Zarządzenie Nr ...76.../2020
z dnia ...13.05.2020 r.
Rektora
Śląskiego Uniwersytetu Medycznego w Katowicach

w sprawie: wprowadzenia „*Instrukcji Bezpieczeństwa Pracy Zdalnej i Urządzeń Mobilnych w Śląskim Uniwersytecie Medycznym w Katowicach*"

Na podstawie § 29 ust. 3 Statutu Śląskiego Uniwersytetu Medycznego w Katowicach (Uchwała Senatu SUM z dnia 29.05.2019 r), § 20 ust. 1 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 (t.j. Dz.U. z 2017 r. poz. 2247),* art. 32 Rozporządzenia 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)zarządzam, co następuje:

§ 1

Wprowadzam „*Instrukcję Bezpieczeństwa Pracy Zdalnej i Urządzeń Mobilnych w Śląskim Uniwersytecie Medycznym w Katowicach*", w brzmieniu stanowiącym Załącznik Nr 1 do niniejszego Zarządzenia.

§ 2

Traci moc obowiązywania Zarządzenie nr 202/2016 z dnia 16.12.2016 r.

§ 3

Treść niniejszego zarządzenia wraz z załącznikami polecam zamieścić na stronie internetowej Uczelni.

§ 4

Zarządzenie wchodzi w życie z dniem podpisania.

REKTOR
Śląskiego Uniwersytetu Medycznego w Katowicach
prof. dr hab. n. med. Przemysław Jałowiecki

Otrzymują:
- Prorektorzy,
- Dziekani Wydziałów,
- Zastępcy Kanclerza,
- Dyrektor Szkoły Doktorskiej,
- Dyrektor Biblioteki SUM,
- Dyrektor ds. Technicznych
- Dyrektor ds. Administracyjno - Gospodarczych
- Kierownicy wszystkich jednostek organizacyjnych SUM
- a/a.

Załącznik Nr 1
do Zarządzenia Nr 76/2020
z dnia 13.05.2020 r.
Rektora SUM

Instrukcja Bezpieczeństwa Pracy Zdalnej i Urządzeń Mobilnych w Śląskim Uniwersytecie Medycznym w Katowicach

1 Wstęp

Treść niniejszej instrukcji określa ogólne zasady bezpieczeństwa informacji przetwarzanych podczas świadczenia pracy zdalnej, w tym w szczególności przy użyciu urządzeń mobilnych (smartfony, tablety, smartwatche) w Śląskim Uniwersytecie Medycznym w Katowicach.

Stosując niniejszą instrukcję należy zapewnić należyte bezpieczeństwo informacji, przez które rozumie się zapewnienie:

- **Poufności informacji** - właściwość zapewniającą, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom fizycznym.
- **Integralności informacji** - właściwość polegającą na tym, że zasób systemu teleinformatycznego nie został zmodyfikowany w sposób nieuprawniony.
- **Dostępności informacji** - właściwość określającą, że zasób systemu teleinformatycznego jest możliwy do wykorzystania na żądanie, w założonym czasie, przez podmiot uprawniony do pracy w systemie teleinformatycznym,
- **Rozliczalności informacji** - właściwość polegająca na przechowywaniu pełnej historii dostępu do danych.

Podstawa prawna

- Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz.U. z 2020 r. poz. 346 z późn. zm.)
- § 20 ust. 2 pkt. 11 Rozporządzenie 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 (tj. Dz.U. z 2017 r. poz. 2247 113 z późn. zm.)
- Art. 32 Rozporządzenia 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), zwane dalej **RODO**.

Podstawa normatywna w oparciu o standardy międzynarodowe

- Norma ISO/EIC 27001

Niniejsza Instrukcja jest integralnym elementem Systemu Zarządzania Bezpieczeństwem Informacji w SUM, podlega przeglądowi i aktualizacji na zasadach określonych w Regulaminie Organizacyjnym w SUM.

