BIULETYN PRAWNY
UNIWERSYTETU MIKOŁAJA KOPERNIKA W TORUNIU

Rok 2017; poz. 452

ZARZĄDZENIE Nr 196

Rektora Uniwersytetu Mikołaja Kopernika w Toruniu

z dnia 19 grudnia 2017 r.

Polityka bezpieczeństwa sieci komputerowej Uniwersytetu Mikołaja Kopernika w Toruniu

Na podstawie art. 66 ust. 2 ustawy z dnia 27 lipca 2005 r. Prawo o szkolnictwie wyższym (Dz. U. z 2016 r., poz. 1842 z późn. zm.)

z a r z ą d z a s i ę, co następuje**:**

Rozdział 1
Pojęcia ogólne

§ 1

1. W Uniwersytecie Mikołaja Kopernika w Toruniu, zwanym dalej „UMK", funkcjonuje sieć komputerowa.
2. Sieć komputerowa UMK, zwana dalej „SK UMK", obejmuje swoim obszarem wszystkie obiekty UMK, w szczególności lokalizacje w Toruniu, Piwnicach i Bydgoszczy oraz usługi sieciowe udostępniane przez UMK na zasobach własnych lub obcych.
3. Podstawową rolą SK UMK jest wspomaganie procesów dydaktycznych, naukowych i zarządzania UMK.
4. UMK nie ponosi odpowiedzialności z tytułu strat wynikających z awarii SK UMK.
5. SK UMK może być użytkowana w sposób nienaruszający obowiązujących przepisów prawnych.
6. Za pośrednictwem SK UMK nie wolno rozpowszechniać bez zgody rektora lub kanclerza treści lub obrazów o charakterze komercyjnym, reklamowym, politycznym itp.

§ 2

1. Polityka bezpieczeństwa SK UMK, zwana dalej „Polityką", wprowadza jednolite zasady działania użytkowników i administratorów sieci i usług w celu zapewnienia należytej ochrony danych.

2. Polityka składa się z dokumentu zasadniczego wydawanego jako zarządzenie rektora oraz trzech załączników określających szczegółowe procedury działania w następujących obszarach SK UMK:
    1) zarządzanie kontami – załącznik nr 1;
    2) zarządzanie domenami – załącznik nr 2;
    3) usługi zewnętrzne, udostępniane przez konto w SK UMK – załącznik nr 3.
3. Odpowiedzialność za utrzymywanie Polityki, w szczególności za zgłaszanie propozycji aktualizacyjnych wynikających ze zmian prawa i technologii, spoczywa na Uczelnianym Centrum Informatycznym UMK, zwanym dalej „UCI"
4. Polityce towarzyszą dokumenty wewnętrzne, zatwierdzane przez dyrektora UCI, precyzujące szczegółowe zasady działania w ramach podsystemów tworzących SK UMK.
5. Jeżeli w tekście używane jest słowo powinno i jego warianty, to należy je interpretować jako nakaz, od którego mogą występować odstępstwa w szczególnie uzasadnionych sytuacjach. Takie odstępstwa muszą być udokumentowane.

§ 3

1. Dedykowane sieci przeznaczone do dostępu gościnnego, takie jak np. wydzielona dla użytkowników zewnętrznych część sieci eduroam, czy sieć obsługi konferencji, są traktowane jako zasoby zewnętrzne względem SK UMK, a ruch wychodzący z tych sieci i kierowany do pozostałej części UMK jest filtrowany na tych samych zasadach, co ruch spoza UMK.
2. Dedykowane sieci dla dostępu gościnnego muszą posiadać własne regulaminy dostępne co najmniej w językach polskim i angielskim.

§ 4

1. Główną domeną internetową UMK jest umk.pl, co oznacza, że na ogólnych stronach uniwersyteckich oraz stronach jednostek UMK inne strony uniwersyteckie są adresowane wyłącznie poprzez tę domenę.
2. Prawo do wnioskowania o zarejestrowanie nazw w domenie umk.pl mają wyłącznie: rektor, kanclerz, dziekani, kierownicy jednostek ogólnouczelnianych i międzywydziałowych.
3. Każda zarejestrowana nazwa w domenie umk.pl musi mieć wyznaczonego opiekuna.
4. Nazwy w domenie umk.pl rejestruje administrator SK UMK na pisemny wniosek uprawnionej osoby.
5. Okres ważności domen i procedurę ich likwidacji opisuje załącznik nr 2.

Rozdział 2
Użytkownicy SK UMK

§ 5

1. Użytkownikiem SK UMK jest każda osoba korzystająca z urządzenia podłączonego do SK UMK lub z usługi sieciowej SK UMK.
2. W celu dostępu do chronionych zasobów SK UMK niezbędne jest posiadanie konta użytkownika SK UMK, zwanego dalej kontem SK UMK.

3. Konto SK UMK dodatkowo daje uprawnienia korzystania z wybranych usług zewnętrznych, określonych w Regulaminie korzystania z usług zewnętrznych, stanowiącym załącznik nr 3 do niniejszego zarządzenia.
4. W niektórych przypadkach, dostęp do konkretnych usług wymaga specjalnych kont powiązanych z usługami. Takie konto nazywa się kontem w usłudze.

