Załącznik do ZW 30/2018

Polityka Bezpieczeństwa Informacji Politechniki Wrocławskiej

1. Polityka Bezpieczeństwa Informacji Politechniki Wrocławskiej określa obowiązujące zasady i wymagania dotyczące bezpieczeństwa informacji.

2. W celu zapewnienia wymaganego poziomu ochrony informacji w realizowanych zadaniach Uczelni wprowadza się System Zarządzania Bezpieczeństwem Informacji (zwany Systemem lub SZBI).

3. System Zarządzania Bezpieczeństwem Informacji dotyczy pracowników wszystkich jednostek/komórek organizacyjnych Uczelni.

4. System Zarządzania Bezpieczeństwem Informacji ma za zadanie:
   1) zagwarantowanie ochrony informacji adekwatnie do poziomu występujących ryzyk oraz wymagań wynikających z przepisów prawa;
   2) zapewnienie ciągłości procesów przetwarzania informacji;
   3) reagowanie na zagrożenia bezpieczeństwa informacji;
   4) zapewnienie poprawnego funkcjonowania systemów informatycznych.

5. Zadania Systemu Zarządzania Bezpieczeństwem Informacji określone w punkcie 4 realizowane są poprzez:
   1) określenie zasad zarządzania bezpieczeństwem informacji;
   2) wskazanie zadań i odpowiedzialności osobom zarządzającym bezpieczeństwem informacji oraz osobom zaangażowanym w przetwarzanie informacji;
   3) wyznaczenie właścicieli aktywów informacyjnych;
   4) wdrożenie i utrzymanie zabezpieczeń fizycznych, technicznych oraz organizacyjnych w systemach informatycznych;
   5) informowanie o zasadach funkcjonowania Systemu Zarządzania Bezpieczeństwa Informacji wszystkich osób zaangażowanych w proces przetwarzania informacji w Politechnice Wrocławskiej, adekwatnie do wykonywanych przez nich zadań;
   6) ciągłe podnoszenie świadomości pracowników w obszarze bezpieczeństwa informacji;
   7) zarządzanie incydentami naruszającymi bezpieczeństwo informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących;
   8) przegląd i utrzymanie Systemu Zarządzania Bezpieczeństwem Informacji;
   9) ciągłe doskonalenie Systemu Zarządzania Bezpieczeństwem Informacji.

6. Zarządzanie bezpieczeństwem informacji w Politechnice Wrocławskiej jest realizowane za pomocą następujących procesów realizowanych w ramach Systemu Zarządzania Bezpieczeństwem Informacji:
   1) zarządzania ryzykiem;
   2) dobierania i stosowania zabezpieczeń;
   3) monitorowania, przeglądu, utrzymania i doskonalenia Systemu;
   4) nadzoru nad dokumentacją i zapisami Systemu;
   5) zarządzania dostępem;
   6) zarządzania incydentami.

7. Podstawą wszelkich działań w zakresie utrzymania i doskonalenia zabezpieczeń informacji w Politechnice Wrocławskiej jest analiza ryzyka dotycząca bezpieczeństwa informacji.

8. Stosowanie i dobieranie odpowiednich zabezpieczeń dokonuje się na podstawie obowiązujących przepisów oraz wyników przeprowadzonej analizy ryzyka bezpieczeństwa informacji w następujących obszarach:
   1) fizycznym;
   2) technicznym;
   3) organizacyjnym.

9. Politechnika Wrocławska dba o zapewnienie adekwatnego do ryzyka poziomu bezpieczeństwa informacji w zakresie trzech podstawowych aspektów tj.:
   1) poufności;
   2) integralności;
   3) dostępności.

10. Monitorowanie i przegląd Systemu Zarządzania Bezpieczeństwem Informacji realizowany jest poprzez:
   1) określanie wartości mierników bezpieczeństwa informacji;
   2) wykonywanie przeglądów Systemu;
   3) wykonywanie audytów wewnętrznych;
   4) wykonywanie audytów zewnętrznych.

