Załącznik nr 2
do Zarządzenia Rektora nr ….. z dnia ….

INSTRUKCJA BEZPIECZEŃSTWA IT

UNIWERSYTETU PRZYRODNICZEGO WE WROCŁAWIU

Spis treści

Rozdział 1. Cel

§ 1

1. Celem wprowadzenia Instrukcji Bezpieczeństwa IT, zwanej dalej Instrukcją, jest stworzenie warunków do skutecznej i efektywnej ochrony informacji oraz Zasobów IT w Uczelni poprzez:
   1.1. Zarządzanie bezpieczeństwem IT zgodnie z obowiązującymi przepisami prawa oraz zasadami określonymi niniejszą Instrukcją i poniższymi aktami tj:
      1.1.1. Polityką Bezpieczeństwa Informacji i Systemów IT Uniwersytetu Przyrodniczego we Wrocławiu zwaną dalej (PBIiSIT),
      1.1.2. Metodyką szacowania ryzyka dla systemów IT Uniwersytetu Przyrodniczego we Wrocławiu,
      1.1.3. Procedura zarządzania incydentami z zakresu bezpieczeństwa informacji i systemów IT w Uniwersytecie Przyrodniczym we Wrocławiu,
      oraz dokumentami powiązanymi:
      1.1.4. Polityką Ochrony Danych Osobowych Uniwersytetu Przyrodniczego we Wrocławiu,
      1.1.5. Procedurą zarządzania dostępami i upoważnieniami do przetwarzania danych w Uniwersytecie Przyrodniczym we Wrocławiu,
      1.1.6. Procedurą dokumentowania i zgłaszania naruszeń bezpieczeństwa ochrony danych osobowych w Uniwersytecie Przyrodniczym we Wrocławiu,
      1.1.7. Procedurą realizacji praw osób, których dane są przetwarzane w Uniwersytecie Przyrodniczym we Wrocławiu.
   1.2. Regularną ocenę skuteczności i efektywności stosowanych mechanizmów bezpieczeństwa Zasobów IT.
   1.3. Minimalizację wystąpienia incydentów bezpieczeństwa IT.
   1.4. Okresową kontrolę przestrzegania zasad bezpieczeństwa IT.
   1.5. Doskonalenie zasad zarządzania bezpieczeństwem IT i mechanizmów je ustanawiających.

Rozdział 2. Skróty i definicje

§ 2

1. Definicje używane w niniejszej Instrukcji mają następujące znaczenie:

   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.

