Politechnika Śląska

Monitor Prawny Politechniki Śląskiej

poz. 346

ZARZĄDZENIE NR 63/2024
REKTORA POLITECHNIKI ŚLĄSKIEJ
z dnia 8 kwietnia 2024 r.

w sprawie Instrukcji zarządzania systemami informatycznymi na Politechnice Śląskiej

Na podstawie art. 23 ust. 1 ustawy z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce (j.t. Dz. U. z 2023 r. poz. 742, z późn. zm.), w związku z ustawą z dnia 17 lutego 2005 r. o informatyzacji podmiotów realizujących działania publiczne (j.t. Dz. U. z 2024 r. poz. 307) oraz rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. 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) (Dz.U.UE.L.2016.119.1), zarządza się, co następuje:

§ 1

Wprowadza się Instrukcję zarządzania systemami informatycznymi na Politechnice Śląskiej stanowiącą załącznik do niniejszego zarządzenia.

§ 2

Traci moc zarządzenie nr 89/2021 Rektora Politechniki Śląskiej z dnia 27 maja 2021 r. w sprawie wprowadzenia Regulaminu przestrzegania zasad ochrony informacji na Politechnice Śląskiej (Monitor Prawny PŚ z 2021 r. poz. 413).

§ 3

Zarządzenie wchodzi w życie z dniem 1 maja 2024 roku.

Rektor PŚ: *A. Mężyk*

Instrukcja zarządzania systemami informatycznymi na Politechnice Śląskiej

Postanowienia ogólne

§ 1

Celem wprowadzenia Instrukcji jest ustalenie zasad zarządzania systemami informatycznymi, za pomocą których przetwarzane są informacje, w tym dane osobowe, oraz określenie odpowiedzialności za poszczególne czynności wynikające z niniejszej Instrukcji.

§ 2

1. Terminologia użyta w niniejszej Instrukcji jest tożsama z terminologią użytą w Polityce ochrony danych osobowych na Politechnice Śląskiej. Pojęcia niezdefiniowane w Polityce ochrony danych osobowych na Politechnice Śląskiej zostały zdefiniowane w słowniku Instrukcji.
2. Ilekroć w Instrukcji jest mowa o:
   1) Uczelni – należy przez to rozumieć Politechnikę Śląską;
   2) danych uwierzytelniających – należy przez to rozumieć informacje pozwalające na zidentyfikowanie użytkownika w systemie informatycznym;
   3) dysponencie systemu informatycznego – należy przez to rozumieć osobę, która decyduje o celach i sposobach wykorzystania systemu informatycznego;
   4) informacjach – należy przez to rozumieć aktywo niezbędne do prowadzenia działalności Uczelni (w tym m.in. wyniki badań naukowych, dane osobowe itp.);
   5) Instrukcji – należy przez to rozumieć niniejszy dokument;
   6) oprogramowaniu – należy przez to rozumieć ogół informacji w postaci zestawu instrukcji, zaimplementowanych interfejsów i zintegrowanych danych przeznaczonych dla komputera do realizacji wyznaczonych celów;
   7) serwerowni – należy przez to rozumieć wydzielone pomieszczenie przeznaczone organizacyjnie i technicznie wyłącznie do umieszczania w nim urządzeń komputerowych, zapewniające odpowiednie warunki do ich pracy, obsługi, ochrony i podłączenie do sieci informatycznej, jak również posiadające wyznaczoną, stałą obsługę techniczną;
   8) systemie informatycznym – należy przez to rozumieć urządzenie lub grupę wzajemnie związanych ze sobą urządzeń komputerowych, których jedno lub więcej dokonuje przetwarzania informacji zgodnie z programem.
3. Wprowadza się następujący podział systemów informatycznych na Politechnice Śląskiej:
   1) systemy informatyczne administrowane centralnie przez Centrum Informatyczne;
   2) systemy informatyczne posiadające wielu użytkowników, nadzorowane przez wyznaczonego administratora danego systemu informatycznego;
   3) systemy informatyczne posiadające jednego użytkownika, któremu za nie przypisano odpowiedzialność.