§ 6

1. Konto SK UMK to zarejestrowane uprawnienie do korzystania z SK UMK.
2. Konto SK UMK posiadać mogą:
   1) pracownicy UMK zatrudnieni na podstawie umowy o pracę bądź umowy cywilno-prawnej;
   2) emeryci i renciści UMK;
   3) inne osoby, którym konto jest niezbędne w związku z prowadzonymi na UMK zajęciami dydaktycznymi lub odbywanymi na UMK kursami, praktykami itp.;
   4) studenci UMK (w tym doktoranci);
   5) goście UMK w czasie ich pobytu w uczelni;
   6) posiadacze karty absolwenta UMK;
   7) inne osoby - w szczególnie uzasadnionych przypadkach, za zgodą dyrektora UCI.
3. Na serwerach ogólnouniwersyteckich jedna osoba może posiadać tylko jedno konto SK UMK.
4. Pracownicy, emeryci, renciści i studenci UMK mają prawo do utrzymywania własnej strony WWW, prowadzonej zgodnie z § 1 ust. 6.

§ 7

1. Procedury dotyczące obsługi kont SK UMK są zawarte w załączniku nr 1.
2. Konta SK UMK posiadaczy karty absolwenta UMK są prowadzone na zasadach określonych przez Regulamin Programu Absolwent.
3. Konto SK UMK używane z naruszeniem § 1 ust. 5 jest blokowane przez administratora SK UMK lub administratora odpowiedniej sieci lokalnej. O fakcie zablokowania konta SK UMK powiadamiany jest właściwy przełożony użytkownika, który po wyjaśnieniu sprawy podejmuje decyzję o odblokowaniu konta.
4. Dodatkowe zasady prowadzenia kont UMK użytkowników w sieciach lokalnych SK UMK mogą zostać określone w regulaminach tych sieci.

§ 8

1. Konta SK UMK osób, które utraciły uprawnienia do ich posiadania tracą ważność i są likwidowane po upływie terminu przewidzianego dla danego typu konta.
2. Użytkownika, który utracił status uprawniający do posiadania konta SK UMK, administrator o terminie wyłączenia konta powiadamia za pomocą e-maila.
3. Identyfikator, ani skojarzone z nim aliasy poczty elektronicznej, zlikwidowanego konta SK UMK nie zostaną ponownie przydzielone innej osobie.
4. Terminy i procedurę likwidacji konta SK UMK opisuje załącznik nr 1.

§ 9

1. Konto funkcyjne, to uprawnienie do realizacji zadań lub prowadzenia usług informacyjnych na potrzeby:

1) jednostek organizacyjnych UMK;
2) zarejestrowanych organizacji studenckich i samorządowych działających w UMK;
3) studenckich kół naukowych;
4) innych instytucji i organizacji, udostępniane na mocy odrębnych przepisów lub ustaleń.

2. Konta funkcyjne jednostek organizacyjnych UMK prowadzi się na zlecenie ich kierownika.
3. Konta funkcyjne organizacji studenckich i samorządowych oraz kół studenckich prowadzi się na ich wniosek zaakceptowany przez rektora lub dziekana.
4. Każde konto funkcyjne musi mieć opiekuna wyznaczonego przez osobę właściwą do zakładania takiego konta.
5. Konta funkcyjne mogą być używane tylko zgodnie z celem, na który zostały przyznane.

§ 10

1. Konto w usłudze, to uprawnienie do uzyskania dostępu do usługi, która nie korzysta z systemu kont SK UMK.
2. Usługi mogą definiować własne regulacje dotyczące wymagań odnośnie kont w usłudze, w szczególności dotyczące sposobu logowania do usługi, wymogów odnośnie jakości i częstotliwości zmiany hasła itp.
3. Usługi mogą definiować własne zasady dotyczące terminów ważności kont oraz procedury ich usuwania.

§ 11

1. Adresy poczty elektronicznej w postaci ID@umk.pl lub ID@cm.umk.pl, gdzie ID jest identyfikatorem spełniającym wymogi poczty elektronicznej mogą być przypisane wyłącznie do kont SK UMK pracowników, emerytów i rencistów UMK, osób wymienionych w § 6 ust. 2 pkt 3 oraz kont funkcyjnych.
2. Pracownik UMK używający konta SK UMK na serwerze ogólnouniwersyteckim otrzymuje domyślnie adres poczty elektronicznej ID@umk.pl lub ID@cm.umk.pl, gdzie ID jest identyfikatorem konta; przy zakładaniu konta jest on informowany o możliwości zdefiniowania dodatkowych adresów poczty.
3. Doktoranci korzystający z konta SK UMK na serwerze ogólnouniwersyteckim używają adresów poczty elektronicznej w postaci ID@doktorant.umk.pl, gdzie ID jest identyfikatorem konta doktoranta.
4. Pozostali studenci korzystający z konta SK UMK na ogólnouniwersyteckim serwerze studenckim używają adresów poczty elektronicznej w postaci ID@stud.umk.pl, gdzie ID jest identyfikatorem konta studenta.
5. Goście UMK w czasie pobytu w uczelni korzystając z konta SK UMK na serwerze ogólnouniwersyteckim UMK (zgodnie z niniejszą Polityką) używają adresów poczty elektronicznej w postaci ID@v.umk.pl, gdzie ID jest identyfikatorem konta.
6. Posiadacze karty absolwenta UMK posługują się adresami poczty elektronicznej określonymi przez Regulamin Programu Absolwent.
7. Użytkownicy kont SK UMK na serwerach lokalnych posługują się adresami poczty elektronicznej ustalanymi na podstawie regulacji dotyczących tych serwerów.

§ 12

1. Pracownicy UMK są zobowiązani do korzystania ze służbowych adresów e-mail podczas prowadzenia korespondencji służbowej.

