Zarządzenie nr 88

Rektora Zachodniopomorskiego Uniwersytetu Technologicznego w Szczecinie

z dnia 15 października 2024 r.

w sprawie wprowadzenia Polityki bezpieczeństwa informacji
w Zachodniopomorskim Uniwersytecie Technologicznym w Szczecinie

Na podstawie art. 23 ustawy z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce (Dz. U. z 2023 r. poz. 742, z późn.zm.) zarządza się, co następuje:

§ 1.

Wprowadza się Politykę bezpieczeństwa informacji w Zachodniopomorskim Uniwersytecie Technologicznym w Szczecinie, która stanowi załącznik do niniejszego zarządzenia.

§ 2.

Zarządzenie wchodzi w życie z dniem podpisania.

Rektor: Arkadiusz Terman

Załącznik

do zarządzenia nr 88 Rektora ZUT z dnia 15 października 2024 r.

Polityka bezpieczeństwa informacji

w Zachodniopomorskim Uniwersytecie Technologicznym w Szczecinie

Postanowienia ogólne

§ 1.

1. Zasoby informacyjne, będące w posiadaniu Zachodniopomorskiego Uniwersytetu Technologicznego w Szczecinie, zwanego dalej „ZUT" lub „Uczelnią", to wysokiej wagi aktywa, mające zasadnicze znaczenie zarówno dla interesów ZUT, jak i pracowników, studentów oraz doktorantów. Ochrona tych aktywów jest podstawowym obowiązkiem każdego pracownika, studenta oraz doktoranta Uczelni.
2. Polityka bezpieczeństwa informacji w ZUT, zwana dalej „Polityką bezpieczeństwa", odnosi się do wszystkich procesów i czynności realizowanych w ramach Uczelni oraz dotyczy wszystkich osób w nich uczestniczących, takich jak: jednostki organizacyjne, pracownicy, studenci, doktoranci i osoby trzecie.
3. Polityka bezpieczeństwa obejmuje wszelkie zasoby informacyjne, systemy komputerowe, sieci, urządzenia końcowe, jak również dane osobowe i inne informacje chronione prawem.
4. Niniejszy dokument został opracowany w oparciu o obowiązujące przepisy prawa, wytyczne, zlecenia oraz w oparciu o najlepsze praktyki.

§ 2.

Ilekroć jest mowa o:

1) Administratorze Systemów Informatycznych (ASI) – należy przez to rozumieć wyznaczonego pracownika odpowiedzialnego za administrowanie określonym zasobem;
2) bezpieczeństwie informacji – należy przez to rozumieć ogół działań podejmowanych w celu zapewnienia poufności, integralności i dostępności przetwarzania informacji;
3) danych osobowych – należy przez to rozumieć informacje o zidentyfikowanej bądź możliwej do zidentyfikowania osobie fizycznej (osobie, której dane dotyczą);
4) incydencie – należy przez to rozumieć niespodziewane bądź niepożądane zdarzenie lub serię zdarzeń, które świadczą o naruszeniu lub wysokim ryzyku naruszenia bezpieczeństwa informacji. Identyfikacja incydentu skutkuje koniecznością podjęcia stosownej reakcji;
5) informacji – należy przez to rozumieć wszelkie zasoby informacyjne stanowiące wartość dla Uczelni;

6) informacjach chronionych – należy przez to rozumieć wszystkie informacje o charakterze finansowym, handlowym, kadrowym, organizacyjnym, strategicznym, technicznym, technologicznym lub inne informacje posiadające wartość dla Uczelni, np. dane osobowe pracowników, studentów, doktorantów;
7) jednostce organizacyjnej – należy przez to rozumieć jednostkę organizacyjną ZUT, np. wydział, szkoła doktorska, jednostki ogólnouczelniane, międzywydziałowe, a także jednostki administracji i samodzielne stanowiska pracy;
8) kierowniku jednostki organizacyjnej – należy przez to rozumieć wyznaczonego pracownika odpowiedzialnego za kierowanie jednostką organizacyjną;
9) logi – należy przez to rozumieć uporządkowane, sekwencyjne zapisy zdarzeń występujących w systemach IT, aplikacjach, urządzeniach sieciowych. Logi są generowane automatycznie, zawierają m.in. datę i czas zdarzenia, status (powodzenie, niepowodzenie), źródło zdarzenia (np. użytkownik, proces) oraz jego opis (np. próba zalogowania);
10) osobie zewnętrznej – należy przez to rozumieć osobę fizyczną, osobę prawną lub jednostkę organizacyjną nieposiadającą osobowości prawnej, której ustawa przyznaje zdolność prawną, niebędącą pracownikiem lub studentem, realizującą na rzecz ZUT prace zlecone przez Uczelnię, uprawnioną do dostępu do informacji;
11) podatności – należy przez to rozumieć lukę w systemie informatycznym, która może zostać wykorzystana do uzyskania nieautoryzowanego dostępu do informacji lub systemu IT, a tym samym sprowadzać ryzyko naruszenia bezpieczeństwa IT oraz bezpieczeństwa informacji, które są przetwarzane;
12) przetwarzaniu informacji – należy przez to rozumieć wszelkie operacje wykonywane na informacjach, takie jak gromadzenie, modyfikowanie, przechowywanie, opracowywanie, udostępnianie, utrwalanie, usuwanie, również w systemach IT;
13) Uczelnianym Centrum Informatyki (UCI) – należy przez to rozumieć jednostkę organizacyjną powołaną do zarządzania infrastrukturą informatyczną Uczelni;
14) urządzeniach końcowych – należy przez to rozumieć każde urządzenie, które łączy się z siecią (np. komputer, smartfon, tablet, drukarka), wykorzystywane przez użytkownika do komunikacji lub przetwarzania danych;
15) użytkowniku – należy przez to rozumieć pracownika, studenta, doktoranta lub osobę zewnętrzną upoważnioną do dostępu do zasobów Uczelni;
16) użytkowniku wewnętrznym – należy przez to rozumieć pracownika, studenta lub doktoranta;