Nadawanie uprawnień do systemów informatycznych

§ 3

1. Do przetwarzania danych osobowych w systemach informatycznych funkcjonujących w Uczelni mogą mieć dostęp wyłącznie osoby posiadające upoważnienie do przetwarzania danych osobowych na Politechnice Śląskiej.
2. Dostęp do systemów informatycznych Politechniki Śląskiej wymagających uwierzytelnienia może mieć tylko zarejestrowany użytkownik systemu. Kontrola dostępu do systemów informatycznych jest zapewniona przez przypisane użytkownikowi identyfikator i dane uwierzytelniające. Uwierzytelnianie w centralnych systemach informatycznych odbywa się z wykorzystaniem centralnego systemu katalogowego Politechniki Śląskiej.

3. W przypadku gdy administrator danego systemu informatycznego nadaje uprawnienia dostępowe bez wykorzystania usługi centralnego systemu katalogowego Politechniki Śląskiej, jest on zobowiązany zapewnić, aby system pozwalał na rozliczalność działań użytkownika w systemie oraz aby dostęp do systemu miały wyłącznie osoby uprawnione.
4. Dla systemów informatycznych administrowanych przez Centrum Informatyczne nadanie i zmiana uprawnień następują na wniosek przełożonego, zgodnie z zasadą wiedzy koniecznej do wykonywania przydzielonych zadań. W przypadku zmiany przydzielonych zadań przełożony jest zobowiązany do złożenia wniosku o zmianę lub odebranie uprawnień.
5. W przypadku powzięcia informacji o ustaniu podstawy nadania identyfikatora w centralnym systemie katalogowym Politechniki Śląskiej administrator systemu informatycznego ma prawo do zablokowania identyfikatora i odebrania uprawnień.
6. Dla pozostałych systemów informatycznych nadanie i zmiana uprawnień następują na podstawie decyzji dysponenta systemu informatycznego, zgodnie z zasadą wiedzy koniecznej do wykonywania przydzielonych zadań i z zachowaniem rozliczalności. Dysponent systemu informatycznego jest zobowiązany do wykonywania okresowych przeglądów nadanych uprawnień, nie rzadziej niż raz w roku.
7. Identyfikator studenta w centralnym systemie katalogowym Politechniki Śląskiej oraz uprawnienia w uczelnianym systemie obsługi studiów nadaje Centrum Informatyczne. Uprawnienia są nadawane po immatrykulacji studenta.
8. Identyfikator doktoranta w centralnym systemie katalogowym Politechniki Śląskiej nadaje Centrum Informatyczne na wniosek dyrektora Szkoły Doktorów. Centrum Informatyczne na wniosek dyrektora Szkoły Doktorów przedłuża ważność konta dla doktoranta do dnia nadania stopnia lub odmowy nadania stopnia przez właściwą radę dyscypliny.
9. Osobom realizującym zadania na podstawie umów cywilnoprawnych identyfikator w centralnym systemie katalogowym Politechniki Śląskiej jest nadawany na wniosek kierownika jednostki, gdzie są realizowane zadania wynikające z umowy.
10. Wolontariuszom identyfikator w centralnym systemie katalogowym Politechniki Śląskiej jest nadawany na wniosek kierownika Biura Karier Studenckich.
11. W pozostałych przypadkach identyfikator w centralnym systemie katalogowym Politechniki Śląskiej jest nadawany po uzyskaniu zgody rektora.
12. Użytkownik ponosi odpowiedzialność za czynności wykonane w systemie informatycznym przy użyciu jego identyfikatora i hasła, w zakresie posiadanych uprawnień.
13. Administratorzy systemów informatycznych prowadzą rejestry użytkowników systemów informatycznych, którymi administrują.