11. Doskonalenie Systemu Zarządzania Bezpieczeństwem Informacji odbywa się poprzez:
   1) przeprowadzanie działań korygujących oraz ocenę ich skuteczności;
   2) przeprowadzanie działań doskonalących oraz ocenę ich skuteczności;
   3) informowanie zainteresowanych stron o działaniach i udoskonaleniach.

12. Nadzór nad dokumentacją i zapisami Systemu prowadzony jest poprzez utrzymywanie i nadzorowanie dokumentacji systemowej i zapisów systemowych.

13. Zarządzanie dostępem do aktywów informacyjnych Politechniki Wrocławskiej realizowane jest za pomocą zatwierdzonych sposobów postępowania oraz mechanizmów

kontrolnych w obszarach fizycznego dostępu do informacji oraz danych i informacji w systemach informatycznych.

14. Zarządzanie dostępem do informacji realizowane jest poprzez:
    1) nadzór nad dostępem do budynków i pomieszczeń zgodnie z przepisami wewnętrznymi Politechniki Wrocławskiej*;*
    2) kontrolę dostępu do obszarów przetwarzania danych osobowych;
    3) zasady nadawania uprawnień do informacji użytkownikom;
    4) kontrolę dostępu do sieci i systemów informatycznych;
    5) zasady nadawania uprawnień użytkownikom systemów informatycznych;
    6) zarządzanie hasłami i innymi danymi uwierzytelniającymi;
    7) politykę czystego biurka;
    8) politykę czystego ekranu;
    9) zabezpieczenia kryptograficzne;
    10) określenie zasad dostępu do kodów źródłowych programów.

15. Zarządzanie incydentami związanymi z bezpieczeństwem informacji realizowane jest poprzez monitorowanie i wykrywanie naruszeń bezpieczeństwa w obszarach fizycznego dostępu, dostępu do informacji i w systemach informatycznych.

16. W celu skutecznego zarządzania incydentem stosuje się zasadę, że wszyscy pracownicy znają zasady informowania o incydentach naruszenia bezpieczeństwa oraz są zobowiązani do zgłaszania incydentów naruszających bezpieczeństwo.

17. Wszelkie informacje wytworzone, przekazywane i przetwarzane w Uczelni, nieoznaczone jako należące do osób trzecich, stanowią własność Uczelni i podlegają ochronie. Do najważniejszych grup informacji podlegających ochronie należą:
    1) dane dotyczące badań naukowych - dane związane z badaniami naukowymi prowadzonymi w Uczelni;
    2) dane finansowe – informacje, które zostały zdefiniowane w ustawie o zasadach finansowania nauki, ustawie o rachunkowości oraz ustawie o finansach publicznych;
    3) dane osobowe – informacje, które zostały zdefiniowane w ustawie o ochronie danych osobowych oraz rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku 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, dalej zwane RODO) wraz z trybem postępowania z informacjami określonym w ww. przepisach i przepisach wykonawczych;
    4) dane związane z ochroną praw autorskich – informacje, które zostały zdefiniowane w ustawie o prawie autorskim i prawach pokrewnych;
    5) informacje publiczne – ochrona informacji publicznych realizuje wymogi ustawy dostępie do informacji publicznej;

6) informacje niejawne – ochrona informacji niejawnych realizuje wymogi ustawy o ochronie informacji niejawnych; za organizację systemu ochrony informacji niejawnych odpowiada Dział Ochrony Informacji Niejawnych i Spraw Obronnych.

18. Wszelkie informacje wytworzone, przekazywane i przetwarzane w Uczelni są chronione adekwatnie do zidentyfikowanego poziomu ochrony:
    1) informacje o poziomie ochrony I – informacje, których naruszenie poufności, integralności lub dostępności nie powoduje strat dla Uczelni;
    2) informacje o poziomie ochrony II – informacje, których naruszenie poufności, integralności lub dostępności może wpłynąć na działalność Uczelni i spowodować ograniczone straty;
    3) informacje o poziomie ochrony III – informacje, których naruszenie poufności, integralności lub dostępności może spowodować naruszenie przepisów prawa lub spowodować straty dla Uczelni;
    4) informacje o poziomie ochrony IV – informacje, których naruszenie poufności, integralności lub dostępności może spowodować poważne naruszenie przepisów prawa lub spowodować wysokie straty dla Uczelni.

