POLITECHNIKA WARSZAWSKA

Zarządzenie nr 142 /2020
Rektora Politechniki Warszawskiej
z dnia 18 listopada 2020 r.

w sprawie bezpieczeństwa informacji w Politechnice Warszawskiej

Na podstawie art. 23 ust 1 ustawy z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce (Dz.U. z 2020, poz. 85, z późn zm.), w związku z ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781), ustawą z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2019 r. poz. 1010, z późn. zm.), ustawą z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz. U. z 2019 r. poz. 1843, z późn.zm.), z Kodeksem pracy, ustawą z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2019 r. poz. 1429, z późn. zm.), ustawą z dnia 27 sierpnia 2009 r. finansach publicznych (Dz. U. z 2019 r. poz. 869, z późn. zm.), ustawą z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2020 r. poz. 346, z późn. zm.) oraz rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2017 r. poz. 2247), zarządza się, co następuje:

§ 1

1. Zarządzenie określa zasady i sposoby postępowania w zakresie zapewniania bezpieczeństwa informacji przetwarzanych w Politechnice Warszawskiej oraz wymagania dotyczące zabezpieczeń organizacyjnych i technicznych, w szczególności:
   1) spełniania wymagań prawnych w zakresie ochrony informacji;
   2) podnoszenia bezpieczeństwa informacji przetwarzanych w Politechnice Warszawskiej;
   3) podnoszenia świadomości pracowników w zakresie bezpieczeństwa informacji.
2. Zarządzenie ma zastosowanie do wszystkich przetwarzanych w Politechnice Warszawskiej informacji, których ujawnienie może narazić Politechnikę Warszawską na szkodę, w szczególności do informacji przetwarzanych w systemach informatycznych.

§ 2

1. Za stosowanie zasad wprowadzonych zarządzeniem oraz wprowadzenie odpowiedniego poziomu bezpieczeństwa informacji, odpowiadają:
   1) kierownicy podstawowych i ogólnouczelnianych jednostek organizacyjnych, z wyłączeniem kierowników jednostek organizacyjnych wchodzących w skład Politechniki Warszawskiej Filia w Płocku;
   2) prorektor ds. Filii w Płocku w stosunku do Politechniki Warszawskiej Filia w Płocku;
   3) kanclerz w odniesieniu do jednostek organizacyjnych administracji centralnej podległych kanclerzowi;
   4) kwestor w odniesieniu do jednostek organizacyjnych administracji centralnej podległych kwestorowi;
   5) kierownicy projektu lub osoby odpowiedzialne za jego realizację w zakresie wynikającym z udziału Politechniki Warszawskiej w projekcie;

6) przewodniczący rady doktorantów;
7) przewodniczący samorządu studentów;
8) kierownicy szkół doktorskich;
9) kierownicy studiów doktoranckich;
10) przewodniczący rady naukowej dyscyplin.

2. Odpowiedni poziom bezpieczeństwa informacji zapewniany jest poprzez:
   1) wdrażanie zabezpieczeń technicznych i organizacyjnych;
   2) nadzór nad przestrzeganiem zasad bezpieczeństwa informacji w jednostce/projekcie.
3. Pracownicy jednostki/osoby realizujące projekt oraz właściciele procesów są zobowiązani do przestrzegania obowiązujących procedur wdrożonych w jednostce/projekcie, w szczególności dotyczących bezpieczeństwa informacji.

§ 3

W Politechnice Warszawskiej dla zapewnienia optymalnej ochrony informacji, stosuje się, adekwatne do potencjalnych zagrożeń, środki:

1) organizacyjne (organizacja wewnętrzna), polegające w szczególności na:
   a) zobowiązaniu pracownika przetwarzającego informacje lub posiadającego informacje podlegające ochronie lub bezpośrednio w dokumentach mających wpływ na bezpieczeństwo informacji, do przestrzegania zasad bezpieczeństwa informacji,
   b) uwzględnieniu przed każdym nowym przedsięwzięciem/projektem oceny czy jego realizacja będzie możliwa i zgodna z obowiązującymi zasadami bezpieczeństwa informacji oraz uwzględnieniu wniosków wynikających z takiej oceny,
   c) przeprowadzaniu okresowo szkoleń dotyczących ochrony informacji;
2) techniczne, które zostaną określone przez Centrum Informatyzacji Politechniki Warszawskiej, w porozumieniu z Działem Bezpieczeństwa Informacji Politechniki Warszawskiej, zwanym dalej „DBI".