Polityka haseł

§ 4

1. Hasło służące do uwierzytelniania w systemie informatyczny składa się z co najmniej 12 znaków.
2. Hasło musi zawierać co najmniej 3 z 4 następujących grup znaków: duże i małe litery alfabetu łacińskiego, cyfry, znaki specjalne.
3. Każde nowe hasło musi być inne niż wcześniej stosowane hasła w centralnym systemie katalogowym Politechniki Śląskiej.
4. Hasło nie może zawierać imienia, nazwiska oraz nazwy użytkownika.
5. Hasło nie powinno zawierać polskich znaków, ze względu na możliwe problemy będące konsekwencją różnego kodowania polskich znaków w różnych aplikacjach i systemach.
6. Zaleca się stosowanie uwierzytelnienia wieloskładnikowego.
7. Zabrania się przechowywania haseł w formie jawnej (niezaszyfrowanej). W razie utraty hasła administrator danego systemu informatycznego na wniosek użytkownika generuje nowe hasło i przekazuje je w sposób bezpieczny użytkownikowi, z wymogiem zmiany hasła po pierwszym logowaniu.
8. Zabronione jest ujawnianie haseł osobom trzecim.
9. Użytkownik jest zobowiązany do zachowania wszelkich środków ostrożności w trakcie wpisywania danych uwierzytelniających.

10. W przypadku gdy istnieje podejrzenie ujawnienia danych uwierzytelniających osobie trzeciej, użytkownik jest zobowiązany do natychmiastowej zmiany tych danych i poinformowania o tym administratora systemu informatycznego.
11. Nie należy wykorzystywać służbowych danych uwierzytelniających (np. identyfikatora użytkownika i hasła) w celu uwierzytelniania w systemach innych niż Politechniki Śląskiej.

Oprogramowanie

§ 5

1. Instalacja oprogramowania na komputerach przeznaczonych tylko do pracy służbowej jest dozwolona wyłącznie za zgodą administratora danego systemu informatycznego.
2. Dla systemów informatycznych administrowanych centralnie zgodę na instalację oprogramowania wyraża dyrektor Centrum Informatycznego.
3. W przypadku systemów informatycznych posiadających wielu użytkowników zgodę na instalację oprogramowania wyraża administrator danego systemu informatycznego.
4. W przypadku systemów informatycznych posiadających jednego użytkownika będącego jednocześnie administratorem odpowiedzialność za zainstalowane oprogramowanie ponosi jego użytkownik.
5. Zakup oprogramowania przez Politechnikę Śląską jest realizowany zgodnie z zasadami obowiązującymi w Uczelni, za zgodą dyrektora Centrum Informatycznego. W uzasadnionych przypadkach dyrektor Centrum Informatycznego konsultuje zakup z inspektorem ochrony danych.
6. Planując zakup oprogramowania, należy dokonać analizy oprogramowania pod kątem integracji z już posiadanymi przez Uczelnię systemami informatycznymi.
7. Dopuszcza się użytkowanie wyłącznie oprogramowania, do którego używania Politechnika Śląska posiada prawo. Spis oprogramowania prowadzi Centrum Informatyczne na podstawie informacji uzyskanych od pełnomocników ds. nadzoru nad oprogramowaniem licencjonowanym.
8. Dokumenty potwierdzające posiadanie licencji na oprogramowanie są przechowywane przez administratora danego systemu informatycznego.