Administrator Danych (AD) - oznacza Uniwersytet Przyrodniczy we Wrocławiu, reprezentowany przez Rektora, który ustala cele i środki przetwarzania danych osobowych.
Bezpieczeństwo IT – stan, w którym Zasoby IT i przetwarzane za ich pośrednictwem informacje oraz wspierane procesy wymagające ochrony są właściwie zabezpieczone poprzez zapewnienie atrybutów bezpieczeństwa tj. dostępności, poufności, integralności oraz technologii funkcjonujących w środowisku ładu informatycznego.
Dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, o których mowa w RODO.
Dostawca IT – każda firma, która na podstawie Umowy IT dostarcza określoną usługę IT – produkt, wsparcie, oprogramowanie, licencje, dostęp do chmury obliczeniowej, baz danych itd.
Dostępność informacji – właściwość, określająca możliwość wykorzystania informacji przez użytkownika na żądanie, w określonym czasie.
Informacje chronione – wszystkie nieujawnione do wiadomości publicznej informacje o charakterze technicznym, technologicznym, handlowym, kadrowym, finansowym, organizacyjnym, strategicznym lub inne informacje posiadające wartość dla Uczelni, w szczególności mogą to być dane osobowe podmiotów wewnętrznych i zewnętrznych.
Integralność informacji – właściwość zapewniająca, że informacja nie została zmieniona lub zniszczona w sposób nieautoryzowany.
IT (*ang. Information Technology*) – całokształt zagadnień, metod, środków i działań związanych z przetwarzaniem informacji. Stanowi połączenie zastosowań informatyki i telekomunikacji, obejmuje również sprzęt komputerowy oraz oprogramowanie, a także narzędzia i inne technologie związane z przetwarzaniem, przesyłaniem, przechowywaniem, zabezpieczaniem i prezentowaniem informacji.
Inspektor Ochrony Danych (IOD) – oznacza rolę w organizacji AD, odpowiedzialną za operacyjne i wykonawcze wsparcie i realizację obowiązków AD wynikających z RODO. Szczegółowy opis zakresu obowiązków roli IOD znajduje się w dokumencie „Polityki Ochrony Danych Osobowych".
Naruszenie bezpieczeństwa IT – pojedyncze zdarzenie lub seria zdarzeń niepożądanych albo niespodziewanych, związanych z bezpieczeństwem informacji i Zasobów IT, które stwarzają znaczne prawdopodobieństwo zakłócenia działań i zagrażają bezpieczeństwu Zasobów IT i informacji w nich przetwarzanej.
Podatność – właściwość Zasobu IT natury architektonicznej, konfiguracyjnej i konstrukcji samego oprogramowania lub sprzętu, na które mogą oddziaływać zagrożenia, z negatywnym skutkiem, a tym samym sprowadzać na środowisko IT, ryzyko naruszenia bezpieczeństwa IT (bądź ryzyka naruszenia prywatności podmiotu w przypadku przetwarzania danych osobowych) i informacji w takim środowisku przetwarzanych.
Poufność informacji – właściwość zapewniająca, że informacja nie jest udostępniana nieupoważnionym osobom, podmiotom lub w celu niezgodnym z przeznaczeniem.
Przetwarzanie informacji – operacje wykonywane w stosunku do informacji (zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie) również w systemach informatycznych.
System teleinformatyczny (system IT) – zespół współpracujących urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych poprzez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci urządzenia końcowego.

Uwierzytelnianie – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

Użytkownik – osoba, zatrudniona w UPWr, która w ramach obowiązków służbowych wykorzystuje powierzony Zasób IT.

Zasoby IT – każde urządzenie i oprogramowanie stanowiące element (poprzez możliwość fizycznego i logicznego połączenia) środowiska teleinformatycznego zapewniające prawidłową pracę operacyjną Uczelni. Są to w szczególności – systemy informatyczne, bazy danych, urządzenia sieciowe, firewall'e, laptopy, stacje robocze, tablety, telefony komórkowe, oprogramowanie aplikacyjne, biurowe, serwery.

Zarządzanie bezpieczeństwem informacji – ogół działań podejmowanych w celu zapewnienia poufności, dostępności i integralności i niezaprzeczalności operacji przetwarzanych informacji.

Zarządzanie bezpieczeństwem IT – ogół działań, podejmowanych w celu zapewnienia organizacyjnej, technicznej i proceduralnej ochrony informacji i Zasobów IT, za pośrednictwem których przetwarzane są informacje i wspierane procesy.

Rozdział 3. Przedmiot

§ 3

1. Niniejsza Instrukcja obejmuje swoim zakresem:
   1.1. opis struktur odpowiedzialnych za zarządzanie bezpieczeństwem IT, ich ról i zakresów odpowiedzialności,
   1.2. zbiór podstawowych wymagań bezpieczeństwa IT dla Zasobów IT,
   1.3. opis organizacyjnych mechanizmów bezpieczeństwa IT,
   1.4. zasady oceny zgodności bezpieczeństwa Zasobów IT.
2. Każde odstępstwo od zasad określonych w niniejszej Instrukcji musi być przeanalizowane i zatwierdzone pod kątem zapewnienia Bezpieczeństwa IT przez Dyrektora CSK i zaakceptowane przez właściwego kompetencyjnie prorektora.