§ 4

1. Osoby wskazane w § 2 ust. 1 mogą wprowadzić Politykę bezpieczeństwa informacji oraz inne dokumenty sankcjonujące kwestie związane z bezpieczeństwem informacji dostosowane do specyfiki jednostki, które powinny zostać skonsultowane z DBI, a następnie przekazane do wiadomości pracowników, poprzez publikację odpowiednio w systemie LEX BAW lub na stronie wydziału/jednostki ogólnouczelnianej.
2. Dokumenty, o których mowa w ust. 1, powinny być zgodne z zarządzeniem oraz sprawdzane i aktualizowane przez kierownika jednostki lub osobę przez niego wskazaną.

§ 5

1. Umowy cywilnoprawne oraz umowy z kontrahentami powinny zawierać, w miarę potrzeb, oświadczenie z klauzulą o odpowiedzialności z zakresu bezpieczeństwa informacji.
2. Osoby wskazane w § 2 ust. 1 powinny wymagać od pracowników, osób zatrudnionych na podstawie umowy cywilnoprawnej oraz kontrahentów stosowania obowiązujących w Politechnice Warszawskiej zasad bezpieczeństwa informacji.
3. Pracownicy oraz osoby świadczące pracę na podstawie umowy cywilnoprawnej powinni mieć dostęp do dotyczących ich aktualnych przepisów wewnętrznych w zakresie bezpieczeństwa informacji.

§ 6

1. W Politechnice Warszawskiej prowadzi się ewidencję aktywów, w szczególności, w zakresie sprzętu teleinformatycznego, ze wskazaniem osób odpowiedzialnych za określone aktywa.
2. Przez aktywa rozumie się w szczególności: komputery, serwery, telefony, urządzenia sieciowe, oprogramowanie, zbiory i bazy danych.
3. Wprowadza się obowiązek utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację, w szczególności, w czasie okresowych przeglądów ewidencyjnych, zgodnie z obowiązującymi w Politechnice Warszawskiej przepisami.
4. Osoby użytkujące aktywa należące do Politechniki Warszawskiej, są zobowiązane do wykorzystywania ich zgodnie z przeznaczeniem i wyłącznie do wykonywania zadań służbowych oraz do ich zwrotu po zakończeniu zatrudnienia lub w każdym czasie na polecenie przełożonego.

§ 7

1. Używanie nośników wymiennych (zewnętrznych) powinno odbywać się jak najrzadziej i ze szczególną ostrożnością, zgodnie z ust. 4.
2. Informacja zawarta na nośnikach wymiennych, w miarę możliwości, powinna być zabezpieczona metodami kryptograficznymi.
3. Nośniki wycofywane z użytkowania powinny być pozbawiane zawartych na nich informacji lub poddawane takiej modyfikacji, aby ich odzyskanie było niemożliwe.
4. Przekazywanie informacji za pośrednictwem nośników zewnętrznych powinno odbywać się w sposób zapewniający poufność i integralność zawartych na nich informacji.
5. Nośniki papierowe zawierające informacje, których ujawnienie może narazić Politechnikę Warszawską na szkodę, należy niszczyć w niszczarce lub przy współpracy z firmami specjalizującymi się w niszczeniu dokumentów.

§ 8

1. Dostęp do informacji przetwarzanych w Politechnice Warszawskiej, niezależnie od jej klasyfikacji, powinien być ograniczony do niezbędnego minimum, zgodnie z uprawnieniami na danym stanowisku.
2. Każdy system informatyczny przetwarzający informacje powinien mieć opisaną procedurę kontroli dostępu, zawierającą w szczególności, zasady nadawania, zmian i odbierania uprawnień, ze szczególnym uwzględnieniem uprawnień uprzywilejowanych np. administracyjnych.
3. Dopuszcza się utworzenie jednej procedury kontroli dostępu dla wielu systemów informatycznych.
4. Za wprowadzenie procedury odpowiada administrator/właściciel systemu.
5. Dostęp do systemu informatycznego musi być ograniczony mechanizmami kontroli dostępu.
6. Każda osoba mająca dostęp do systemu informatycznego musi posiadać własny identyfikator jednoznacznie identyfikujący ją w systemie.

7. Hasła i kody uwierzytelniające użytkownika w systemie są generowane wyłącznie na jego użytek. Użytkownik ma obowiązek chronić je przed ujawnieniem innym osobom, a w przypadku ujawnienia - jak najszybciej zmienić.
8. Hasła używane do uwierzytelnienia muszą zawierać minimum 8 znaków, składać się z małych i wielkich liter oraz cyfr lub znaków specjalnych.
9. Przeglądu praw do dostępu dla systemu informatycznego dokonuje administrator systemu, przynajmniej raz w roku lub w przypadku podejrzenia, że uprawnienia nadane w systemie są nieaktualne.