Procedury kończenia i rozpoczynania pracy przez użytkowników systemów informatycznych

§ 6

1. Przed rozpoczęciem pracy każdy użytkownik jest zobowiązany ustawić monitor komputera w taki sposób, aby żadna z nieuprawnionych osób nie mogła zobaczyć informacji wyświetlanych na ekranie.
2. Użytkownik, rozpoczynając pracę w systemie informatycznym, powinien się zalogować, korzystając z własnych danych uwierzytelniających.
3. Użytkownik systemu informatycznego jest zobowiązany do zabezpieczenia swojego komputera na czas opuszczenia miejsca pracy poprzez zamknięcie sesji (wylogowanie się) lub zablokowanie dostępu do komputera wygaszaczem ekranu chronionym hasłem, a w przypadku zakończenia pracy – wyłączania komputera.
4. Zabrania się użytkownikom samodzielnego wyłączania, blokowania i odinstalowywania programów zabezpieczających system informatyczny (np. programów antywirusowych, zapór sieciowych). W uzasadnionych przypadkach administrator systemu informatycznego może zezwolić na czasowe ich wyłączenie.
5. Sprzęt służbowy stanowi własność Uczelni, co oznacza, że pracownicy powinni korzystać z tego sprzętu zgodnie z jego przeznaczeniem.

Testowanie i wprowadzanie nowego oprogramowania

§ 7

1. Zaleca się oddzielenie środowisk testowych i produkcyjnych celem redukcji ryzyka związanego z nieuprawnionym dostępem lub zmianami w środowisku produkcyjnym.
2. Zabrania się kopiowania danych osobowych do systemu pracującego w środowisku testowym, dopóki nie zostaną wdrożone odpowiednie zabezpieczenia.

Zabezpieczanie systemu przed działaniem szkodliwego oprogramowania

§ 8

1. Za szkody wyrządzone w systemie informatycznym przez działania użytkownika niezgodne z instrukcją użytkowania systemu informatycznego odpowiada użytkownik odpowiedzialny za dane stanowisko komputerowe lub osoba aktualnie korzystająca ze stanowiska.
2. Administrator systemu informatycznego na podstawie analizy ryzyka stosuje i nadzoruje zabezpieczenia systemu informatycznego przeciwko zidentyfikowanym zagrożeniom, w szczególności przeciwko:
   1) nieuprawnionemu dostępowi;
   2) szkodliwemu oprogramowaniu.
3. Dla systemów informatycznych centralnych i użytkowanych przez wielu użytkowników administrator dokonuje analizy ryzyka po konsultacji z LASI i na podstawie jej wyników wdraża odpowiednie dla zidentyfikowanego ryzyka zabezpieczenia przed działaniem szkodliwego oprogramowania.
4. Administrator systemu informatycznego jest zobowiązany do dbania o bezpieczeństwo systemu informatycznego w szczególności poprzez:
   1) instalację aktualizacji oprogramowania;
   2) regularną weryfikację poprawności konfiguracji;
   3) wykonywanie kopii zapasowych.
5. Administrator systemu informatycznego jest zobowiązany do wycofywania z eksploatacji oprogramowania niewspieranego przez producenta (w szczególności systemów operacyjnych). Dopuszcza się stosowanie oprogramowania niespełniającego tego warunku w systemach informatycznych odseparowanych od reszty sieci komputerowej Politechniki Śląskiej.

Procedury tworzenia kopii zapasowych

§ 9

1. Na Politechnice Śląskiej wprowadzono harmonogram tworzenia kopii zapasowych dla informacji i systemów informatycznych znajdujących w administrowaniu Centrum Informatycznego. Harmonogram nie podlega publikacji.
2. Dla informacji i systemów informatycznych znajdujących się w administrowaniu Centrum Informatycznego wykonywane są trzy kopie zapasowe na dwóch różnych nośnikach. Jedna kopia informacji jest przechowywana poza siedzibą Centrum Informatycznego.
3. Okresowo kopie zapasowe podlegają testowaniu pod względem rzeczywistej możliwości odtworzenia informacji i środowisk służących do odtworzenia informacji.
4. Za terminowość i poprawność wykonywania kopii zapasowych i oprogramowania dla systemów informatycznych administrowanych przez Centrum Informatyczne odpowiada ASI.
5. Dla pozostałych systemów informatycznych administrator danego systemu informatycznego określa zasady i harmonogram wykonywania kopii zapasowych na podstawie analizy ryzyka dotyczącej zapewnienia ciągłości działania w przypadku utraty informacji. Analizy ryzyka dokonuje się po konsultacji z LASI.
6. Dla systemów informatycznych z jednym użytkownikiem zaleca się wykonywanie automatycznych kopii informacji z użyciem dostępnego w systemie operacyjnym mechanizmu wykonywania kopii zapasowych, nie rzadziej niż raz w tygodniu, przy użyciu usług chmurowych dostępnych na Politechnice Śląskiej (np. dysk sieciowy OneDrive usługi Microsoft 365).