2 Zakres odpowiedzialności

Pracownik SUM wykonujący pracę zdalną lub pracownik podmiotu, któremu na podstawie umowy udzielono zdalnego dostępu do wybranych zasobów SUM, odpowiada za:

1. Bezpieczeństwo informacji przetwarzanych w zakresie pracy zdalnej i/lub użytkowania służbowego urządzenia mobilnego,
2. Bezpieczne przetwarzanie danych w systemach chmurowych, do których uzyskał dostęp w ramach zadań pracowniczych,
3. Stosowanie zasad określonych w niniejszej Instrukcji oraz *Polityce Bezpieczeństwa Informacji SUM*,
4. Korzystanie z udostępnionych zasobów lub systemów informatycznych zgodnie z ich instrukcją obsługi, powszechnie obowiązującym prawem, regulacjami wewnętrznymi SUM oraz wyłącznie w określonym celu i zakresie przetwarzania udostępnionych zasobów,
5. Użytkowanie urządzeń im powierzonych w sposób nienaruszający praw i dobrego imienia Śląskiego Uniwersytetu Medycznego w Katowicach,
6. Zgłaszania wszelkich nieprawidłowości w działaniu systemu informatycznego lub dostrzeżonych podatności do Centrum Informatyki i Informatyzacji SUM,
7. Zgłaszanie incydentów i naruszeń bezpieczeństwa do Działu ds. Bezpieczeństwa Informacji zgodnie z obowiązującą w Uczelni procedurą.

Kierownik jednostki organizacyjnej SUM, której pracownik świadczy pracę zdalną, odpowiada za:

1. Zezwalanie podległym pracownikom na wykonywanie pracy zdalnej na zasadach określonych w wewnętrznych aktach prawnych z zachowaniem zasad bezpieczeństwa informacji adekwatnie do wykonywanych przez nich obowiązków,
2. Nadzorowanie bezpieczeństwa informacji w zakresie powierzonej pracy zdalnej.
3. Decydowanie o formie i zakresie kształcenia na odległość,
4. Nadzorowanie aktualności uprawnień i upoważnień podległych pracowników wykonujących pracę zdalną, w szczególności upoważnień do przetwarzania danych osobowych i uprawnień w zakresie elektronicznej poczty służbowej.

Centrum Informatyki i Informatyzacji (ICI) odpowiada za:

1. Utrzymywanie i aktualizację mechanizmów zdalnego dostępu,
2. Nadawanie uprawnień do zdalnego dostępu oraz ograniczenie ich do niezbędnego minimum,
3. Nadawanie uprawnień do systemów chmurowych dopuszczonych do użytkowania w SUM,
4. W przypadku dostępu do serwerów SUM przez podmioty zewnętrzne ICI odpowiada za wyznaczenie administratorów do nadzoru prowadzonych zdalnie czynności i weryfikacji bezpieczeństwa systemu po ich zakończeniu,

5. W przypadku zwrotu urządzenia służbowego będącego własnością Uczelni przeznaczonego do pracy zdalnej, pracownik ICI weryfikuje stan bezpieczeństwa urządzenia, zabezpiecza zapisane na nim dane (przekazując do właściwego kierownika jednostki organizacyjnej SUM) oraz dokonuje kasowania danych za pomocą oprogramowania do bezpiecznego i skutecznego kasowania danych,
6. Instalację oprogramowania antywirusowego w służbowym urządzeniu mobilnym przed jego wydaniem pracownikowi,
7. Współpracę z Działem ds. Bezpieczeństwa Informacji w każdym przypadku dotyczącym bezpieczeństwa informacji przetwarzanych w zakresie pracy zdalnej i systemów informatycznych umożliwiających jej świadczenie,
   Współpracę z Działem Technicznym w przypadku incydentów związanych z bezpieczeństwem informacji w zakresie urządzeń mobilnych.

Dział realizujący lub tworzący umowę, która uwzględnia możliwość zdalnego dostępu do zasobów SUM zobowiązany jest:

1. Uwzględnić w umowach zapisy gwarantujące poufność, dostępność i integralność danych, a w przypadku przetwarzania danych osobowych uwzględnić zapisy dot. powierzenia przetwarzania danych osobowych na zasadach określonych w art. 28 RODO (powierzenie przetwarzania danych osobowych),
2. Każda umowa lub wzorzec umowy uwzględniająca dostęp zewnętrzny do zasobów informacyjnych Uczelni winna zostać zaopiniowana przez Dział ds. Bezpieczeństwa Informacji oraz Centrum Informatyki i Informatyzacji SUM.