2. Nie zaleca się konfigurowania automatycznego przekierowywania poczty otrzymywanej na adres UMK na serwery spoza UMK. UCI nie ponosi odpowiedzialności za problemy związane z dostarczeniem poczty, jeśli na koncie jest skonfigurowane przekierowanie na serwer spoza UMK.

§ 13

1. W celu ochrony sieci użytkownik SK UMK jest zobowiązany do dbania o bezpieczeństwo swoich kont, w szczególności do ochrony swoich haseł i innych danych służących do uwierzytelnienia.
2. Użytkownik nie może żądać zmiany hasła czy otwarcia zablokowanego dostępu drogą telefoniczną, jeżeli nie ma możliwości identyfikacji dzwoniącego.
3. Zabrania się użytkownikowi SK UMK:
   1) umożliwiania innym osobom korzystania ze swoich kont i związanych z nimi uprawnień;
   2) podejmowania prób wykorzystania obcego konta i uruchamiania aplikacji deszyfrujących hasła;
   3) prowadzenia działań mających na celu podsłuchiwanie lub przechwytywanie informacji przepływającej w sieci;
   4) zmiany przydzielonego adresu IP urządzeń (z wyjątkiem sytuacji uzgodnionych z administratorem odpowiedniej sieci);
   5) uruchamiania aplikacji, które mogą zakłócać lub destabilizować pracę systemu lub sieci komputerowej, bądź naruszyć prywatność zasobów systemowych;
   6) wysyłania masowej poczty kierowanej do losowych odbiorców (spam).
4. W przypadku nieprzestrzegania powyższych zasad przez użytkownika, administrator może czasowo ograniczyć lub zablokować dostęp do sieci lub usługi.

§ 14

1. Zawartość konta użytkownika, w szczególności zawartość skrzynki pocztowej jest chroniona tajemnicą służbową.
2. W uzasadnionych przypadkach na mocy decyzji rektora lub kanclerza zawartość konta może być udostępniona osobom trzecim.

Rozdział 3
Opis SK UMK

§ 15

Składniki SK UMK na terenie Torunia i Piwnic:

1) sieć serwerów usług centralnych UMK administrowana bezpośrednio przez UCI, służąca różnego rodzaju usługom i wymagająca różnego rodzaju dostępu dla użytkowników, podzielona na podobszary zarówno pod względem logicznym jak i geograficznym;
2) wewnętrzna sieć UCI obejmująca stacje robocze pracowników UCI podzielona na obszary dostępu;
3) sieć administracji UMK, administrowana przez Pracownię Komputeryzacji Administracji Uczelni UCI, w większości korzystająca z odrębnych pomieszczeń i oddzielnej infrastruktury kablowej lub wydzielonych kanałów transmisyjnych w ramach sieci TORMAN;

4) sieci lokalne jednostek organizacyjnych UMK z reguły mające odrębność terytorialną i adresową (odrębny routing IP), które mogą być administrowane przez ich jednostki macierzyste lub ich administrowanie może być powierzone UCI, a sieci jednostek organizacyjnych są przyłączane poprzez urządzenia brzegowe sieci TORMAN;
5) sieć bezprzewodowa UMK będąca w zarządzie UCI;
6) sieć domów studenckich i hoteli asystenckich.

§ 16

Składniki SK UMK w Bydgoszczy:
1) sieci lokalne CM UMK administrowane bezpośrednio przez Dział Informatyczny CM, służące różnego rodzaju usługom i wymagające różnego rodzaju dostępu dla użytkowników, podzielone na podobszary zarówno pod względem logicznym jak i geograficznym. Sieci lokalne mogą funkcjonować poprzez urządzenia i infrastrukturę sieci BYDMAN;
2) lokalna Sieć administracji CM UMK, administrowana bezpośrednio przez Dział Informatyczny CM, podłączona do centralnej infrastruktury kablowej;
3) sieci jednostek organizacyjnych z reguły będące częścią lokalnych sieci CM UMK, posiadające w wyjątkowych sytuacjach odrębność adresową, mogą być administrowane przez jednostki macierzyste lub administrowanie może być powierzone Działowi Informatycznemu CM;
4) sieć bezprzewodowa UMK będąca w zarządzie Działu Informatycznego CM;
5) sieć domów studenckich i hoteli asystenckich.

§17

Zarządzanie siecią w lokalizacjach UMK innych niż wymienione w § 15 i 16 zależy od statusu lokalizacji i musi być uregulowane przez właściwe dla danej lokalizacji kierownictwo.

§ 18

Zależność SK UMK od czynników zewnętrznych:
1) SK UMK korzysta z łączy sieci TORMAN, BYDMAN oraz innych łączy telekomunikacyjnych zarówno poprzez wykorzystanie dedykowanych światłowodów, jak i kanałów cyfrowych;
2) niniejsza Polityka nie reguluje spraw sieci TORMAN i traktuje ją jak obiekt zewnętrzny, przedstawia jednak oczekiwania względem dostępności zasobów sieci TORMAN i innych operatorów;
3) w uzasadnionych przypadkach SK UMK może korzystać z usług operatorów komercyjnych.

§ 19

1. Funkcję administratora SK UMK pełni UCI, w imieniu którego działają:
   1) poza Collegium Medicum - kierownik Pracowni Sieci Uczelnianej UCI lub inna osoba upoważniona przez dyrektora UCI;
   2) w Collegium Medicum - kierownik Działu Informatycznego CM lub inna upoważniona przez niego osoba.
2. Kierownik jednostki organizacyjnej posiadającej sieć lokalną powołuje administratora tej sieci i powiadamia o swojej decyzji dyrektora UCI.