Korzystanie z urządzeń mobilnych będących własnością lub użyczonych Politechnice Śląskiej

§ 10

1. W Uczelni prowadzi się rejestr urządzeń mobilnych udostępnianych pracownikom.
2. Użytkownik odpowiada za zabezpieczenie należących do Politechniki Śląskiej lub użyczonych Politechnice Śląskiej urządzeń mobilnych przed zniszczeniem, uszkodzeniem, utratą lub kradzieżą.
3. Osoby korzystające z urządzeń mobilnych są zobowiązane do zachowania ostrożności podczas korzystania z nich w miejscach publicznych, salach konferencyjnych i innych niezabezpieczonych obszarach.
4. Zakazane jest użyczanie sprzętu mobilnego osobom nieupoważnionym.
5. Urządzenia mobilne muszą posiadać zabezpieczenia dostępu przed osobami nieuprawnionymi.

6. Dane osobowe w urządzeniach mobilnych wymagają szyfrowania w przypadku wynoszenia sprzętu poza teren Uczelni.
7. Dostęp do sieci Politechniki Śląskiej przez pracowników korzystających z urządzeń mobilnych należących do Uczelni jest realizowany poprzez mechanizm VPN lub VDI zapewniający uwierzytelnienie użytkownika i szyfrowanie danych osobowych.
8. W przypadku korzystania z prywatnych urządzeń mobilnych konieczne jest odseparowanie operacji wykonywanych w celach prywatnych od operacji wykonywanych w celach służbowych.

Zasady bezpieczeństwa przy wykonywaniu pracy zdalnej

§ 11

Zasady bezpieczeństwa przy wykonywaniu pracy zdalnej zostały opisane w zarządzeniu nr 62/2024 Rektora Politechniki Śląskiej z dnia 8 kwietnia 2024r. w sprawie Polityki ochrony danych osobowych na Politechnice Śląskiej.

Procedura konserwacji i napraw sprzętu służącego do przetwarzania informacji

§ 12

1. Wszelkie prace konserwacyjne i naprawy urządzeń służących do przetwarzania informacji, zlecone osobom i podmiotom zewnętrznym, można wykonywać wyłącznie pod warunkiem zastosowania w umowach klauzul o zachowaniu poufności.
2. W przypadku braku możliwości zawarcia stosownej umowy należy zdemontować wszystkie nośniki przed udostępnieniem sprzętu do naprawy lub dokonać trwałego usunięcia informacji. W przypadku urządzeń, z których nie można usunąć nośników informacji, diagnostyka i naprawa takiego urządzenia jest możliwa wyłącznie w obecności administratora danego systemu informatycznego, LASI lub innej osoby wskazanej przez ASI.
3. W przypadku naprawy polegającej na wymianie uszkodzonego nośnika informacji uszkodzony nośnik nie podlega przekazaniu firmie dokonującej naprawy i musi być zutylizowany w sposób gwarantujący trwałe usunięcie informacji.
4. W przypadku przekazania sprzętu komputerowego innej osobie zatrudnionej na Politechnice Śląskiej administrator danego systemu informatycznego jest zobowiązany do usunięcia informacji z komputera lub też dostosowanie zasobów informacji zapisanych na dysku do zakresu upoważnienia, które posiada osoba, której sprzęt komputerowy jest przekazywany.