Dział Techniczny odpowiada za:

1. Zamawianie nowych telefonów lub smartfonów zgodnie z obowiązującymi procedurami i przepisami wraz z zainstalowanym oprogramowaniem antywirusowym aktualizowanym przez cały okres trwania umowy,
2. Poinstruowanie użytkownika telefonu o konieczności ustawienia blokady ekranu,
3. Współpracę z Centrum Informatyki i Informatyzacji SUM i Działem ds. Bezpieczeństwa Informacji w przypadku incydentów związanych z bezpieczeństwem informacji w zakresie urządzeń mobilnych.

Wybrane jednostki organizacyjne, w szczególności: Ośrodek Egzaminów i Ewaluacji Jakości Kształcenia, Centrum Dydaktyki i Symulacji Medycznej, Centrum Symulacji Medycznej w Zabrzu, Centrum Informatyki i Informatyzacji SUM odpowiadają za nadzór nad urządzeniami mobilnymi służącymi do przeprowadzania testów zgodnie z przyjętym Regulaminem.

Dział Administracyjno-Gospodarczy w Katowicach odpowiada za przygotowanie umów z użytkownikami aparatów telefonicznych.

3 Główne zasady bezpieczeństwa informacji przy wykonywaniu pracy zdalnej

Niniejszy rozdział reguluje zagadnienia związane ze zdalnym wykonywaniem pracy w tym łączeniem się do zasobów SUM z poza sieci Uczelni.

1. Zabrania się przetwarzania informacji, o których mowa w ustawie z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych na zasadach zdalnej pracy.
2. Każdy pracownik pracujący zdalnie powinien posiadać konto e-mail służbowe oraz upoważnienie do przetwarzania danych osobowych oraz uczestniczyć w szkoleniu z zakresu bezpieczeństwa informacji i ochrony danych osobowych.
3. Przy wykonywaniu pracy zdalnej obowiązują odpowiednio zapisy *Polityki Bezpieczeństwa Informacji w SUM* oraz powiązanych z nią *Regulaminu Użytkownika Systemów Informatycznych* w SUM oraz *Instrukcji Zarządzania Systemami Informatycznymi w SUM.*
4. Dane służbowe bez względy na ich formę winny być zawsze odseparowane od danych prywatnych.
5. Materiały dydaktyczne udostępniane online muszą zostać opatrzone przez autora informacją o pochodzeniu oraz nie naruszać praw autorskich innych osób lub podmiotów.
6. Wszelkie materiały dydaktyczne udostępnione Studentom i Pracownikom w ramach systemów umożliwiających zdalną pracę i wideokonferencje podlega ochronie prawnej w szczególności przewidzianej w przepisach o prawie autorskim i prawach pokrewnych, przepisach o ochronie danych osobowych i innych powszechnie obowiązujących przepisach regulujących tajemnice ustawowe.
7. Wszelkie naruszenia bezpieczeństwa informacji należy zgłaszać do Działu ds. Bezpieczeństwa Informacji SUM.

3.1 Bezpieczeństwo informacji pracy zdalnej świadczonej z wykorzystaniem technologii ICT

1. Zaleca się aby miejsce nawiązywania połączenia gwarantowało:
    a. poufność przesyłanych i przetwarzanych na ekranie komputera informacji,
    b. stabilność łącza internetowego,
    c. szyfrowanie sieci bezprzewodowej używanej do zdalnej pracy,
    d. spełniało wymogi bezpiecznej pracy (BHP).
2. Zaleca się użytkownikom pracującym zdalnie, aby przed rozpoczęciem pracy zweryfikowali czy miejsce zdalnego łączenia spełnia odpowiednie warunki bezpieczeństwa informatycznego (np. łączenie się przez zabezpieczoną sieć Wi-Fi - szyfrowaną) i fizycznego, a w szczególności miejsce zapewnia, że podczas zdalnej pracy nieuprawniona osoba (w tym rodzina i przyjaciele) nie wejdzie w posiadanie informacji przesyłanych podczas pracy zdalnej.