3. Za eksploatację sieci lokalnej odpowiedzialny jest jej Administrator współpracujący z Administratorem SK UMK.
4. Administrator sieci lokalnej prowadzi konta SK UMK na komputerach w swojej sieci oraz jest zobowiązany zagwarantować, by zasady zarządzania kontami były zgodne z § 6.
5. Administrator sieci lokalnej jest zobowiązany zagwarantować, by ochrona gniazd sieciowych była realizowana zgodnie z § 41.
6. Administrator sieci lokalnej współpracuje z Administratorem SK UMK w celu zachowania ciągłości, spójności i bezpieczeństwa SK UMK.
7. Siecią domów studenckich i hoteli asystenckich zarządzają administratorzy powołani przez kanclerza w porozumieniu z dyrektorem UCI i współpracujący z kierownikiem Działu Domów Studenckich i Hoteli Asystenckich.

Rozdział 4
Zabezpieczenia fizyczne i odporność na awarie

§ 20

1. SK UMK powinna być realizowana w sposób bezawaryjny zapewniający automatyczne przełączania na systemy zapasowe. Realizacja tej zasady musi uwzględniać bilans kosztów i analizę ryzyka.
2. Pojedyncze punkty awarii, jak również systemy, których przełączenie nie następuje automatycznie muszą być zinwentaryzowane, a sposób reakcji na ich awarię musi być przygotowany i odpowiednio udokumentowany.
3. Główne punkty SK UMK, w szczególności lokalizacje, w których umieszczono serwery, muszą być połączone więcej niż jedną trasą światłowodową, tak by zapewnić ciągłość pracy systemu w przypadku awarii jednej z tras światłowodowych.

§ 21

1. Usługi centralne realizuje się z zapewnieniem zasad bezawaryjności z uwzględnieniem rozproszenia danych pod względem zarówno logicznym, jak i geograficznym.
2. Realizacja usług uwzględnia ich płynne przeniesienie na inny serwer w trybie automatycznym bądź wymagającym ingerencji administratora. Wybór metody zabezpieczeń, określenie maksymalnego dopuszczalnego czasu awarii zależy od krytyczności usługi i jest opisany w dokumencie wewnętrznym [redundancja serwerów].

§ 22

1. Serwery, macierze przechowujące dane, przełączniki sieci serwerów, umieszcza się w kilku niezależnych lokalizacjach zwanych dalej serwerowniami, zapewniając możliwość migrowania zasobów.
2. Serwerownie są zamykane, klimatyzowane i umieszczone w budynkach objętych dozorem portierów bądź elektronicznym. Dostęp do pomieszczeń jest ograniczony do grupy upoważnionych administratorów. Zaleca się, aby serwerownie były wyposażone w zamki elektroniczne połączone z rejestratorem wejść.
3. Osoby sprzątające serwerownie muszą mieć upoważnienie oraz zostać przeszkolone; upoważnienie i fakt przeszkolenia muszą być udokumentowane.
4. Remonty i naprawy prowadzone w serwerowniach są wstępnie uzgadniane z administratorami i odbywają się pod ich nadzorem.

5. Serwerownie powinny być objęte monitoringiem przy pomocy kamer rejestrujących co najmniej moment wejścia do pomieszczenia.
6. Serwery, macierze i przełączniki są dołączone do sieci energetycznej zabezpieczonej urządzeniami typu UPS i w miarę możliwości również generatorami energii elektrycznej.
7. Serwery wirtualizacyjne, macierze i przełączniki realizujące klaster serwerów lokuje się tak, by każdy element posiadał zapasowy składnik umieszczony w serwerowni zasilanej z awaryjnego generatora energii elektrycznej.
8. Kluczowe urządzenia są wyposażone w zwielokrotnione zasilanie podłączone do oddzielnych obwodów.
9. Klimatyzacja serwerowni musi zapewniać utrzymanie temperatury umożliwiającej pracę urządzeń przez okres co najmniej 4 godzin również przy braku zasilania zewnętrznego.
10. Urządzenia UPS i generatory awaryjne podlegają procedurze testów sprawności opisanej w dokumencie wewnętrznym [serwerownie].
11. Dokument wewnętrzny [serwerownie] zawiera listę serwerowni wraz z opisem ich zabezpieczeń.

Rozdział 5
Ochrona danych i usług

§ 23

Jednostką odpowiedzialną za funkcjonowanie podstawowych usług sieciowych i koordynującą działania dotyczące udostępniania usług sieciowych w SK UMK jest UCI, a w przypadku usług prowadzonych lokalnie w Collegium Medicum - Dział Informatyczny CM.

§ 24

1. Serwery usług (fizyczne lub wirtualne) umieszcza się w rozdzielnych sieciach wirtualnych w zależności od realizowanych przez nie funkcji oraz sposobu dostępu użytkowników. W szczególności serwery, na które użytkownicy mogą się logować, uruchamiać własne programy, strony internetowe i usługi, są umieszczane w sieci wydzielonej. Lista wydzielonych podsieci oraz rozdział serwerów usług opisuje dokument wewnętrzny [podsieci serwerów].
2. Dostęp do sieci serwerów usług centralnych oraz serwerów administracji jest chroniony systemami firewall. Zasady dostępu do konfiguracji firewalla, dokumentacji wprowadzanych zmian oraz redundancji firewalla są opisane w dokumencie wewnętrznym [firewall].
3. Dostęp do serwerów wirtualnych jest chroniony systemem haseł zgodnie z zasadami opisanymi w rozdziale 9 niniejszego dokumentu.