Postępowanie z nośnikami informacji

§ 13

1. Nośniki informacji niezainstalowane w urządzeniu komputerowym muszą być przechowywane w sposób zabezpieczający przed dostępem osób niepowołanych, w warunkach zgodnych z zaleceniami producenta.
2. Wycofanie nośnika informacji z eksploatacji musi być poprzedzone trwałym usunięciem informacji (uniemożliwiającym odczyt).
3. W przypadku wycofywania z eksploatacji nośnika, z którego nie można trwale usunąć informacji, należy dokonać utylizacji nośnika w sposób gwarantujący brak możliwości odczytu.
4. Za właściwe przechowanie, zabezpieczenie i prawidłowe wycofanie z eksploatacji nośników informacji odpowiada jednostka posiadająca nośnik na inwentarzu.
5. W przypadku nośników, które są używane poza wyznaczonymi pomieszczeniami (w szczególności nośniki przeznaczone do przenoszenia danych poza pomieszczenia Politechniki Śląskiej) konieczne jest zastosowanie technik kryptograficznych gwarantujących brak możliwości odczytu informacji bez znajomości kodów dostępu.
6. Zaleca się, aby podłączenia nośnika informacji do komputera w sposób automatyczny wymuszało skanowanie nośnika przez oprogramowanie antywirusowe.
7. Wprowadza się zakaz ładowania prywatnych urządzeń z użyciem portów USB komputerów lub innych urządzeń służbowych.

Poczta elektroniczna

§ 14

1. Korzystanie ze służbowej poczty elektronicznej jest jednym ze sposobów realizowania obowiązków powierzonych użytkownikowi poczty i powinno być realizowane wyłącznie w celach służbowych związanych z realizowaniem zadań.
2. Użytkownicy poczty elektronicznej są odpowiedzialni za korzystanie z niej w taki sposób, aby zminimalizować ryzyko naruszenia bezpieczeństwa informacji.
3. Zaleca się, aby przed wysłaniem pierwszej wiadomości użytkownik spersonalizował środowisko wysyłania wiadomości, w tym ustawił podpis pod wysyłanymi wiadomościami zgodnie z obowiązującym Systemem identyfikacji wizualnej.
4. W przypadku czasowej nieobecności wymagane jest ustawienie odpowiedzi automatycznej zawierającej informację o okresie nieobecności oraz o osobie, która zastępuje pracownika podczas jego nieobecności i do której nadawca może przekazać wiadomość.
5. Każda wysyłana wiadomość powinna zawierać dane identyfikujące autora wiadomości, jego jednostkę oraz funkcję, w jakiej występuje.
6. Jeżeli kilku pracowników korzysta z ogólnego adresu e-mail, np. kontakt@polsl.pl, to każda wysyłana wiadomość powinna być podpisana imieniem i nazwiskiem osoby, która jest autorem wiadomości.
7. Wiadomości należy wysyłać z zachowaniem należytej staranności w zakresie sprawdzenia poprawności treści, załączników, a także jej adresatów.
8. Przekazywanie wiadomości do wielu adresatów w sposób ujawniający dane adresatów w polach „DO” lub „DW”/ ”DO WIADOMOŚCI” jest dozwolone tylko w sytuacjach w których jest to celowe, żeby każdy z odbiorców znał dane pozostałych adresatów. W pozostałych sytuacjach zaleca się wykorzystywanie w korespondencji masowej pola „UDW”/„UKRYTE DO WIADOMOSCI”
9. Pole „UDW/„UKRYTE DO WIADOMOŚCI” powinno być wykorzystywane do wysyłania wiadomości z dodatkowym ukryciem przed adresatem faktu istnienia (i tożsamości) trzeciej strony wskazanej w tym polu.
10. Wszelkie wiadomości budzące podejrzenia co do tego, że mogą zawierać szkodliwe oprogramowanie, należy przesyłać do Centrum Informatycznego w formie załącznika na adres postmaster@polsl.pl celem weryfikacji, nie otwierając załączników i nie klikając w linki.
11. Pliki zawierające dane osobowe przed wysłaniem ich do osób trzecich muszą być zabezpieczone hasłem, które powinno być przekazane do odbiorcy innym kanałem łączności (np. telefonicznie/SMS).
12. Zabrania się używania poczty elektronicznej:
    1) do tworzenia, wysyłania lub przechowywania wiadomości e-mail lub załączników, które mogą być uznane za nielegalne lub powszechnie uznane za obraźliwe, nieetyczne lub w inny sposób niestosowne;
    2) do oficjalnego reprezentowania pracodawcy bez odpowiedniego upoważnienia;
    3) do każdego innego niezgodnego z prawem, nieetycznego celu.
13. Zabronione jest uczestniczenie w przechwytywaniu, podglądaniu, zapisywaniu, zmienianiu lub ujawnianiu wiadomości e-mail należącej do innej osoby.
14. W uzasadnionych przypadkach rektor Politechniki Śląskiej może podjąć decyzję o udzieleniu dostępu do skrzynki pocztowej (np. na wniosek odpowiednich służb).