§ 9

W Politechnice Warszawskiej do zabezpieczenia informacji stosuje się zabezpieczenia kryptograficzne, w szczególności do zabezpieczania: dysków, urządzeń przenośnych, informacji przesyłanych drogą elektroniczną w sposób adekwatny do zagrożeń lub wymogów przepisu prawa.

§ 10

1. Obszarem przetwarzania informacji w Politechnice Warszawskiej mogą być wszystkie budynki i pomieszczenia należące lub użytkowane przez Politechnikę Warszawską.
2. Przez obszar bezpieczny rozumie się pomieszczenia z ograniczonym dostępem, wymagające szczególnego nadzoru, w szczególności: serwerownie, pomieszczenia biurowe, sekretariaty.
3. Obszarem bezpiecznym mogą być pomieszczenia biurowe lub dydaktyczne zlokalizowane w budynkach i lokalach administrowanych przez głównych użytkowników obiektu.
4. Obszar, o którym mowa w ust. 2, powinien być zabezpieczony adekwatnie do zagrożeń mogących mieć wpływ na bezpieczeństwo informacji przetwarzanej w tym obszarze.
5. Za odpowiednią ochronę obszarów bezpiecznych odpowiadają główni użytkownicy lub wyznaczone przez nich osoby użytkujące dany obszar.

§ 11

1. Sprzęt służący do przetwarzania informacji należy odpowiednio zabezpieczyć, aby zredukować ryzyko wynikające z zagrożeń, w szczególności przed dostępem osób nieuprawnionych.
2. Wszystkie serwerowe systemy informatyczne powinny zostać wyposażone w urządzenia chroniące przed awariami zasilania, które pozwalają na bezpieczne zakończenie prac oraz zamknięcie systemu.
3. Okablowanie zasilające oraz telekomunikacyjne używane do przetwarzania informacji powinno być chronione poprzez zabezpieczenie urządzeń sieciowych oraz okablowania przed dostępem osób nieupoważnionych np. poprzez zastosowanie odpowiednich dedykowanych szaf i listew montażowych. Punkty dostępowe do sieci wewnętrznej, znajdujące się poza obszarem bezpiecznym, należy fizycznie odłączyć.
4. Dla zapewnienia właściwego poziomu bezpieczeństwa informacji oraz zapewnienia użytkownikom ciągłej i bezawaryjnej pracy należy przeprowadzać regularne przeglądy i konserwacje sprzętu teleinformatycznego, systemów oraz oprogramowania.
5. Zakres prac i częstotliwość ich wykonywania określa dokumentacja techniczna i użytkowa sprzętu komputerowego, systemów i oprogramowania.

6. Decyzję o zasadności wyniesienia sprzętu (poza obszar bezpieczny) mogą podjąć osoby wskazane w § 2 ust. 1 , w podległych sobie jednostkach.
7. Sprzęt zawierający informacje wynoszony poza obszar bezpieczny, powinien być objęty szczególną ochroną na wypadek kradzieży, zniszczeń bądź zgubienia.
8. Użytkownicy sprzętu wykorzystywanego do przetwarzania informacji, odpowiadają za zabezpieczenie sprzętu pozostawionego bez opieki np. zamknięcie laptopa w szafie, zamknięcie drzwi do pomieszczenia, w którym znajduje się komputer.
9. Osoby przetwarzające informacje powinny stosować zasadę czystego biurka i ekranu.

§ 12

Systemy informatyczne używane do przetwarzania informacji powinny posiadać procedury eksploatacyjne, zawierające co najmniej:
1) zapis do czego system jest przeznaczony;
2) proces nadania zmiany i odebrania uprawnień;
3) procedury rozpoczęcia i zakończenia pracy;
4) wskazanie osób pełniących funkcje zarządcze systemu np. administratorzy/właściciel systemu;
5) procedurę postępowania w przypadku wystąpienia sytuacji kryzysowej.

§ 13

1. W Politechnice Warszawskiej stosuje się ustandaryzowane, zarządzane centralnie, oprogramowanie antywirusowe.
2. W przypadku niemożności zainstalowania oprogramowania antywirusowego – standardowego, należy zainstalować indywidualne oprogramowanie antywirusowe, po uprzedniej akceptacji Centrum Informatyzacji Politechniki Warszawskiej.
3. W sytuacji zainstalowania indywidualnego oprogramowania odpowiedzialność za aktualizację oraz legalność oprogramowania ponosi użytkownik urządzenia, na którym zostało zainstalowane takie oprogramowanie.

§ 14

Wszystkie systemy sieciowe powinny posiadać harmonogram wykonywania kopii zapasowych, zawierający co najmniej:
1) częstotliwość wykonywania i testowania kopii zapasowych;
2) rodzaj wykonywania kopii;
3) osobę odpowiedzialną za wykonanie i testowanie kopii;
4) rodzaj nośnika, na którym wykonywane są kopie.