17) zasobie – należy przez to rozumieć urządzenie końcowe lub usługę informatyczną świadczoną na rzecz Uczelni przez Uczelniane Centrum Informatyki lub inne podmioty zewnętrzne, opartą na przetwarzaniu informacji.

Cele Polityki bezpieczeństwa

§ 3.

Celami Polityki bezpieczeństwa są:

1) ustanowienie zasad i procedur związanych z przetwarzaniem i ochroną zasobów informacyjnych i infrastruktury technicznej;
2) określenie ogólnych ram bezpieczeństwa wszystkich przetwarzanych informacji oraz sposób zabezpieczenia systemów komputerowych;
3) zapewnienie, w odniesieniu do przetwarzanych informacji chronionych, odpowiedniego poziomu atrybutów bezpieczeństwa zgodnie z poniższymi kryteriami:
   a) dostępność – Uczelnia zapewnia, że dane oraz informacje przechowywane w jej systemach są dostępne dla uprawnionych użytkowników w każdym momencie, z minimalnymi przerwami w działaniu;
   b) integralność – Uczelnia zapewnia, że dane oraz informacje przechowywane w jej systemach są chronione przed nieautoryzowanymi modyfikacjami;
   c) poufność – Uczelnia zobowiązuje się do ochrony poufności danych oraz informacji wrażliwych poprzez wdrożenie odpowiednich środków technicznych i organizacyjnych.

Ogólne zasady bezpieczeństwa informacji

§ 4.

1. Uczelnia zapewnia, że wszystkie informacje chronione są przechowywane w sposób zapewniający kryteria bezpieczeństwa, tj. poufność, integralność i dostępność. Dane wrażliwe muszą być szyfrowane zarówno podczas przesyłania, jak i przechowywania.
2. Uczelnia zapewnia, że sieci komputerowe i wszelkie systemy informatyczne funkcjonujące na Uczelni są chronione przed nieautoryzowanym dostępem za pomocą wszelkich niezbędnych do tego celu systemów informatycznych. Wszelkie próby nieautoryzowanego dostępu są odnotowywane w systemie logów. Dokumentacja zawierająca szczegółowe informacje na temat konfiguracji zabezpieczeń jest przechowywana i na bieżąco uaktualniana w Uczelnianym Centrum Informatyki.
3. W ramach bezpieczeństwa fizycznego Uczelnia zapewnia ochronę budynków, urządzeń i infrastruktury przed zagrożeniami fizycznymi, w tym kradzieżami, zniszczeniem mienia oraz zagrożeniami wynikającymi z katastrof naturalnych.

4. Uczelniane Centrum Informatyki opracowuje i na bieżąco uaktualnia dokumenty: “Plan ciągłości działania”, “Plan odzyskania danych”, “Zasady i procedury bezpieczeństwa infrastruktury informatycznej ZUT”, “Procedury zarządzania tożsamością w Zachodniopomorskim Uniwersytecie Technologicznym w Szczecinie”, “Analizę ryzyka bezpieczeństwa informacji” oraz “Plan zarządzania incydentami”. Dokumenty te podlegają corocznemu przeglądowi.

§ 5.