Serwerownie

§ 15

1. Serwerownia powinna być zlokalizowana w pomieszczeniu o dostępie kontrolowanym i ograniczonym wyłącznie do osób upoważnionych.
2. Serwerownia musi być wyposażona w kontrolę wizyjną pomieszczenia.
3. Serwerownia musi znajdować się w pomieszczeniu posiadającym adekwatne zabezpieczenie przed wpływem czynników zewnętrznych (np. zalaniem, wilgocią, włamaniem).
4. Serwerownia powinna zapewniać adekwatne warunki do pracy zainstalowanych urządzeń komputerowych, w szczególności musi:

1) Zapewniać odpowiedni poziom zasilania urządzeń komputerowych w energię elektryczną, z zapewnieniem podtrzymania zasilania i ochrony przeciwprzepięciowej;
2) zapewnić właściwe do poprawnej pracy urządzeń warunki klimatyczne – temperaturę, wilgotność;
3) posiadać drzwi o odpowiedniej klasie odporności przeciwpożarowej, zabezpieczone w sposób, który uniemożliwi dostęp osobom nieuprawnionym.

5. Serwerownia musi posiadać adekwatne zabezpieczenia przeciwpożarowe, w tym system detekcji pożaru.
6. Tworzenie nowej serwerowni odbywa się po konsultacji i za zgodą ASI.
7. Decyzja o lokalizacji nowych systemów centralnych oraz nowych systemów informatycznych posiadających wielu użytkowników jest podejmowana w konsultacji z ASI.

Zarządzanie incydentami

§ 16

1. Użytkownicy systemu informatycznego są zobowiązani do poinformowania administratora danego systemu informatycznego o każdym przypadku niewłaściwego funkcjonowania systemu informatycznego.
2. W przypadku wadliwego działania systemu informatycznego użytkowników obowiązuje całkowity zakaz wykonywania jakichkolwiek napraw.
3. Do diagnozowania usterki lub wadliwego działania systemu informatycznego upoważniony jest tylko administrator właściwy dla danego systemu informatycznego lub inna osoba wskazana przez jego dysponenta.
4. Dysponent lub administrator danego systemu informatycznego może wydać polecenie zabezpieczenia komputera pracownika Uczelni w celu dokonania szczegółowego badania incydentu.
5. Jeżeli na skutek wystąpienia incydentu nastąpiło naruszenie bezpieczeństwa informacji, administrator danego systemu informatycznego sporządza kartę incydentu, która zawiera:
   1) datę i godzinę zdarzenia;
   2) miejsce wystąpienia zdarzenia;
   3) opis zdarzenia;
   4) imię i nazwisko osoby zgłaszającej;
   5) proponowany termin zakończenia wdrożenia działań naprawczych oraz imię i nazwisko osoby odpowiedzianej za ich wdrożenie;
   6) kwalifikację pod względem naruszenia ochrony danych osobowych.
6. Jeżeli incydent skutkował naruszeniem ochrony danych osobowych, administrator danego systemu informatycznego zawiadamia niezwłocznie o tym fakcie inspektora ochrony danych.