3. Należy na bieżąco aktualizować system operacyjny oraz towarzyszące oprogramowanie, w szczególności takie jak przeglądarka stron internetowych, program pocztowy, pakiet biurowy, czytnik plików PDF, program antywirusowy.
4. W przypadku prywatnego komputera, współdzielonego z innymi osobami zaleca się, aby zapewniał on odrębne profile użytkowników chronione hasłem.
5. Należy sprawdzić czy program antywirusowy posiada aktualną bazę i czy ochrona rezydentna działa.
6. Należy pobierać oprogramowanie wyłącznie ze stron producentów. Zabrania się przetwarzania danych służbowych na nieautoryzowanym oprogramowaniu.
7. Należy unikać wchodzenia na nieznane czy przypadkowe strony internetowe.
8. W celach służbowych należy korzystać wyłącznie z poczty pracowniczej w domenie sum.edu.pl, która zapewnia szyfrowanie komunikacji i ochronę antywirusową.
9. Zabrania się otwierania załączników z nieznanych źródeł dostarczanych poprzez korespondencję elektroniczną.
10. Należy dostosować złożoność haseł odpowiednio do zagrożeń i krytyczności chronionych nim zasobów.
11. Nie należy zapamiętywać haseł w aplikacjach (np. w przeglądarkach internetowych)
12. Zaleca się używanie menagerów haseł, w celu uniknięcia zapisywania haseł na kartkach.
13. Nie należy używać tych samych haseł w różnych systemach informatycznych.
14. Korzystając z domowego routera WIFI należy użyć skomplikowanego hasła dostępowego, jeśli to możliwe wyłączyć WPS (uwierzytelnienie PIN'em) oraz zmień domyślne hasło administratora.
15. Nie należy logować się do systemów informatycznych w przypadkowych miejscach z niezaufanych urządzeń lub publicznych niezabezpieczonych sieci Wi-Fi.
16. Należy wykonywać regularne kopie zapasowe.
17. Zaleca się korzystanie ze sprawdzonego oprogramowania do szyfrowania e-maili lub nośników danych.
18. Należy szyfrować dane osobowe przesyłane pocztą elektroniczną.
19. Należy szyfrować dyski twarde w komputerach przenośnych i inne służbowe nośniki wymienne, w szczególności wolumeny (partycje lub foldery), w których przechowywane są dane niezbędne do wykonywania pracy zdalnej.
20. Przy pracy zdalnej należy korzystać z szyfrowanego połączenia VPN, co umożliwia usługa Zdalnej Pracy udostępniana przez Centrum Informatyki i Informatyzacji SUM (https://informatyka.sum.edu.pl).
21. Należy blokować komputer za każdym razem kiedy zamierza się opuścić stanowisko pracy:
    a. skrót klawiszowy dla Microsoft Windows: Win+L lub
    b. skrót klawiszowy dla Apple Mac OS: Control+Command+Q
22. Należy korzystać z automatycznego blokowania komputera po pewnym krótkim czasie bezczynności.
23. Przy wykonywaniu zadań służbowych należy unikać uruchamiania aplikacji użytkowych do celów prywatnych aby zredukować ryzyko omyłkowego udostepnienia danych.

24. Nie należy umieszczać w komputerze nośników USB nieznanego pochodzenia, ponieważ może znajdować się na nich złośliwe oprogramowanie.
25. Zabrania się przydzielania dostępu na zasadzie telepracy do zasobów i systemów przetwarzających dane osobowe wrażliwe i inne dane szczególnie chronione takie jak tajemnica przedsiębiorstwa.
26. Zaleca się przetwarzanie informacji w ramach zdalnego pulpitu, a w przypadku jego braku nakazuje się przechowywanie danych służbowych w usłudze *edysk.sum.edu.pl* po zakończeniu pracy i wgraniu opracowywanych plików na ww. eDysk. Należy usunąć wszelkie kopie z komputera, z którego nawiązywano zdalne połączenie.
27. Jeśli podczas zdalnej pracy wykorzystywane jest licencjonowane oprogramowanie, którego licencjobiorcą jest SUM wówczas zdalnie łącząca się osoba:
    a. winna przestrzegać postanowień tej licencji,
    b. w przypadku niektórych licencji programowych niezbędnym będzie zarejestrowanie się w systemie wskazanym przez Centrum Informatyki i Informatyzacji SUM.
28. W przypadku udostępniania pulpitu lub kontroli nad komputerem prywatnym należy zabezpieczyć pliki służbowe przed nieuprawnionym dostępem.