1. Dostęp do zasobów jest przyznawany każdemu użytkownikowi poprzez nadanie uprawnień. Zasady nadawania uprawnień w systemach przetwarzających dane osobowe określa Instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w ZUT, stanowiąca załącznik nr 2 do zarządzenia nr 89 Rektora ZUT z dnia 2 października 2018 r., z późn. zm., natomiast zarządzanie dostępem do wszystkich pozostałych systemów określają Zasady korzystania z infrastruktury informatycznej ZUT (zarządzenie nr 32 Rektora ZUT z dnia 5 czerwca 2019 r.).
2. Dostęp do systemów informatycznych Uczelni przyznawany jest na podstawie zasady najmniejszych uprawnień, tj. użytkownik otrzymuje dostęp wyłącznie do tych informacji i zasobów, które są niezbędne do wykonywania pracy. Celem działania jest zminimalizowanie zagrożeń związanych z niepożądanym wglądem w newralgiczne dane oraz zapobieganie wyciekom danych powodowanych przez cyberataki.
3. Wszyscy użytkownicy systemów informatycznych Uczelni są zobowiązani do przestrzegania “Zasad korzystania z infrastruktury ZUT”. Treść aktualnej wersji dokumentu jest publikowana w serwisie WWW Uczelnianego Centrum Informatyki w zakładce “Regulaminy i procedury”.

Zasady zgłaszania incydentów bezpieczeństwa

§ 6.

1. W przypadku podejrzenia zaistnienia incydentu, każdy Użytkownik zobowiązany jest do natychmiastowego zgłoszenia tego faktu za pomocą jednego z poniższych kanałów informacyjnych:
   1) informatycznego systemu wsparcia użytkowników, dostępnego za pośrednictwem strony internetowej https://helpdesk.zut.edu.pl;
   2) wiadomości e-mail, kierowanej na adres uci@zut.edu.pl;
   3) telefonicznie pod numerem +48 91 449 58 00.
2. Uczelniane Centrum Informatyki zarządza obsługą incydentów zgodnie z “Planem zarządzania incydentami”. Dokument ten jest na bieżąco aktualizowany i podlega corocznym przeglądom.

Szkolenia użytkowników wewnętrznych

§ 7.

1. Każdy użytkownik wewnętrzny jest zobowiązany do udziału przynajmniej raz w roku w szkoleniu dotyczącym bezpieczeństwa informatycznego.
2. Szkolenie, o którym mowa w ust. 1, Uczelniane Centrum Informatyki udostępnia na swojej stronie internetowej pod adresem: https://uci.zut.edu.pl/szkolenia.

Zakres odpowiedzialności

§ 8.

1. Każdy użytkownik zobowiązany jest do przestrzegania zapisów w dokumencie “Zasady korzystania z infrastruktury informatycznej ZUT”. W szczególności dotyczy to ochrony danych uwierzytelniających, które umożliwiają dostęp do zasobów.
2. Kierownicy jednostek organizacyjnych są odpowiedzialni za zapewnienie, że wszystkie osoby w podległych im jednostkach przestrzegają zapisów niniejszego dokumentu.
3. ASI zobowiązany jest do stosowania się do procedur obowiązujących w Uczelni w zakresie zarządzania bezpieczeństwem.
4. Dyrektor Uczelnianego Centrum Informatyki jest odpowiedzialny za nadzór nad przestrzeganiem procedur w zakresie zarządzania bezpieczeństwem informacji.
5. Rektor sprawuje ogólny nadzór nad bezpieczeństwem informacji w Uczelni, zapewniając zgodność działań z przyjętymi zasadami i regulacjami.

Kontrole i audyty bezpieczeństwa

§ 9.

1. Procedury bezpieczeństwa informacji podlegają corocznemu audytowi, prowadzonemu przez audytora wewnętrznego lub odpowiedni podmiot zewnętrzny. Audyt ma na celu ocenę zgodności procedur z obowiązującymi przepisami i standardami bezpieczeństwa, a także identyfikację potencjalnych luk i zagrożeń.
2. Zakres audytu obejmuje ocenę skuteczności wdrożonych środków ochrony, analizę ryzyka, przegląd polityk i procedur bezpieczeństwa oraz weryfikację zgodności z przepisami prawa.
3. Raport z audytu zawiera wnioski, rekomendacje oraz ewentualne zalecenia dotyczące działań naprawczych.
4. Działania naprawcze powinny być wdrożone w ustalonym terminie, a ich realizacja regularnie monitorowana i raportowana. Za realizację zaleceń wynikających z audytu odpowiedzialni są kierownicy jednostek, ASI, Dyrektor UCI oraz Rektor.

Przepisy końcowe

§ 10.

Niniejszy dokument podlega bieżącej aktualizacji i corocznym przeglądom. Naruszenie zasad określonych w niniejszej Polityce może skutkować odpowiedzialnością dyscyplinarną zgodnie z wewnętrznymi regulacjami Uczelni oraz obowiązującymi przepisami prawa.