
   9) zasoby wymagane do przywrócenia ciągłości działania systemu (personel, wsparcie firm zewnętrznych, wymagane dodatkowe czy zamienne urządzenia oraz oprogramowanie, czas tworzenia systemów kopii zapasowych itp.).
9. W przypadku, jeżeli na terenie Rzeczpospolitej Polskiej zostanie ogłoszony jeden z poziomów alarmów terrorystycznych CRP (ALFA, BRAVO, CHARLIE, DELTA), a zgłoszony incydent wypełnia przesłanki uznania go za terrorystyczny lub mający wpływ na infrastrukturę krytyczną Państwa (Rzeczpospolitej), IOD dokonuje jego zgłoszenia odpowiednim służbom zgodnie z przyjętą procedurą. W przypadku, jeżeli IOD jest niedostępny, to zgłoszenia powinien dokonać Kanclerz Uczelni w uzgodnieniu z AD.
10. Jeżeli istotność incydentu jest wysoka i może mieć wpływ na wystąpienie podobnego incydentu lub spowodowanie innego incydentu przez to samo zagrożenie w innym podmiocie publicznym IOD zawiadamia rządowy zespół reagowania na incydenty komputerowe CERT. Zgłoszenie wysyła na adres cert@cert.pl lub zgłasza telefonicznie. W przypadku, jeżeli IOD jest niedostępny, to zgłoszenia powinien dokonać Kanclerz Uczelni w uzgodnieniu z AD.
11. W przypadku, gdy zgłoszony incydent w obszarze bezpieczeństwa danych osobowych, jako zdarzenie większej wagi zostanie przez IOD uznane za zdarzenie mniejszej wagi, to zamyka on sprawę, o czym powiadamia Kanclerza Uczelni i osobę zgłaszającą. Zamknięcie winno być odnotowane w rejestrze incydentów.
12. 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.

13. 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.
14. 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 i przygotowuje stosowne dokumenty.
15. Jeżeli zawiadomienie osób, których dane dotyczą wymagałoby niewspółmiernie dużego wysiłku, IOD przygotowuje publiczny komunikat lub wybiera inny stosowny środek, za pomocą którego zawiadomienie zostanie tym osobom przekazane.
16. W przypadku stwierdzenia działań umyślnych i ustalenia sprawcy incydentu, IOD przekazuje wyniki analizy wraz z zabezpieczonym materiałem dowodowym AD w celu wyciągnięcia konsekwencji służbowych wobec sprawcy(ów), ewentualnego zawiadomienia organów ścigania lub podjęcie kroków prawnych wobec osób trzecich.
17. W przypadku braku ustalenia sprawcy(ów) powstania incydentu w obszarze bezpieczeństwa danych osobowych lub przyczyn incydentu związanych z zdarzeniem losowym, IOD kończy analizę zgłoszenia formułując zalecania podjęcia konkretnych działań lub określonych zachowań dla pracowników Uczelni lub podmiotów zewnętrznych, które przekazuje w formie pisemnej Kanclerzowi Uczelni.
18. IOD sporządza półroczny raport ze zgłoszonych w tym okresie incydentów w zakresie bezpieczeństwa danych osobowych (zdarzenia większej wagi) z określeniem głównych przyczyn wstąpienia tych incydentów, zakresu szkód jakie wyrządziły oraz propozycji działań zaradczych w celu uniknięcia takich zdarzeń w przyszłości.
19. IOD na bieżąco dokumentuje swoje działania na każdym etapie procesów zarządzania incydentem w obszarze bezpieczeństwa danych osobowych, w formie notatek służbowych oraz korespondencji elektronicznej lub tradycyjnej.

§ 7.
Szkolenia

1. Brak wiedzy i umiejętności poprawnego rozpoznawania klasyfikacji oraz oceny poziomu i istotności incydentów zgodnie ze zgłoszeniem nie powinien być przyczyną zaniechania takich zgłoszeń, chociażby z samego podejrzenia wystąpienia incydentu.
2. W miarę posiadanych zasobów, co najmniej raz w roku należy przeprowadzić okresowe szkolenia pracowników Uczelni w zakresie zarządzania incydentami. Niezależnie od prowadzonych szkoleń wskazane jest przeprowadzenie szkoleń dla każdego nowo zatrudnionego pracownika celem zapewnienia znajomości zasad prawidłowego zgłaszania incydentów.

Załączniki:
załącznik nr 1 - zgłoszenie incydentu.
załącznik nr 2 - rejestru incydentów bezpieczeństwa informacji.

Załącznik nr 1 do Procedury zarządzania incydentami związanymi z bezpieczeństwem informacji.

Zgłoszenie incydentu

data: ..... **godzina: .....**

osoba zgłaszająca:

kontakt tel.: .....

kontakt mailowy: .....

Opis zdarzenia (czego dotyczy - np. obsługi systemu, sprzętu informatycznego, poczty elektronicznej itp.)	Jakie dowody dołączono do zgłoszenia? (mogą to być np.: zrzut ekranu, link, kopia poczty elektronicznej, opis komunikatu w systemie etc.)

Załącznik nr 2 do Procedury zarządzania incydentami związanymi z bezpieczeństwem informacji.

REJESTR INCYDENTÓW BEZPIECZEŃSTWA INFORMACJI

nr kolejny	krótki opis incydentu	czy incydent mniejszej wagi, czy większej wagi (M/W)	czy dołączono dokumenty w sprawie (zrzut ekranu, zapisy komunikatów etc.) (T/N)	data, godzina zgłoszenia	kto zgłosił	osoba obsługująca incydent	czy incydent naruszył ochronę danych osobowych (T/N)	czy powiadomiono o incydencie IOD, instytucje zewnętrzne (cert.gov.pl, PUODO)	kiedy i w jaki sposób usunięto skutki incydentu	podjęte działania korygujące - zmiany w zasadach bezpieczeństwa	data, godzina zamknięcia obsługi incydentu	uwagi