Rozdział 4. Odpowiedzialność i obszar stosowania

§ 4

1. Do stosowania zapisów niniejszej Instrukcji zobowiązani są w szczególności pracownicy CSK oraz wszyscy użytkownicy systemów teleinformatycznych w Uniwersytecie Przyrodniczym we Wrocławiu.

Rozdział 5. Struktury Bezpieczeństwa IT

§ 5

1. W celu zapewnienia efektywnego zarządzania bezpieczeństwem IT została ustanowiona struktura bezpieczeństwa IT, w której określono następujące role i odpowiedzialności:
   1.1. **Właściwy kompetencyjnie prorektor** realizuje działania nadzorcze i opiniujące w procesie zarządzania Bezpieczeństwem IT poprzez:

1.1.1. opiniowanie zaproponowanych przez Dyrektora CSK kierunków rozwoju obszaru bezpieczeństwa IT i zapewnienie spójności podejmowanych działań z celami strategicznymi Uczelni,
1.1.2. opiniowanie polityk, procedur i innych regulacji wewnętrznych dotyczących Bezpieczeństwa IT,
1.1.3. opiniowanie podejmowanych inicjatyw w celu ograniczania ryzyka wystąpienia działań niepożądanych w obszarze Bezpieczeństwa IT,
1.1.4. zatwierdzenie potrzeb i wydatków w obszarze bezpieczeństwa IT.

1.2. **Dyrektor CSK** nadzoruje, koordynuje i odpowiada za działania w procesie zarządzania bezpieczeństwem IT poprzez:
1.2.1. opracowanie struktury, podziału kompetencji i odpowiedzialności w obszarze CSK w zakresie bezpieczeństwa IT,
1.2.2. nadzór nad realizacją procesów i instrukcji będących w zakresie działań operacyjnych bezpieczeństwa IT,
1.2.3. okresowe kontrole i nadzór nad wdrożeniem i utrzymaniem postanowień wynikających z regulacji w obszarze bezpieczeństwa IT,
1.2.4. koordynację działań w zakresie okresowych planów audytów bezpieczeństwa IT,
1.2.5. prowadzenie analiz i ocen ryzyka, raportowanie do właściwego kompetencyjnie prorektora Uczelni o stanie bezpieczeństwa IT,
1.2.6. gromadzenie i bilansowanie potrzeb oraz wnioskowanie o środki rzeczowo-finansowe niezbędne dla wdrożenia wymaganych mechanizmów bezpieczeństwa IT,
1.2.7. zapewnienie utrzymania i stałego rozwoju rozwiązań w obszarze bezpieczeństwa IT adekwatnie do najnowszych trendów i standardów oraz w oparciu o wynik analizy ryzyka bezpieczeństwa IT,
1.2.8. monitorowanie realizacji oraz doskonalenie procedur bezpieczeństwa IT,
1.2.9. opracowywanie, aktualizację regulacji wewnętrznych w obszarze bezpieczeństwa IT i właściwy dobór mechanizmów bezpieczeństwa Zasobów IT oraz przedkładanie do zaopiniowania właściwemu kompetencyjnie prorektorowi,
1.2.10. badanie i monitorowanie anomalii sieciowych pod kątem bezpieczeństwa IT,
1.2.11. organizacja regularnych przeglądów, planu monitorowania bezpieczeństwa oraz testów bezpieczeństwa Zasobów IT,
1.2.12. reagowanie na zidentyfikowane zagrożenia oraz przypadki naruszenia bezpieczeństwa IT,
1.2.13. nadzór nad prowadzeniem przez ASI ewidencji nadanych uprawnień w Zasobach IT.