§ 25

1. Odpowiedzialność za realizację prawidłowej ochrony danych przechowywanych na serwerach ponoszą wyznaczeni administratorzy.
2. Dane przechowywane na serwerach muszą być chronione w sposób dostosowany do konkretnych potrzeb.
3. Istotne dane powinny być chronione przed ich utratą, nieupoważnioną modyfikacją oraz przypadkowym skasowaniem.

4. Jeżeli na podstawie specyfiki udostępnianego zasobu czy usługi, albo charakteru przechowywanych danych, zasadne jest zastosowanie niższego poziomu ochrony, niż ten o którym mowa w ust. 3, użytkowników tych zasobów i usług informuje się o poziomie ryzyka.
5. W przypadku utrzymywania kilku kopii danych należy zapewnić przechowywanie ich w różnych lokalizacjach.
6. Szczegółowe zasady utrzymywania kopii zapasowych zależą od konkretnych systemów i są opisane w dokumencie wewnętrznym [zasady tworzenia kopii zapasowych].
7. Każdy system kopii zapasowych musi być wyposażony w opis działania i opis procedury odzyskiwania danych. Opis procedury odzyskiwania danych musi być łatwo dostępny również w przypadku szerokiej awarii systemu informatycznego.

§ 26

1. W logach systemowych zbierane są informacje na temat działania systemu oraz na temat aktywności użytkowników.
2. Logi systemowe dotyczące kluczowych elementów bezpieczeństwa systemu są automatycznie tworzone na centralnym systemie logów, tak by w przypadku włamania uniemożliwić zatarcie śladów włamania.
3. Logi systemowe traktuje się jak dokumenty objęte tajemnicą służbową.
4. Czas i sposób przechowywania logów zależy od ich rodzaju i jest opisany szczegółowo w dokumencie wewnętrznym [instrukcja przechowywania logów systemowych], przy czym podlega następującym zasadom ogólnym:
   1) logi zawierające informacje o aktywności użytkowników są przechowywane nie dłużej niż jeden rok i po tym czasie są automatycznie kasowane;
   2) dozwolone jest dłuższe przechowywanie wyciągów z logów systemowych tworzonych dla celów statystycznych, wyciągi te nie powinny zawierać informacji pozwalających na identyfikację działań użytkownika;
   3) poszczególne usługi informatyczne mogą w uzasadnionych przypadkach przechowywać własne logi przez czas dłuższy, informacja ta zostaje umieszczona w polityce prywatności publikowanej przez daną usługę.

§ 27

1. Serwery fizyczne, macierze, urządzenia sieciowe, serwery wirtualne i usługi centralne są monitorowane przez specjalizowane oprogramowanie.
2. W przypadku stwierdzenia awarii usługi, system monitorujący podejmuje próbę automatycznego restartu usługi.
3. Informacje o krytycznych awariach są wysyłane pocztą e-mail oraz przy pomocy dodatkowego kanału komunikacyjnego, np. komunikatów SMS, do całej grupy administratorów odpowiedzialnych za dany obszar działania.
4. Monitorowanie dostępności serwerów i usług powinno być realizowane przez co najmniej dwa serwery umieszczone w różnych lokalizacjach, a dodatkowy kanał komunikacyjny, o którym mowa w ust. 3, powinien umożliwić przesłanie komunikatu bez udziału SK UMK, tak by uniezależnić system komunikatów od awarii składników SK UMK.

§ 28

1. Serwery usług muszą być aktualizowane poprzez instalowanie bieżących poprawek bezpieczeństwa.

2. W przypadku otrzymania informacji o pojawieniu się zagrożenia UCI rozsyła informacje do odpowiedniej grupy odbiorców, nie zwalnia to jednak administratorów podsieci SK UMK od odpowiedzialności za bezpieczeństwo administrowanych przez nich sieci.
3. Szczególną uwagę przykłada się do zagrożeń mających wpływ na bezpieczną komunikację pomiędzy użytkownikami a serwerami, zadaniem administratorów jest utrzymanie odpowiedniego poziomu bezpieczeństwa, nawet jeżeli oznacza to ograniczenie dostępu z niektórych urządzeń użytkowników.

§ 29

Administratorzy mają prawo limitowania wielkości udostępnianych zasobów serwera, a w uzasadnionych przypadkach mogą ograniczyć dostęp do usług sieciowych, operacji typu uruchomienie programu, odczytu/zapisu plików lub połączenia z innym systemem.

§ 30

1. Usługi dostępne przez sieć uruchamiane na serwerach SK UMK muszą korzystać z bezpiecznego oprogramowania.
2. W przypadku, gdy zamawiane jest wykonanie oprogramowania realizującego usługi dostępne przez sieć, na przykład wykonanie serwisu WWW, dysponent środków musi zagwarantować, że będzie rezerwował środki niezbędne do zapewnienia wsparcia na oprogramowanie, przez cały okres jego eksploatacji.

§ 31

1. W przypadku stwierdzenia, że do serwera usług uzyskały dostęp nieupoważnione osoby, administratorzy podejmują odpowiednie kroki naprawcze.
2. Wszelkie przypadki naruszenia zasad dostępu są rejestrowane.
3. Jeżeli nieuprawniony dostęp dotyczy konta użytkownika, administratorzy blokują konto i w miarę możliwości powiadamiają o tym użytkownika.
4. Jeżeli nieuprawniony dostęp dotyczy poziomu zarządzania serwerem, to administrator serwera powinien dokonać sprawdzenia logów oraz przeprowadzić audyt oprogramowania systemowego, a następnie podjąć działania w celu zlikwidowania przyczyny tego incydentu.