3.2 Bezpieczeństwo fizyczne i osobowe

1. Sprzęt wykorzystywany do zdalnej pracy należy przechowywać w nadzorowanym miejscu i nie pozostawiać go bez opieki.
2. W przypadku konieczności wydruku pliku służbowego na urządzeniu prywatnym należy zapewnić aby:
    a. wszystkie wydruki zostały zabezpieczone, w szczególności w sytuacji awarii drukarki,
    b. po zakończeniu wydruku aby nośniki pamięci zostały odłączone i zabrane z urządzenia drukującego,
    c. wydruki zostały przekazane autoryzowanemu odbiorcy lub skutecznie zniszczone po ustaniu ich użyteczności służbowej.
3. Nie należy skanować dokumentów na urządzeniach wielofunkcyjnych niebędących własnością Uczelni.
4. Zabrania się wykonywania zdjęć dokumentom za pomocą prywatnych smartfonów, w tym także dokonywania innej formy ich odwzorowania za pośrednictwem nieautoryzowanych środków przetwarzania.
5. Prowadząc służbowe rozmowy telefoniczne lub uczestnicząc w wideokonferencjach należy zapewnić aby osoby postronne nie miały sposobności do zapoznania się z omawianymi sprawami.

3.3 Zasady prowadzenia wideokonferencji

1. Wideokonferencje prowadzi się z wykorzystaniem narzędzi informatycznych autoryzowanych i udostępnionych przez Uczelnię lub przez podmiot będący gospodarzem Wideokonferencji.
2. Uczestnicząc w wideokonferencjach należy zadbać aby obszar objęty wideotransmisją (w szczególności za uczestnikiem) zapewniał prywatność uczestnika. Należy w tym zakresie dobrać ustawienie kamery tak aby obszar za uczestnikiem stanowiła ściana lub jednolite tło, nienaruszające jego prywatności. W przypadku gdy system informatyczny to umożliwia należy skorzystać z opcji automatycznego zamazywania lub podmiany tła.
3. Odchodząc od miejsca wideokonferencji należy się z niej rozłączyć lub wyłączyć mikrofon i kamerę na czas nieobecności lub prowadzenia rozmowy prywatnej.
4. Nagrywanie wideokonferencji musi być prawnie uzasadnione i nie może naruszać prywatności uczestników wideokonferencji.
5. Prowadzący wideokonferencje informuje o jej nagrywaniu jej uczestników przed rozpoczęciem nagrywania.
6. W przypadku konieczności udostepnienia pulpitu innym uczestnikom wideokonferencji należy upewnić się, że nie zostaną udostępnione w ten sposób informacje podlegające szczególnej ochronie oraz że wszyscy uczestnicy konferencji uprawnieni są do dostępu do prezentowanych treści.
7. W ramach wideokonferencji mogą być udostępniane innym uczestnikom pliki jednakże wyłącznie w zakresie autoryzowanego przez Uczelnię narzędzia do prowadzenia wideokonferencji.