19. Za wskazanie określonego poziomu ochrony informacji odpowiada właściciel tej informacji (kierownik jednostki/komórki organizacyjnej).

20. W zakresie odpowiedzialności za bezpieczeństwo informacji kierownicy jednostek/komórek organizacyjnych odpowiadają za:
    1) identyfikowanie i dokumentowanie zagrożeń dla bezpieczeństwa informacji;
    2) definiowanie oraz realizację działań zapobiegającym zagrożeniom;
    3) organizację szkoleń dla pracowników;
    4) poprawność merytoryczną danych gromadzonych za pomocą systemów informatycznych;
    5) wnioskowanie o nadanie, zmianę lub odebranie uprawnień;
    6) wprowadzanie zabezpieczeń dla zasobów, nad którymi sprawują nadzór;
    7) podejmowanie odpowiednich działań w przypadku wykrycia incydentów i naruszeń bezpieczeństwa;
    8) nadzorowanie przestrzegania zasad Systemu.

21. Odpowiedzialność za bezpieczeństwo informacji w Politechnice Wrocławskiej ponoszą wszyscy pracownicy zgodnie z posiadanymi zakresami obowiązków. Każdy pracownik zobowiązany jest dbać o bezpieczeństwo powierzonych mu do przetwarzania, archiwizowania lub przechowywania informacji zgodnie z obowiązującymi przepisami wewnętrznymi, w tym m. in.:
    1) stosować zasady określone Systemem Zarządzania Bezpieczeństwem Informacji oraz innymi dokumentami wewnętrznymi;
    2) chronić informacje podlegające ochronie przed dostępem do nich osób nieuprawnionych;

3) chronić dane przed przypadkowym lub umyślnym zniszczeniem, utratą lub modyfikacją;
4) chronić sprzęt, wydruki komputerowe i inne nośniki zawierające dane chronione;
5) utrzymywać w tajemnicy szczegóły technologiczne systemów także po ustaniu zatrudnienia na Politechnice Wrocławskiej;
6) stosować się do szczegółowych zaleceń w zakresie bezpiecznej obsługi systemów informatycznych.

22. W Politechnice Wrocławskiej nadzór nad Polityką Bezpieczeństwa Informacji pełni Prorektor ds. Organizacji i Rozwoju (Administrator Danych), który w szczególności odpowiedzialny jest za:
1) nadzór nad realizacją Polityki Bezpieczeństwa Informacji;
2) nadzór nad dokumentacją Systemu na etapie jej opracowywania, weryfikacji, aktualizacji, udostępniania i przechowywania;
3) zapewnienie, że procesy potrzebne w Systemie są ustanowione, wdrożone i utrzymywane;
4) nadzór nad planowaniem prac dotyczących Systemu oraz ich realizacją;
5) nadzór działań wdrożeniowych, korygujących i organizację przeglądów dotyczących Systemu;
6) powiadamianie Rektora działaniach niezgodnych z obowiązującym Systemem;
7) nadzór szkoleń z zakresu Systemu;
8) koordynację działań związanych z ochroną informacji na Politechnice Wrocławskiej;
9) wprowadzanie zatwierdzonych szczegółowych polityk bezpieczeństwa;
10) zarządzanie przeprowadzenia analizy ryzyk dotyczących bezpieczeństwa informacji;
11) nadzór nad utrzymywaniem wykazu zasobów informacyjnych;
12) analizę raportów z wszelkich zdarzeń związanych z bezpieczeństwem wszystkich zasobów informacyjnych;
13) monitorowanie zachowania właściwego poziomu bezpieczeństwa informacji;
14) sprawowanie nadzoru nad przestrzeganiem zasad ochrony informacji.

