Załącznik Nr 3
do Zarządzenia Rektora Nr …. z dnia

Procedura zarządzania incydentami z zakresu bezpieczeństwa informacji i systemów IT w Uniwersytecie Przyrodniczym we Wrocławiu

Wrocław 2019

Rozdział 1. Skróty i definicje 3
Rozdział 2. Cel 3
Rozdział 3. Ogólne zasady 3

Rozdział 1. Skróty i definicje

§ 1

Uczelnia – Uniwersytet Przyrodniczy we Wrocławiu

Administrator Danych (AD) – Uniwersytet Przyrodniczy we Wrocławiu, reprezentowany przez Rektora

IOD – Inspektor Ochrony Danych

CSK – Centrum Sieci Komputerowych

Administrator Systemów Informatycznych (ASI) – pracownik administrujący określonym systemem IT. Rolą ASI jest zapewnienie efektywnego zarządzania operacyjnego danego systemu IT i sprawnej jego pracy. Do typowych zadań administratora należy nadzorowanie pracy powierzonych systemów IT, zarządzanie kontami i uprawnieniami użytkowników (na poziomie systemowym), konfiguracja zasobu, instalowanie i aktualizacja oprogramowania, nadzorowanie, wykrywanie i eliminowanie błędów oraz nieprawidłowości, asystowanie i współpraca z zewnętrznymi specjalistami przy pracach instalacyjnych, konfiguracyjnych i naprawczych, a także zapewnienie aktualności dokumentacji takiego zasobu obejmującego również dokumentację zmian mających bezpośredni wpływ na jego funkcjonalność. ASI odpowiada za właściwą i aktualną informację o systemach.

Jednostki organizacyjne – jednostki, o których mowa w § 8 Regulaminu organizacyjnego UPWr. tj. wydziały, jednostki organizacyjne wchodzące w skład wydziałów, jednostki ogólnouczelniane, międzywydziałowe i pozawydziałowe oraz wspólne, a także jednostki administracyjne i samodzielne stanowiska.

Kierownik jednostki organizacyjnej – osoba kierująca jednostką organizacyjną UPWr.

Rozdział 2. Cel

§ 2 Cel

Procedura zarządzania incydentami z zakresu bezpieczeństwa informacji i systemów IT ma na celu zapewnienie ciągłości operacyjnej oraz ograniczenie wpływu przypadków naruszeń bezpieczeństwa zasobów informacyjnych, w tym bezpieczeństwa przetwarzania danych osobowych na działalność Uniwersytetu Przyrodniczego we Wrocławiu.

Z niniejszej procedury wyłączone są informacje niejawne, dla których stosowane są odrębne przepisy.

Rozdział 3. Ogólne zasady

§ 3 Kategorie incydentów

1. Incydent bezpieczeństwa informacji i systemów IT to zdarzenie, którego skutkiem jest lub może być naruszenie bezpieczeństwa aktywów informacyjnych. Jego przyczyną może być:

a) zdarzenie losowe zewnętrzne (np. klęski żywiołowe, pożary, zakłócenia w dostawie energii elektrycznej itp.), którego wystąpienie może powodować zniszczenie lub uszkodzenie infrastruktury informatycznej oraz zakłócenie ciągłości pracy systemów nie powodując naruszenia poufności danych,
b) 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,
c) świadome i celowe działania mające na celu naruszenie poufności zasobów informacyjnych, w tym poufności danych osobowych.

2. Incydentami bezpieczeństwa informacji i systemów IT w szczególności są:
   a) naruszenie poufności, tj. ujawnienie informacji niepowołanym osobom,
   b) naruszenie integralności, tj. zniszczenie, uszkodzenie lub przekłamanie informacji,
   c) naruszenie dostępności, tj. braku dostępu do danych przez uprawnionych użytkowników.
3. Przyczyny incydentów bezpieczeństwa informacji i systemów IT mogą dotyczyć:
   a) niewłaściwego wykorzystywania zasobów informatycznych lub niewłaściwe postępowanie z dokumentacją papierową,
   b) działania szkodliwego oprogramowania,
   c) próby omijania systemów zabezpieczeń,
   d) nieautoryzowanego dostępu do systemów, aplikacji i dokumentów,
   e) zniszczenia lub kradzież urządzeń wykorzystywanych do przetwarzania i przechowywania informacji,
   f) zniszczenia lub kradzież nośników danych,
   g) próby wyłudzenia informacji,
   h) ataków socjotechnicznych, ataków z wykorzystaniem technik zagrażających poufności, integralności lub dostępności informacji,
   i) nieprawidłowości w zakresie zabezpieczenia przechowywania danych, w tym danych osobowych,
   j) naruszenia zasad obowiązujących w Uczelni dotyczących bezpieczeństwa informacji, w tym danych osobowych (np. pozostawienie włączonego komputera i / lub nie wylogowanie się po zakończeniu pracy lub podczas przerwy w pracy.).