3.4 Narzędzia wideokonferencyjne i aplikacje chmurowe

1. Na potrzeby realizacji połączeń wideokonferencyjnych wykorzystuje się:
    a. wewnętrzne rozwiązania wideokonferencyjne stanowiące funkcjonalność platformy elearningowej,
    b. rozwiązania wideokonferencyjne udostępniane w ramach ogólnopolskiej szerokopasmowej sieci optycznej nauki PIONIER,
    c. rozwiązania wideokonferencyjne dedykowane dla potrzeb zarządczych oraz edukacyjnych udostępniane nieodpłatnie przez dostawców usług wideokonferencyjnych o ile spełniają one wymagania w zakresie przepisów RODO i nie stoją w sprzeczności z przepisami krajowymi.
2. W celu zapewnienia studentom i doktorantom narzędzi wspierających procesy dydaktyczne dopuszcza się stosowanie aplikacji chmurowych zintegrowanych na poziomie autoryzacji ze środowiskiem Uniwersytetu w zakresie usługi Microsoft Office 365 (zwana dalej: Office365) przy zachowaniu poniższych zasad:
    a. konto dostępowe do usługi zakładane jest automatycznie a dane do logowania wydawane są w bezpiecznej kopercie wraz z legitymacją,

b. odzyskiwanie hasła do konta przeprowadzane jest samodzielnie przez Studenta z wykorzystanie opcji przypominania hasła na stronie Wirtualnej Uczelni (https://u10.sum.edu.pl),
c. konto dostępowe do usługi zakładane jest wyłącznie na czas trwania studiów,
d. konto dostępowe do usługi jest jednocześnie kontem poczty uczelnianej Studenta.
e. konto dostępowe do usługi jest używane w pozostałych usługach udostępnianych studentom a w szczególności dotyczy:
   – Systemu Elearningowego SUM,
   – Usługi Wirtualnej Uczelni,
   – Usługi Systemu Egzaminacyjnego E-Tester,
   – Usługi PROXY zapewniającej zdalny dostęp do zasobów SUM,
f. za bezpieczeństwo indywidualnych danych autoryzacyjnych (login i hasło) odpowiada użytkownik.
g. Uniwersytet zastrzega sobie prawo aktywowania bądź deaktywowania programów w ramach usługi Office365 w zależności od profilu użytkownika.

3. W celu zapewnienia Wykładowcom Uniwersytetu narzędzi wspierających procesy dydaktyczne dopuszcza się stosowanie aplikacji chmurowych zintegrowanych na poziomie autoryzacji ze środowiskiem Uniwersytetu w zakresie usługi Microsoft Office 365 przy zachowaniu poniższych zasad:
   a. konto dostępowe do usługi zakładane jest wyłącznie na czas trwania stosunku pracy,
   b. konto dostępowe do usługi zakładane jest przez Centrum Informatyki i Informatyzacji SUM na wniosek Pracownika wysłany z konta poczty służbowej SUM. Dane dostępowe do usługi zostają przesłane na adres poczty służbowej wnioskodawcy,
   c. konto dostępowe do usługi jest używane do korzystania z platformy wideokonferencyjnej https://obrady.sum.edu.pl,
   d. usługa dostępna jest wyłącznie celem wsparcia kształcenia zdalnego z wykorzystaniem platformy Microsoft Teams. Pozostałe procesy kształcenia na odległość związane z publikacją materiałów dydaktycznych oraz procesem weryfikacji wiedzy z wykorzystaniem testów realizowane są za pomocą wewnętrznych narzędzi informatycznych Uczelni.
   e. usługa nie stanowi alternatywy dla poczty uczelnianej w domenie @sum.edu.pl. Adres usługi Office365 w domenie @365.sum.edu.pl może być wykorzystywany wyłącznie do komunikacji w grupie użytkowników domeny @365.sum.edu.pl w celach dydaktycznych.
4. Do doktorantów, kandydatów na stopień doktora i doktora habilitowanego w tym gości i uczestniczących w obradach organów nadających stopnie w SUM oraz słuchaczy studiów podyplomowych ww. przepisy stosuje się odpowiednio.