1.3. **Administrator Systemów Informatycznych** (ASI) uczestniczy w procesie zapewniania bezpieczeństwa IT, poprzez:
1.3.1. zapewnienie zgodności stanu faktycznego zabezpieczeń eksploatowanych Zasobów IT z regulacjami wewnętrznymi w obszarze bezpieczeństwa IT,
1.3.2. dokonywanie zmian konfiguracyjnych w administrowanych Zasobach IT,
1.3.3. opracowanie dokumentacji mechanizmów bezpieczeństwa zaimplementowanych w nadzorowanych Zasobach IT,
1.3.4. prowadzenie ewidencji nadanych uprawnień w Zasobach IT,

1.3.5. reagowanie na przypadki naruszenia zasad bezpieczeństwa IT w odniesieniu do eksploatowanych Zasobów IT.

1.4. **Użytkownik Zasobu IT** eksploatuje powierzony dostęp do systemów, postępując zgodnie z obowiązującymi regulacjami wewnętrznymi ustalającymi zasady bezpiecznego użytkowania Zasobów IT w Uczelni opisanymi w PBIiSIT.

Rozdział 6. Dokumentowanie Zasobów IT

§ 6

1. Dokumentacja Zasobu IT w zakresie wymagań bezpieczeństwa powinna obejmować:
   1.1. opis funkcjonalny Zasobu IT oraz wykaz wspieranych przezeń procesów,
   1.2. zakres przetwarzanych informacji i okres ich retencji
   1.3. opis fizycznej i logicznej architektury Zasobu IT,
   1.4. opis zgodności Zasobu IT z wymaganiami bezpieczeństwa,
   1.5. opis integracji i powiązań Zasobu IT z innymi Zasobami IT,
   1.6. informacje dotyczące lokalizacji, warunków eksploatacji i utrzymania Zasobu IT,
   1.7. wymagania dotyczące wycofania Zasobu IT z eksploatacji.
2. Powyższa dokumentacja jest sporządzana przez Administratorów Systemów Informatycznych (ASI), zatwierdzana przez Dyrektora CSK i znajduje się w CSK.

Rozdział 7. Mechanizmy kontrolne bezpieczeństwa IT

§ 7

1. Mechanizmy kontrolne bezpieczeństwa Zasobów IT mają na celu zapewnienie, że cechy bezpieczeństwa tj. dostępności, poufności, integralności, będą funkcjonowały na oczekiwanym poziomie i muszą być adekwatne do przyjętej w Uczelni „Metodyki szacowania ryzyka dla systemów IT" (ze względu na bezpieczeństwo informacji w nich przetwarzanych).
2. Informacje w Uczelni mogą być przetwarzane wyłącznie z wykorzystaniem Zasobów IT zgodnych z wymaganiami bezpieczeństwa.
3. Dobór, wdrożenie i modyfikacja mechanizmów bezpieczeństwa Zasobów IT następuje na podstawie wyników oceny ryzyka bezpieczeństwa IT przeprowadzonej dla tych Zasobów IT przez ASI, zatwierdzonych przez Dyrektora CSK.
4. W celu zapewnienia bezpieczeństwa informacji przetwarzanych z wykorzystaniem Zasobów IT wprowadza się podstawowe ogólne wymagania bezpieczeństwa dla Zasobów IT w następujących obszarach:
   4.1. klasyfikacja bezpieczeństwa Zasobów IT,
   4.2. bezpieczeństwo komunikacji sieciowej,
   4.3. kontrola dostępu,
   4.4. zabezpieczanie urządzeń końcowych (stacjonarnych),
   4.5. urządzenia końcowe (mobilne),
   4.6. usługi chmurowe,
   4.7. zarządzanie zmianą zasobów IT,
   4.8. kopie zapasowe,
   4.9. dostępność Zasobów IT,

4.10. zarządzanie podatnościami Zasobów IT,
4.11. eksploatacja i utrzymanie Zasobów IT,
4.12. wycofanie Zasobów IT z eksploatacji,
4.13. bezpieczeństwo poczty elektronicznej,
4.14. bezpieczeństwo aplikacji webowych,
4.15. monitorowanie bezpieczeństwa IT,
4.16. bezpieczeństwo środowisk zwirtualizowanych,
4.17. bezpieczeństwo serwerów,
4.18. bezpieczeństwo IT,
4.19. edukacja i doskonalenie świadomości bezpieczeństwa IT.