§ 4 Zakres obowiązywania procedury zarządzania incydentami w zakresie bezpieczeństwa informacji i systemów IT

Procedura zarządzania incydentami w zakresie bezpieczeństwa informacji i systemów IT obowiązuje we wszystkich jednostkach organizacyjnych Uczelni. Procedura obowiązuje również podmioty zewnętrzne, które dopuszczono do przetwarzania danych, w tym danych osobowych będącymi zasobami informacyjnymi Uczelni.

W przypadku uzyskania informacji o wystąpieniu incydentu bądź podejrzenie naruszenia bezpieczeństwa informacji i systemów IT w Uniwersytecie Przyrodniczym we Wrocławiu, każdy

pracownik ma obowiązek niezwłocznie poinformować, o tym fakcie kierownika jednostki organizacyjnej, w której jest zatrudniony.

§ 5 Zgłaszanie incydentów z zakresu bezpieczeństwa systemów IT

1. Naruszenie bezpieczeństwa systemów IT w Uczelni należy zgłaszać do Dyrektora CSK. Osoba zgłaszająca odpowiada za wyczerpujący opis incydentu odpowiednio do posiadanej wiedzy i umiejętności.
2. Zgłoszenie musi zawierać następujące informacje:
   a) imię i nazwisko osoby zgłaszającej,
   b) jednostkę organizacyjną Uczelni lub nazwę podmiotu zewnętrznego,
   c) miejsce i datę wystąpienia incydentu,
   d) opis incydentu.
3. Brak umiejętności poprawnego rozpoznania incydentu przez osobę zgłaszającą nie może być przyczyną zaniechania zgłoszenia.
4. Dyrektor CSK niezwłocznie zgłasza incydent Inspektorowi Ochrony Danych (IOD)

§ 6 Podejmowanie działań w związku ze zgłaszanymi incydentami z zakresu bezpieczeństwa informacji i systemów IT

1. Zgłoszenie incydentu rejestrowane jest przez CSK w wewnętrznym rejestrze.
2. Osoba zgłaszająca incydent powinna w miarę możliwości zabezpieczyć materiał dowodowy.
3. Działania związane z obsługą zgłoszenia w pierwszej kolejności dotyczą rozpoznania i kwalifikacji zgłoszenia. W przypadku, kiedy zgłoszenie zakwalifikowane zostało jako incydent bezpieczeństwa informacji, dokonywana jest jego ocena istotności. Powyższe działania wykonuje Dyrektor CSK w porozumieniu z IOD.
4. Przy ocenie istotności incydentu pod uwagę brane są następujące czynniki:
   1) powstałe szkody będące wynikiem incydentu,
   2) wpływ incydentu na działanie systemów,
   3) wpływ incydentu na prawidłowe funkcjonowanie Uczelni,
   4) koszty usunięcia skutków incydentu,
   5) szacowany czas naprawy skutków wywołanych incydentem,
   6) oszacowanie zasobów koniecznych do przywrócenia ciągłości działania systemów.
5. Zakwalifikowanie zgłoszenia incydentu jako nienaruszającego bezpieczeństwo informacji kończy postępowanie, o czym IOD informuje zgłaszającego.
6. W przypadku zakwalifikowania zdarzenia jako incydentu związanego z bezpieczeństwem informacji, Dyrektor CSK w porozumieniu z IOD podejmuje działania zabezpieczające i naprawcze zmierzające do zniwelowania szkód powstałych w wyniku incydentu.

7. W przypadku, gdy incydent dotyczy systemów informatycznych i zakwalifikowany jest jako wysoki, Dyrektor CSK zawiadamia Wrocławskie Centrum Sieciowo-Superkomputerowe (na podstawie zawartej umowy).
8. Poinformowany o wynikach analizy incydentu oraz podjętych działaniach naprawczych IOD informuje o tym fakcie Rektora.
9. W przypadku stwierdzenia działań zamierzonych, przy jednoczesnym zidentyfikowaniu sprawcy incydentu, Rektor podejmuje decyzję dotyczącą wyciągnięcia ewentualnych konsekwencji dyscyplinarnych wobec sprawcy incydentu będącego pracownikiem UPWr.
10. W przypadku wykrycia incydentu noszącego znamiona przestępstwa należy powiadomić organy ścigania.
11. Powyższe działania raportowane są w rejestrze incydentów związanych z bezpieczeństwem informacji i systemów IT.

§ 7 Podejmowanie działań w związku ze zgłaszanymi incydentami naruszenia bezpieczeństwa przetwarzania danych osobowych

Podejmowanie działań oraz zgłoszenie incydentu związanego z naruszeniem ochrony danych osobowych odbywa się zgodnie z „Procedurą dokumentowania i zgłaszania naruszeń bezpieczeństwa ochrony danych osobowych w Uniwersytecie Przyrodniczym we Wrocławiu" (Zał. Nr 3 do Zarządzenia Rektora Nr 11/2019 z 21.01.2019 r.).