3.5 Korzystanie z usługi Microsoft Office 365 w SUM

1. W ramach usługi Microsoft Office365 plan A1 student i pracownik otrzymuje dostęp do:
   a. programów biurowych w wersji Office Web Apps,
   b. skrzynki pocztowej dedykowanej studentom,
   c. wirtualnego dysku przeznaczonego do tymczasowego przechowywania materiałów dydaktycznych,
   d. –usługi wideokonferencyjnej Microsoft Teams.
2. Użytkownik przyjmuje do wiadomości, że usługa będzie realizowana w oparciu o zasoby techniczne oraz oprogramowanie Microsoft Corporation.
3. Podczas tworzenia konta studenta, w usłudze Microsoft Office365 zapisywane będą następujące dane: imię, nazwisko, adres email.
4. Podczas tworzenia konta pracownika, w usłudze Microsoft Office365 zapisywane będą następujące dane: imię, nazwisko, adres email a w celu zapewnienia możliwości samodzielnego odzyskiwania hasła, użytkownik przy pierwszym logowaniu uzupełnia prywatny adres email i nr telefonu umożliwiający autoryzację
5. Każdy użytkownik w dowolnym momencie może zażądać usunięcia jego konta z usługi Microsoft Office365. W tym celu należy w formie pisemnej przekazać żądanie usunięcia konta do Centrum Informatyki i Informatyzacji.
6. Żądanie, o których mowa w ustępie poprzedzającym nie może utrudniać lub uniemożliwiać realizacji zadań dydaktycznych, prowadzenia prac służbowych lub innych zadań Uczelni wynikających z przepisów powszechnie obowiązujących.

3.6 Spójność i integralność danych

1. Pliki i dokumenty nadpisane w zakresie zdalnej pracy należy uaktualnić z ich wersjami przechowywanymi w zasobach systemów informatycznych Uczelni w celu zapewnienia integralności i spójności danych.
2. Celem uniknięcia braku integracji pomiędzy wersjami plików zaleca się wersjonowanie plików poprzez np. stosowania odpowiedniego nazewnictwa plików z inkrementowanym numerem wersji pliku.
3. Zabrania się usuwania metainformacji z dokumentów służbowych. Zaleca się usunięcie tych informacji z dokumentów gotowych wysyłanych do odbiorcy zewnętrznego.
4. Zabrania się usuwania metainformacji z dokumentów podpisanych cyfrowo.
5. W przypadku procedowania dokumentu podpisanego cyfrowo należy zachować zarówno dokument jak i doliczone do niego dodatkowe pliki (np. sygnatury potwierdzeń podpisu cyfrowego zapisane w formacie .XML)
6. Wszelkie dokumenty służbowe podpisane cyfrowo należy archiwizować po zakończeniu zdalnej pracy w zasobach komputerowych Uczelni.
7. Po zakończeniu świadczenia zdalnej pracy należy przenieść wszelkie pliki na służbowe urządzenie na terenie Uczelni lub zwrócić kierownikowi jednostki organizacyjnej.

8. Po zabezpieczeniu plików służbowych, o którym mowa w ustępie poprzedzającym należy skutecznie je usunąć z prywatnego komputera lub zaszyfrować w celu kontynuowania na nich pracy.

3.7 Główne zasady bezpieczeństwa urządzeń mobilnych

Niniejszy rozdział zawiera główne i uogólnione zasady bezpieczeństwa przetwarzania mobilnego. Urządzenia mobilne należy wykorzystywać zgodnie z ich z służbowym przeznaczeniem.

1. Przy przetwarzaniu danych służbowych na urządzeniach mobilnych stosuje się odpowiednio przepisy wcześniejszych rozdziałów niniejszej Instrukcji.
2. Posługując się urządzeniem mobilnym będącym własnością SUM należy zapewnić przetwarzanie informacji w sposób gwarantujący ich poufność, dostępność, integralność oraz rozliczalność.
3. Służbowe urządzenie mobilne winno być zabezpieczone co najmniej programem antywirusowym, blokadą ekranu i/lub innym mechanizmem kontroli dostępu.
4. Urządzenie mobilne wydane pracownikowi powinno znajdować się pod jego nieustannym nadzorem.
5. Podczas podróży służbowych należy zapewnić szczególny nadzór nad urządzeniem.
6. W zakresie służbowych urządzeń mobilnych zabrania się w szczególności:
    a. pozostawiania służbowych urządzeń mobilnych w miejscach nienadzorowanych.
    b. samowolnego instalowania aplikacji.
    c. synchronizacji urządzeń służbowych z prywatnym kontem.
    d. przekazywania/wypożyczania urządzenia osobom trzecim.
    e. zamawiania usług poprzez aplikacje zainstalowane w urządzeniu.
    f. przechowywania danych służbowych w tzw. usługach chmurowych tj. poza serwerami SUM, za wyjątkiem autoryzowanych przez SUM systemów informatycznych.
    g. nagrywania rozmów służbowych bez zezwolenia Władz Uczelni.
    h. fotografowania bez zezwolenia władz uczelni miejsc, w których w szczególności elementy sceny stanowią tajemnicę prawnie chronioną.
    i. udostępniania sieci internetowej poprzez funkcję routera.
    j. przechowywania w pamięci urządzenia danych wrażliwych i danych stanowiących tajemnicę przedsiębiorstwa.
7. W zakresie prywatnych urządzeń mobilnych zabrania się w szczególności:
    a. podłączania prywatnych urządzeń mobilnych do komputerów podłączonych do sieci SUMnet oraz jej podsieci.
    b. udostępniania sieci internetowej na terenie SUM poprzez uruchomienie w urządzeniu mobilnym funkcji routera Wi-Fi.