5. Ogólne wymagania bezpieczeństwa IT w Uczelni, o których mowa w ust. 4 zostały opisane w PBIiSIT.
6. Postępowanie dotyczące właściwego zarządzania dostępami i uprawnieniami do Zasobów IT zostało opisane w „Procedurze zarządzania dostępami i upoważnieniami do Zasobów IT".
7. Zasoby IT podlegają w swoim cyklu życia monitorowaniu, weryfikacji i ocenie pod kątem spełnienia wymagań bezpieczeństwa IT, adekwatnych do klasy bezpieczeństwa danego Zasobu.
8. Nadzór nad spełnieniem wymagań bezpieczeństwa Zasobów IT zostaje zakończony po wycofaniu Zasobu IT z eksploatacji, z wyjątkiem wymagań odnoszących się do retencji danych, które były przetwarzane przez wycofany Zasób IT, a których okres retencji nie minął w momencie ich wycofania.
9. Współpraca z Dostawcami IT wymaga stosowania nadzoru i monitorowania ich aktywności w dziedzinie bezpieczeństwa wdrażania, utrzymania i rozwoju Zasobów IT w Uczelni, co powinno mieć swoje odzwierciedlenie w zawartych umowach.

Rozdział 8. Zarządzanie zmianą Zasobów IT

§ 8

1. Dyrektor CSK oraz ASI, bądź osoby upoważnione przez Dyrektora CSK rozpatrują zmiany tj. modyfikacje bądź rozszerzenie systemu, pod kątem uwzględnienia i spełnienia wymagań przyjętych w niniejszej Instrukcji, w sposób gwarantujący utrzymanie akceptowalnego poziomu bezpieczeństwa IT poprzez:
   1.1. wykonanie analizy ryzyka przed dokonaniem zmiany i podjęcie działań minimalizujących zagrożenia związane z bezpieczeństwem przetwarzanych informacji,
   1.2. udział w procedurach weryfikacji i potwierdzenia zgodności Zasobu IT z wymaganiami bezpieczeństwa IT określonymi w PBIiSTI.
2. Zmiany zatwierdza właściwy kompetencyjnie prorektor.

Rozdział 9. Ocena zgodności bezpieczeństwa Zasobów IT

§ 9

1. Każdy Zasób IT w swoim cyklu życia podlega okresowej ocenie zgodności zaimplementowanych w nim mechanizmów bezpieczeństwa IT oraz identyfikacji objawów niespełnienia wymagań wynikających z PBIiSIT.

2. Ocena zgodności bezpieczeństwa Zasobów IT ma na celu:
   2.1. spełnienie wymogów prawa i regulacji wewnętrznych w obszarze bezpieczeństwa IT,
   2.2. optymalizację nakładów finansowych i organizacyjnych ponoszonych w związku ze stosowaniem zabezpieczeń w odniesieniu do Zasobu IT.

3. Ocenie zgodności powinny podlegać Zasoby IT działające również poza infrastrukturą Uczelni oraz utrzymywane lub zarządzane przez Dostawców IT.

4. Ocena zgodności bezpieczeństwa Zasobów IT musi być realizowana w toku:
   4.1. projektowania Zasobu IT,
   4.2. wdrożenia Zasobu IT,
   4.3. utrzymania i eksploatacji Zasobu IT,
   4.4. rozwoju Zasobu IT,
   4.5. wyłączenia z eksploatacji Zasobu IT.

5. Dyrektor CSK oraz ASI w porozumieniu z IOD decydują o częstości stosowania i doborze sposobu oceny zgodności Zasobu IT z wymaganiami bezpieczeństwa spośród następujących metod:
   5.1. testów bezpieczeństwa badających w ustalonym zakresie faktyczną zgodność Zasobu IT z wymaganiami bezpieczeństwa,
   5.2. audytu bezpieczeństwa IT.