§ 32

1. We wszystkich przypadkach, gdy z dostępem do serwera wiążą się elementy bezpieczeństwa, takie jak przekazywanie danych logowania, obsługa dokumentów, czy przetwarzanie danych osobowych, połączenie między serwerem a stacją roboczą musi się odbywać przez kanał szyfrowany.
2. Serwer udostępniający bezpieczną usługę wymusza korzystanie z kanału szyfrowanego, a parametry szyfrowania muszą być zgodne z aktualnymi zaleceniami bezpieczeństwa.
3. W przypadku przetwarzania danych osobowych niezbędne jest zapewnienie ochrony opisanej w Instrukcji Bezpieczeństwa danego systemu przetwarzania danych osobowych.

§ 33

1. Wszyscy administratorzy systemów informatycznych są zobowiązani do zachowania tajemnicy służbowej. Obowiązek zachowania tajemnicy pozostaje w mocy również po ustaniu zatrudnienia na UMK.
2. Tajemnicą służbową objęte są w szczególności:
   1) informacje na temat konfiguracji sieci i systemów informatycznych UMK;
   2) hasła i inne dane dostępowe;
   3) wszelkie dane osobowe;
   4) zawartość katalogów domowych i korespondencja użytkowników;
   5) dane administracji;
   6) logi systemowe zawierające informacje na temat aktywności użytkowników.
3. Udostępnienie danych objętych tajemnicą służbową jest możliwe wyłącznie na pisemny wniosek i musi być poprzedzone uzyskaniem zgody rektora, kanclerza lub upoważnionych przez nich osób.

Rozdział 6
Usługi informacyjne

§ 34

1. UCI utrzymuje uniwersytecki serwer nazw (DNS) na potrzeby SK UMK. Udostępnienie serwera nazw w lokalnej sieci odbywa się w porozumieniu z administratorem SK UMK.
2. Obsługa poddomen UMK na serwerach znajdujących się poza SK UMK może mieć miejsce jedynie w szczególnie uzasadnionych przypadkach i wymaga zgody rektora.

§ 35

1. UCI utrzymuje uniwersytecki serwer poczty elektronicznej, odpowiada za jego prawidłową konfigurację i ciągłą dostępność.
2. Usługi sieciowe uruchomione pod nazwami zarejestrowanymi w domenie umk.pl działają na serwerach SK UMK, Rejestracja domeny nie może służyć wyłącznie przekierowaniu usługi na serwer poza UMK bądź osadzeniu treści pobieranej z serwera zewnętrznego.
3. Sieci lokalne SK UMK mogą dysponować własnymi serwerami poczty elektronicznej bądź korzystać z serwera uniwersyteckiego. Administrator SK UMK ma prawo podjąć decyzję o zablokowaniu dostępu do serwisu poczty elektronicznej w sieci lokalnej po stwierdzeniu niepoprawnego funkcjonowania tej usługi.

§ 36

1. Zadaniem serwerów obsługujących pocztę elektroniczną jest dostarczanie przesyłek z jednoczesną ochroną użytkowników przed spamem i przesyłkami zawierającymi niepożądane oprogramowanie.
2. Przesyłki rozpoznane jako podejrzane, ale nie zakwalifikowane jako ewidentny spam, muszą być odpowiednio oznakowane, tak by użytkownik mógł zdefiniować własne reguły postępowania.
3. Użytkownicy są zobowiązani do stosowania zasady ograniczonego zaufania, a w szczególności do nie podejmowania działań takich jak podanie własnego hasła, czy zmiana hasła w odpowiedzi na otrzymany list.

4. Z uwagi na zagrożenia polegające na rozsyłaniu spamu z SK UMK i związanych z tym konsekwencji, poczta elektroniczna może być wysyłana wyłącznie za pośrednictwem odpowiednio zabezpieczonych serwerów.
5. Poczta elektroniczna wysyłana z SK UMK musi być skanowana pod kątem spamu i zawierania niepożądanego oprogramowania; przesyłki rozpoznane jako groźne muszą być blokowane, a użytkownik, z którego konta wysłano taką korespondencję musi zostać powiadomiony.
6. Zabrania się stosowania formularzy internetowych pozwalających na wysyłanie poczty do dowolnych odbiorców.

§ 37

1. Wysyłanie poczty do ogółu pracowników lub studentów wymaga zgody rektora, prorektora, kanclerza, lub upoważnionej przez nich osoby.
2. Zgody na wysyłanie takiej poczty udziela się jednorazowo lub na stałe.
3. Użytkownikowi posiadającemu taką zgodę UCI udostępnia adres pozwalający na zrealizowanie wysyłki.

§ 38

1. UCI utrzymuje uniwersytecki serwer WWW, odpowiada za jego prawidłową konfigurację i ciągłą dostępność.
2. Sieci lokalne SK UMK mogą dysponować własnymi serwerami WWW bądź korzystać z serwera uniwersyteckiego. Administrator SK UMK ma prawo podjąć decyzję o zablokowaniu dostępu do serwisu WWW w sieci lokalnej po stwierdzeniu niepoprawnego funkcjonowania tej usługi.