c. prowadzenia prywatnych rozmów telefonicznych w pomieszczeniach SUM, w których odbywa się rozmowa na tematy służbowe. Należy wówczas przejść w miejsce, w którym rozmów służbowych nie słychać np. na korytarz.
d. zabierania prywatnych urządzeń mobilnych na spotkania, których przedmiotem mogą być informacje niejawne, prawnie chronione lub sklasyfikowane jako noszące znamiona poufności.
e. wykorzystywania funkcji dyktafonu w celu nagrywania rozmów służbowych.
f. rejestrowania zajęć dydaktycznych bez zgody Władz Uczelni.

8. Zaleca się zachować szczególną ostrożność podczas odbierania rozmów telefonicznych z zagranicznych numerów, których się nie spodziewamy, a w przypadku zainicjowania takiej rozmowy, kiedy nie będzie można zrozumieć lub usłyszeć drugiej strony należy się niezwłocznie rozłączyć.

3.8 Postępowanie w przypadku zagubienia, kradzieży lub podejrzenia incydentu związanego z bezpieczeństwem informacji

1. W przypadku incydentu bezpieczeństwa informacji lub naruszenia ochrony danych osobowych podczas pracy zdalnej należy niezwłocznie powiadomić Dział ds. Bezpieczeństwa Informacji i opisać okoliczności tego naruszenia wraz z przesłaniem dowodów (zrzuty ekranu) na adres e-mail: incydent@sum.edu.pl.
2. Jeśli naruszenie dotyczy urządzenia prywatnego, wykorzystywanego do pracy za usunięcie awarii lub skutków incydentu odpowiada jego właściciel.
3. Jeśli naruszenie dotyczy urządzenia mobilnego należy niezwłocznie powiadomić operatora o kradzieży z jednoczesnym wnioskiem o blokadę urządzenia i/lub karty SIM.
4. W przypadku zagubienia lub kradzieży urządzenia mobilnego po potwierdzeniu tego faktu przez użytkownika urządzenia mobilnego, ICI w przypadku gdy jest to możliwe zdalnie wymazuje wszelkie informacje z urządzenia i uruchamia na nim zdalną blokadę.
5. Jeśli oprogramowanie antywirusowe umożliwia opcję lokalizacji telefonu i blokady antykradzieżowej wówczas należy użyć tych funkcji. W przypadku pozytywnego zlokalizowania urządzenia skradzionego należy przekazać Policji informacje o lokalizacji.
6. Należy dokonać zgłoszenia na Policję.

W przypadku podejrzanego działania urządzenia służbowego należy niezwłocznie zgłosić ten fakt do Działu Technicznego SUM.

Wszystkie niezgodności związane z postanowieniami niniejszej instrukcji należy zgłaszać zgodne z Zarządzeniem Rektora SUM w sprawie wprowadzenia *„Instrukcji Zarządzania Incydentami w Zakresie Bezpieczeństwa Informacji w Śląskim Uniwersytecie Medycznym w Katowicach”*.

REKTOR
Śląskiego Uniwersytetu Medycznego w Katowicach
prof. dr hab. n. med. Przemysław Jałowiecki