23. W Politechnice Wrocławskiej powołany jest Administrator Bezpieczeństwa Informacji (ABI/IODO) podległy Administratorowi Danych, który w pierwszej kolejności realizuje zadania określone w RODO, Ustawie i przepisach wykonawczych, a szczegółowy zakres działania określony jest w Zarządzeniu Wewnętrznym *w sprawie organizacji przetwarzania danych osobowych w Politechnice Wrocławskiej i dokumentacji związanej z tym przetwarzaniem.* ABI realizuje w szczególności zadania:
1) tworzenie oraz aktualizowanie dokumentacji ochrony danych osobowych;
2) informowanie administratora danych;
3) monitorowanie przestrzegania przepisów o ochronie danych osobowych;
4) pełnienie funkcji punktu kontaktowego dla podmiotów danych osobowych;
5) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych osobowych oraz współpraca z organem nadzorczym;

6) reagowanie na incydenty naruszające przepisy o ochronie danych osobowych;
7) wspieranie administratora danych w wykonywaniu przez niego zadań przewidzianych w przepisach o ochronie danych osobowych we wszystkich czynnościach, w których z uwagi na charakter podejmowanych działań jest to możliwe;
8) informowanie administratora danych oraz pracowników, którzy przetwarzają dane osobowe, o konkretnych obowiązkach spoczywających na nich na mocy przepisów o ochronie danych osobowych;
9) merytoryczne wspieranie administratora danych oraz pracowników w podejmowaniu działań zmierzających do zapewnienia zgodnego z prawem przetwarzania danych;
10) wspieranie administratora danych w wykazaniu jednej z przesłanek przetwarzania danych osobowych, o których mowa w art. 6–11 RODO;
11) analizowanie ryzyka dla bezpieczeństwa danych osobowych;
12) szkolenie pracowników z zakresu bezpieczeństwa danych osobowych.

24. W Politechnice Wrocławskiej nadzór nad Polityką Bezpieczeństwa Systemów Informatycznych pełni Prorektor ds. Współpracy z Gospodarką i Informatyzacji, który w zakresie systemów informatycznych w szczególności odpowiedzialny jest za:
1) nadzór nad dokumentacją Systemu w zakresie systemów i aktywów informatycznych na etapie jej opracowywania, weryfikacji, aktualizacji, udostępniania i przechowywania;
2) zapewnienie, że procesy potrzebne w Systemie w zakresie systemów i aktywów informatycznych są ustanowione, wdrożone i utrzymywane;
3) nadzór nad planowaniem prac dotyczących Systemu w zakresie systemów i aktywów informatycznych oraz ich realizacją;
4) nadzorowanie działań wdrożeniowych, korygujących i organizację przeglądów dotyczących bezpieczeństwa systemów informatycznych;
5) powiadamianie Rektora działaniach niezgodnych z obowiązującym Systemem w zakresie systemów i aktywów informatycznych;
6) nadzorowanie szkoleń z zakresu bezpieczeństwa systemów informatycznych;
7) wprowadzanie zatwierdzonych szczegółowych polityk bezpieczeństwa; dotyczących systemów informatycznych;
8) zarządzanie przeprowadzenia analizy ryzyk dotyczących bezpieczeństwa systemów informatycznych;
9) nadzór nad utrzymywaniem wykazu zasobów informatycznych;
10) analizę raportów z wszelkich zdarzeń związanych z bezpieczeństwem wszystkich zasobów informatycznych;
11) monitorowanie zachowania właściwego poziomu bezpieczeństwa informatycznego;
12) sprawowanie nadzoru nad przestrzeganiem zasad ochrony informacji w systemach informatycznych.