6. Wyniki oceny zgodności Zasobu IT warunkują akceptację Dyrektora CSK w zakresie wdrożenia, modyfikacji, utrzymania danego Zasobu IT lub wycofania go z eksploatacji.

Rozdział 10. Monitorowanie bezpieczeństwa IT

§ 10

1. Monitorowanie bezpieczeństwa Zasobów IT, prowadzone jest przez CSK zgodnie z zapisami PBIiSIT § 17 oraz poniższymi zasadami:
   1.1. w celu zapewnienia skutecznego monitorowania stanu bezpieczeństwa Zasobów IT, ustalany jest zakres monitorowania bezpieczeństwa Zasobów IT oraz wykaz monitorowanych Zasobów IT,
   1.2. ASI kierując się wymaganiami dostępności Zasobu IT, dobiera metody monitorowania, w tym wykaz narzędzi i systemów informatycznych służących do monitorowania bezpieczeństwa Zasobów IT,
   1.3. raportowanie odbywa się w trakcie obsługi zdarzeń rejestrowanych przez narzędzia monitorujące, obsługiwane przez ASI.
2. Implementacja mechanizmów monitorowania bezpieczeństwa Zasobów IT jest realizowana przy uwzględnieniu obowiązującej klasyfikacji informacji przetwarzanych przez dany Zasób IT oraz klasy bezpieczeństwa tego Zasobu IT.
3. Zasoby IT, zgodnie z ich klasą bezpieczeństwa, muszą mieć zaimplementowane mechanizmy pozwalające na monitoring ich bezpieczeństwa.
4. Odpowiedzialność za monitorowanie bezpieczeństwa IT spoczywa na Dyrektorze CSK.

Rozdział 11. Zarządzanie incydentami bezpieczeństwa IT

§ 11

1. Zidentyfikowane zagrożenia i podatności Zasobów IT, które stwarzają ryzyko dla bezpieczeństwa środowiska przetwarzania informacji chronionych, są zarządzane zgodnie z obowiązującą w Uczelni, „Procedurą zarządzania incydentami z zakresu bezpieczeństwa informacji w Uniwersytecie Przyrodniczym we Wrocławiu".
2. Właściwa obsługa naruszeń bezpieczeństwa IT wymaga podjęcia skoordynowanych działań mających na celu: identyfikację, neutralizację bezpośredniego oddziaływania czynników warunkujących powstanie incydentu, udokumentowanie przebiegu zdarzenia, obsługi incydentu oraz wdrożenie rozwiązań, które ograniczą negatywne skutki incydentu oraz zminimalizują ryzyko wystąpienia takiego samego lub podobnych incydentów w przyszłości

Rozdział 12. Audyty i testy bezpieczeństwa Zasobów IT w CSK

§ 12

1. W ramach sprawowanego nadzoru nad bezpieczeństwem Zasobów IT Dyrektor CSK przeprowadza audyt zgodnie z zaakceptowanym przez właściwego kompetencyjnie prorektora rocznym planem audytów bezpieczeństwa IT.
2. Plan audytu zawiera informacje na temat zakresu, planowanego terminu oraz nazwisk audytorów i jest zatwierdzany przez właściwego kompetencyjnie prorektora.
3. Audyt bezpieczeństwa IT można przeprowadzić także poza planem rocznym w wyniku podejrzenia lub zaistnienia nowych zagrożeń, podatności lub wystąpienia incydentu bezpieczeństwa, w tzw. trybie doraźnym. O przeprowadzeniu takiego audytu decyduje właściwy kompetencyjnie prorektor, na wniosek Dyrektora CSK lub IOD.
4. Dyrektor CSK organizuje testy bezpieczeństwa Zasobów IT okresowo, nie rzadziej niż raz na rok, w porozumieniu z właściwie kompetencyjnym prorektorem.