§ 39

1. Administrator serwera WWW określa warunki techniczne utrzymywania stron WWW użytkowników.
2. Strony WWW użytkowników służą do celów edukacyjnych i naukowych, a w przypadku jednostek organizacyjnych i organizacji – do celów zgodnych z ich działalnością statutową.
3. Użytkownik jest odpowiedzialny za treści umieszczane na jego stronie WWW. W szczególności stosuje się § 1 ust. 5.

Rozdział 7
Zarządzanie warstwą sieciową

§ 40

1. Poszczególne budynki UMK są okablowane na potrzeby połączeń SK UMK.
2. Połączenia między budynkami, w zależności od sytuacji mogą być realizowane przy pomocy tras i urządzeń sieci TORMAN i sieci zewnętrznych operatorów telekomunikacyjnych.
3. Monitoring sieci TORMAN obejmuje zarówno urządzenia samej sieci TORMAN, jak i wybrane urządzenia sieci lokalnej.

4. Punkty koncentracji sieci w budynkach powinny być zlokalizowane w zamykanych, klimatyzowanych pomieszczeniach, a w przypadku braku takiej możliwości urządzenia muszą być montowane w szafkach zamykanych na klucz. Dostęp do kluczy musi być ograniczony i rejestrowany.
5. Sieci budynków są obsługiwane przez zarządzalne przełączniki umożliwiające monitoring, jak i kontrolę dostępu do poszczególnych gniazd.
6. Połącznia między gniazdami przełączników, a końcowymi gniazdami sieci muszą być udokumentowane.
7. W przypadku realizowania inwestycji budowlanych, których zasięg obejmuje modernizację lub budowę okablowania w budynku, niezbędnym elementem odbioru inwestycji jest protokół odbioru okablowania sieci strukturalnej stwierdzający zgodność wykonania okablowania z zakładanymi normami oraz odbiór pełnej dokumentacji powykonawczej sieci strukturalnej.

§ 41

1. Dołączanie urządzeń do sieci przewodowej będącej częścią SK UMK podlega ochronie.
2. Gniazda sieciowe w obszarach ogólnodostępnych są skonfigurowane w sposób pozwalający na identyfikację użytkownika korzystającego z takiego gniazda.
3. Minimalnym wymaganiem ochrony w pomieszczeniach z ograniczonym dostępem jest kontrola adresów przydzielanych przez serwer DHCP oraz monitoring sieci pod względem pojawiania się w niej nieznanych urządzeń.

§ 42

1. UMK utrzymuje centralną sieć bezprzewodową połączoną z ogólnoświatowym systemem eduroam.
2. Dostęp do sieci eduroam wymaga posiadania aktywnego konta SK UMK upoważniającego do korzystania sieci lub konta w innej instytucji włączonej w system eduroam.
3. Konta SK UMK pracowników i studentów UMK upoważniają do dostępu do sieci eduroam na całym świecie.
4. Konta SK UMK absolwentów UMK uprawniają do dostępu do eduroam wyłącznie na terenie UMK.
5. Urządzenia osób mających konta eduroam poza UMK oraz posiadaczy konta absolwenta UMK są umieszczane w wirtualnej podsieci, która jest traktowana jako sieć zewnętrzna w stosunku do UMK. W sieci tej nie działa automatyczny dostęp do czasopism elektronicznych subskrybowanych przez UMK.
6. Sieć eduroam służy dostępowi do sieci na terenie UMK i nie może być używana w celu tworzenia stałych połączeń sieciowych poprzez np. anteny kierunkowe i wzmacniacze sygnału.
7. W sytuacjach rodzących podejrzenie, że konto użytkownika jest nadużywane, np. z jednego konta korzysta duża liczba urządzeń, lub sposób korzystania wskazuje na zestawienie stałego łącza, administratorzy mogą zablokować uprawnienie korzystania z sieci przez użytkownika.

§ 43

1. Wewnątrz SK UMK zabrania się uruchamiania niezabezpieczonych sieci bezprzewodowych.

2. Urządzenia dostępowe łączności bezprzewodowej mogą być podłączane do SK UMK wyłącznie w porozumieniu z administratorem SK UMK lub osobą upoważnioną przez administratora SK UMK do podejmowania takich decyzji na określonym terenie; podłączanie urządzeń bez porozumienia będzie traktowane jako poważne naruszenie bezpieczeństwa SK UMK.
3. W uzasadnionych przypadkach administratorzy SK UMK mogą stosować metody zagłuszania nieznanych urządzeń bezprzewodowych.
4. Urządzenia korzystające z sieci bezprzewodowej nie mogą zakłócać pracy innych użytkowników sieci, a użytkownicy takich urządzeń są zobowiązani do przestrzegania zaleceń administratora SK UMK.

Rozdział 8
Urządzenia użytkowników

§ 44

1. Stacje robocze będące własnością UMK, powinny być chronione aktualizowanym na bieżąco oprogramowaniem zapewniającym bezpieczeństwo systemu komputerowego. UMK zapewnia niezbędne licencje na oprogramowanie ochronne, zgodnie z zasadami finansowymi ustalanymi przez rektora.
2. W przypadku przetwarzania danych osobowych niezbędne jest zapewnienie ochrony opisanej w Instrukcji Bezpieczeństwa danego systemu przetwarzania danych osobowych.
3. Opisy ochrony różnych systemów operacyjnych są na bieżąco aktualizowane i dostępne na stronach UCI.
4. Za bezpieczeństwo oprogramowania stacji roboczej odpowiedzialny jest Administrator Oprogramowania przydzielony do danej stacji.