Zabezpieczenia sieci

§ 17

1. Sieć Politechniki Śląskiej jest podzielona na sieć szkieletową i sieci lokalne poszczególnych jednostek.
2. Sieci lokalne poszczególnych jednostek są oddzielone od siebie.
3. Sieć Politechniki Śląskiej powinna być wyposażona w centralne urządzenie klasy firewall oraz IDS (Intrusion Detection System).
4. Sieć Politechniki Śląskiej powinna być chroniona systemem anty-DDoS.
5. Systemy informatyczne udostępniające usługi na zewnątrz sieci Politechniki Śląskiej podlegają rejestracji i są monitorowane pod względem ciągłości działania.
6. Dostęp do sieci bezprzewodowej Politechniki Śląskiej powinien być realizowany wyłącznie po uwierzytelnieniu użytkownika.
7. Przyłączenie urządzeń do sieci Politechniki Śląskiej musi następować zgodnie z Regulaminem Sieci Komputerowej Politechniki Śląskiej.
8. Sieć Politechniki Śląskiej i korzystanie z usług sieciowych są monitorowane w celu detekcji zagrożeń i zapewnienia prawidłowego funkcjonowania sieci i poszczególnych systemów. Informacje pochodzące z systemów informatycznych, w tym sieciowych, mogą być poddane dalszej analizie w celu realizacji tego celu.

9. Zaleca się stosowanie mechanizmów odseparowania sieci służącej pracownikom do wykonywania czynności służbowych od innych sieci, w szczególności sieci doświadczalnych, badawczych, gościnnych lub udostępnianych podmiotom zewnętrznym.
10. Dostęp administracyjny do urządzeń sieci szkieletowej Politechniki Śląskiej musi być ograniczony wyłącznie do osób uprawnionych.
11. Urządzenia sieci szkieletowej Politechniki Śląskiej muszą być objęte aktywnym kontraktem serwisowym i/lub własnym magazynem części zapasowych.
12. Urządzenia sieci szkieletowej Politechniki Śląskiej powinny być objęte nadzorem przez automatyczny system nadzoru oraz nadzorem przez całodobowych operatorów (NOC/SOC).

Synchronizacja zegarów systemów informatycznych

§ 18

1. We wszystkich systemach informatycznych Politechniki Śląskiej jest wymagana automatyczna aktualizacja czasu z serwerami czasu dostępnymi w sieci Politechniki Śląskiej.
2. W przypadku urządzeń posiadających zegar, ale nieposiadających możliwości automatycznej synchronizacji, administrator systemu informatycznego jest zobowiązany do regularnej aktualizacji czasu.
3. Za prawidłową konfigurację lub synchronizację czasu w urządzeniu odpowiada administrator urządzenia.

Dzienniki systemów informatycznych

§ 19

Rejestracja błędów jest prowadzona w sposób automatyczny w dzienniku pracy systemu informatycznego. Nadzór nad dziennikiem prowadzi administrator danego systemu informatycznego, który analizuje wszystkie odnotowane w nim zdarzenia mające wpływ na bezpieczeństwo informacji w systemie, w szczególności przerwy w pracy, awarie, incydenty.

Audyty i sprawdzenia

§ 20

Dyrektor Centrum Informatycznego oraz dyrektor Centrum Komputerowego zapewniają minimum raz na rok wykonanie audytu w centralnych systemach informatycznych Politechniki Śląskiej. Powyższy obowiązek wynika z § 20 ust. 2 pkt 14 rozporządzenia 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 (j.t. Dz. U. z 2017 r. poz. 2247).