25. W Politechnice Wrocławskiej powołany jest Administrator Bezpieczeństwa Systemu Informatycznego, który odpowiedzialny jest za:
    1) sprawowanie nadzoru nad bezpieczeństwem systemów informatycznych;
    2) sprawowanie nadzoru nad przygotowaniem dokumentów polityk bezpieczeństwa dla systemów informatycznych;
    3) sprawowanie nadzoru nad przygotowaniem dokumentów dotyczących planów ciągłości działania i planów awaryjnych dla systemów informatycznych;
    4) opiniowanie i wprowadzanie polityk bezpieczeństwa dla systemów informatycznych;
    5) opracowanie, sprawdzenie i wprowadzanie planów ciągłości działania i planów awaryjnych dla systemów informatycznych;
    6) opiniowanie i sprawdzanie proponowanych zmian i rozwiązań w politykach dla systemów informatycznych;
    7) ocenę pracy systemów informatycznych w celu wykrycia potencjalnych zagrożeń, w szczególności identyfikacji wszelkich nieprawidłowości związanych z bezpieczeństwem systemów informatycznych;
    8) przeprowadzanie analizy ryzyka dla systemów informatycznych;
    9) prowadzenie analizy podatności systemów informatycznych;
    10) weryfikację zgodności informatycznych środków przetwarzania z odpowiednimi politykami bezpieczeństwa i autoryzowanie ich do stosowania na Politechnice Wrocławskiej;
    11) opracowanie, sprawdzenie, wprowadzenie i utrzymywanie standardów bezpieczeństwa dotyczących systemów informatycznych;
    12) analizowanie raportów z wszelkich zdarzeń związanych z bezpieczeństwem systemów informatycznych;
    13) szkolenie pracowników z zakresu bezpieczeństwa informacji w systemach informatycznych;
    14) informowanie Prorektora ds. Współpracy z Gospodarką i Informatyzacji o wszelkich incydentach dotyczących naruszenia bezpieczeństwa informacji dotyczących systemów informatycznych, a w przypadku stwierdzenia incydentów dotyczących ochrony danych osobowych informowanie również ABI/IODO.

26. W celu zapewnienia ww. aspektów bezpieczeństwa informacji w Uczelni stosowane są odpowiednie zasady utrzymania oraz użytkowania systemów informatycznych. Najważniejsze zasady to:
    1) wszystkie systemy informatyczne przed dopuszczeniem do stosowania muszą spełniać minimalne wymagania bezpieczeństwa i standardy przyjęte do stosowania na Uczelni;
    2) wdrażanie, eksploatacja oraz utrzymanie systemów informatycznych jest realizowane za pomocą kompetentnych i świadomych zagadnień bezpieczeństwa pracowników oraz firm zewnętrznych;
    3) prowadzenie kontroli wprowadzanych zmian w systemach informatycznych***;***

4) prowadzenie prac testowych i rozwojowych na oddzielnych urządzeniach i środowiskach; prowadzenie prac rozwojowych i testowych może być realizowane przez firmy zewnętrzne na podstawie odpowiednich umów dotyczących rozwoju i utrzymania oprogramowania oraz aplikacji;
5) nadzorowanie usług dostarczanych przez strony trzecie, a w szczególności wszelkich wprowadzanych do nich zmian;
6) stosowanie ochrony przed „złośliwymi" i szkodliwymi programami np. typu malware;
7) kopie zapasowe są tworzone zgodnie z ogólnie przyjętymi zasadami i dobrymi praktykami producentów rozwiązań i systemów oraz stosownie do tych zasad i dobrych praktyk testowane;
8) stosowanie zasad postępowania z nośnikami danych zgodnie z dobrymi praktykami;
9) monitorowanie aktywów informacyjnych oraz zasobów systemów informatycznych w celu wykrycia naruszeń bezpieczeństwa informacji oraz ich zapobieganiu;
10) stosowanie wdrożonych zasad postępowania oraz mechanizmów reagowania na incydenty w sytuacji wykrycia incydentu naruszenia bezpieczeństwa informacji;
11) szczegółowe standardy bezpieczeństwa są tworzone dla kluczowych składników infrastruktury sieciowej wtedy, gdy jest to adekwatne do oszacowanych ryzyk.

27. W celu zapewnienia ciągłości działania Politechniki Wrocławskiej, które związane jest z przetwarzaniem informacji dla poszczególnych obszarów i systemów krytycznych tworzone są plany postępowania w sytuacjach awaryjnych i kryzysowych.

28. W Uczelni mogą być powołani administratorzy danych, którzy będą sprawować nadzór nad innymi, niż wskazane powyżej, grupami informacji podlegającymi ochronie.

29. W szczególnie uzasadnionych wypadkach o odstąpieniu od Polityki Bezpieczeństwa Informacji decyduje Rektor.

30. Wytyczne dotyczące poszczególnych obszarów objętych Polityką Bezpieczeństwa Informacji zawarte są szczegółowych regulacjach Systemu Zarządzania Bezpieczeństwem Informacji.