§ 45

W SK UMK mogą być podłączane prywatne urządzenia użytkowników, przy zachowaniu następujących zasad:

1) użytkownik korzystający z urządzenia prywatnego ponosi odpowiedzialność za zagrożenia, które mogą wyniknąć z braku należytej ochrony jego urządzenia;
2) użytkownik jest zobowiązany do właściwej ochrony własnego urządzenia, tak by wykluczyć niepowołany dostęp do usług np. za pomocą haseł zachowanych na urządzeniu;
3) w przypadku, gdy zachodzi podejrzenie, że urządzenie dostało się w niepowołane ręce, użytkownik jest zobowiązany do niezwłocznej zmiany wszystkich haseł dostępowych w systemach UMK;
4) instrukcje bezpieczeństwa konkretnych usług mogą wprowadzać dodatkowe ograniczenia na dostęp z urządzeń prywatnych.

§ 46

1. W przypadku stwierdzenia, że w SK UMK pracuje urządzenie zakłócające działanie sieci, bądź naruszające zasady niniejszej Polityki, właściwy administrator sieci ma prawo do natychmiastowego wyłączenia dostępu takiego urządzenia do sieci.

2. O stwierdzonych przypadkach naruszenia Polityki administrator powiadamia użytkownika urządzenia, a w uzasadnionych przypadkach lub przy braku reakcji użytkownika, również właściwego zwierzchnika użytkownika.
3. Wszelkie przypadki stwierdzonych naruszeń niniejszej Polityki są rejestrowane przez administratorów.

Rozdział 9
Polityka haseł dostępowych

§ 47

Administratorzy usług centralnych w celu dostępu do serwerów korzystają z uwierzytelniania dwuetapowego na serwerze dostępowym. Drugim elementem uwierzytelniania jest losowa liczba wygenerowana na zewnętrznym urządzeniu.

§ 48

1. Użytkownicy są zobowiązani do zachowania danych dostępowych w tajemnicy. W szczególności niedozwolone jest przekazywanie komukolwiek hasła dostępowego do konta indywidualnego.
2. Hasła muszą spełniać wymogi bezpieczeństwa wymuszane poprzez systemy zmiany haseł.
3. W systemach, w których przetwarzane są dane osobowe stosowane są hasła specyficzne dla tych systemów i wymuszana jest zmiana haseł użytkowników nie rzadziej niż raz na miesiąc, chyba że stosowane są dodatkowe mechanizmy zabezpieczające np. tokeny, czy listy haseł jednorazowych.
4. Dopuszczalne jest stosowanie w systemach UMK ustawienie nowego hasła przez usługę SMS, przy czym polityka zarządzania konkretnego systemu musi regulować zasady weryfikacji numerów telefonów powiązanych z kontami.

Rozdział 10
Zmiana użytkownika sprzętu oraz utylizacja sprzętu elektronicznego i nośników mogących zawierać dane

§ 49

Użytkownik sprzętu elektronicznego przekazywanego innemu użytkownikowi, a mogącego zawierać dane wymagające ochrony jest zobowiązany do dokonania oceny ryzyka związanego z ewentualnym udostępnieniem danych. Jeżeli jest to niezbędne, kasuje dane w sposób nie pozwalający na ich odzyskanie. W przypadku wątpliwości użytkownik kontaktuje się w tej sprawie z właściwym administratorem sieci.

§ 50

1. Sprzęt elektroniczny podlega ogólnym zasadom utylizacji przyjętym na UMK.
2. Odbiór i utylizacja sprzętu, który może zawierać dane wymagające ochrony, na przykład takiego, na którym przetwarzano dane osobowe, można powierzyć wyłącznie podmiotom posiadających odpowiednie uprawnienia potwierdzone stosownym certyfikatem.

3. Przeznaczony do utylizacji sprzęt, który może zawierać dane wymagające ochrony musi być odpowiednio oznakowany na obudowie, tak by możliwe było właściwe przekazanie go podmiotowi utylizującemu.

§ 51

Jeżeli nośniki danych zawierające dane wymagające ochrony nie zostały poddane procedurze likwidacji danych, to można je powierzyć w celu utylizacji wyłącznie podmiotom posiadającym odpowiednią certyfikację.

§ 52

Jeśli sprzęt zawierający nośniki danych z danymi wymagającymi ochrony podlega naprawie gwarancyjnej, to musi być spełniony jeden z poniższych warunków:
1) dane na nośniku są przechowywanie w formie zaszyfrowanej;
2) nośnik danych nie może zostać przekazany firmie realizującej naprawę, dopuszczalna jest jedynie wymiana nośnika z pozostawieniem oryginalnego nośnika u właściciela.

Rozdział 11
Przepisy końcowe

§ 53

1. Tracą moc:
   1) zarządzenie Nr 144 Rektora UMK z dnia 19 października 2009 r. w sprawie korzystania w celach służbowych z adresów służbowych e-mail przez pracowników UMK (Biuletyn Prawny UMK Nr 9, poz. 283);
   2) zarządzenie Nr 76 Rektora UMK z dnia 18 września 2007 r. – Regulamin Sieci Komputerowej Uniwersytetu Mikołaja Kopernika w Toruniu (Biuletyn Prawny UMK Nr 7, poz. 178).
2. Zarządzenie wchodzi w życie z dniem 19 grudnia 2017 r., z wyjątkiem § 20 - § 22 oraz § 24 - § 26, które wchodzą w życie z dniem 1 lipca 2018 r.

R E K T O R

prof. dr hab. Andrzej Tretyn