§ 15

1. Systemy informatyczne powinny tworzyć dzienniki zdarzeń, rejestrujące działania użytkowników oraz administratorów.
2. Dzienniki zdarzeń powinny być przechowywane przez możliwie jak najdłuższy czas. Czas przechowywania dzienników zdarzeń oraz częstotliwość ich przeglądania powinien określić administrator/właściciel systemu.

3. Wszystkie systemy informatyczne powinny mieć zsynchronizowane zegary, według jednego wzorca czasu określonego przez Centrum Informatyzacji Politechniki Warszawskiej.

§ 16

1. Każde oprogramowanie instalowane w systemach produkcyjnych powinno zostać wcześniej przetestowane w środowiskach testowych.
2. Każda instalacja w systemie produkcyjnym powinna zostać odnotowana w dzienniku zdarzeń.

§ 17

1. Administrator systemu powinien na bieżąco monitorować podatności techniczne systemu, na podstawie wykorzystywania opublikowanych podatności technicznych systemów teleinformatycznych.
2. Wszystkie odkryte podatności techniczne powinny zostać ocenione pod kątem związanego z nimi ryzyka oraz powinny zostać podjęte odpowiednie środki w celu jego przeciwdziałania.
3. Użytkownicy systemów informatycznych nie powinni samodzielnie instalować żadnego oprogramowania.
4. W przypadku konieczności zainstalowania dodatkowego oprogramowania, fakt ten powinien być zgłoszony do odpowiedniego administratora systemu, który opiekuje się danym systemem/urządzeniem.
5. Zobowiązuje się administratorów systemów, o których mowa w ust. 4, do obniżenia uprawnień użytkowników do użytkownika normalnego i nie stosowania uprawnień administratora lokalnego dla użytkowników.
6. Przepisy ust. 1 - 5 nie mają zastosowania do środowisk laboratoryjnych i komputerów wykorzystywanych do prowadzenia badań naukowych.

§ 18

Sieci teleinformatyczne PW powinny być zarządzane i nadzorowane zgodnie z Regulaminem sieci teleinformatycznych PW.

§ 19

1. W systemach informatycznych zabezpieczenie informacji polega na stosowaniu odpowiednich zabezpieczeń m.in. kryptograficznych.
2. Rodzaj zabezpieczenia komunikacji z podmiotami zewnętrznymi powinien zostać, w razie potrzeby, zawarty w odpowiednich porozumieniach/umowach.

§ 20

1. Każdy nowo wprowadzany lub rozbudowywany system informatyczny powinien mieć sprecyzowane wymagania dotyczące bezpieczeństwa informacji. Za sprecyzowanie wymagań odpowiadają osoby wskazane w § 2 ust. 1.
2. Wszystkie usługi aplikacyjne wystawione w sieciach publicznych należy odpowiednio zabezpieczyć przed nieuczciwymi działaniami oraz nieuprawnionym ujawnieniem i zmianą.

§ 21

1. Dane testowe należące do kategorii danych chronionych powinny być starannie wybierane, chronione i nadzorowane w celu wykonywania powtarzalnych testów.
2. W przypadku konieczności testowania na danych rzeczywistych, należy zapewnić ich bezpieczeństwo na poziomie takim, jak zbiór danych źródłowych.

§ 22

1. W uzasadnionych przypadkach w zawieranych umowach z podmiotami zewnętrznymi, zamieszcza się informację o wymaganiach dotyczących bezpieczeństwa informacji w Politechnice Warszawskiej. Przepisy dotyczące bezpieczeństwa informacji można konsultować z DBI.
2. W trakcie trwania umowy należy monitorować realizację określonych w umowie wymagań bezpieczeństwa informacji przez podmioty zewnętrzne. Za monitoring odpowiada osoba odpowiedzialna za realizację umowy lub osoba przez nią wskazana.
3. Wszelkie incydenty mające wpływ na bezpieczeństwo informacji należy niezwłocznie zgłaszać mailowo do DBI na adres: incydent.odo@pw.edu.pl.

§ 23

1. Środki przetwarzania informacji należy wdrażać z nadmiarem wystarczającym do spełnienia wymagań dostępności.
2. Administratorzy systemów i sieci powinni monitorować stan wykorzystania zasobów tak, aby z wyprzedzeniem planować rozbudowę infrastruktury.

§ 24

Traci moc zarządzenie nr 38/2016 Rektora PW z dnia 9 sierpnia 2016 r. w sprawie bezpieczeństwa informacji w Politechnice Warszawskiej.

§ 25

Zarządzenie wchodzi w życie z dniem podpisania.

REKTOR

prof. dr hab. inż. Krzysztof Zaremba