Załącznik do Zarządzenia Rektora nr 47/2022 z dnia 13 grudnia 2022 r.

2022

Regulamin korzystania z komputerów i mobilnych nośników danych

W UNIWERSYTECIE MUZYCZNYM FRYDERYKA CHOPINA

KINGA WÓJCIK-PRZĄDKA

Spis treści

Cel dokumentu

Zasady bezpieczeństwa informacji Uniwersytetu Muzycznego Fryderyka Chopina (dalej UMFC) zobowiązują wszystkich pracowników oraz osoby zatrudnione na podstawie umów cywilnoprawnych do zachowania poufności, integralności i dostępności informacji, w tym danych osobowych.

Niniejszy Regulamin jest aktem wewnętrznego stosowania w UMFC. Stanowi przyjęty do stosowania środek organizacyjny służący zapewnieniu bezpieczeństwa informacji UMFC i minimalizacji ryzyka, które może wystąpić w tym obszarze. Celem Regulaminu jest określenie i przedstawienie zasad m.in:

a) wykonywania pracy w sposób zdalny (na odległość) w bezpieczny sposób,
b) korzystania z udostępnionego przez pracodawcę komputera lub laptopa do realizowania obowiązków służbowych na rzecz UMFC,
c) zapewniania bezpieczeństwa w przypadku wykorzystywania sprzętu prywatnego do zadań służbowych,
d) zapewniania bezpieczeństwa pozostałych przenośnych nośników danych,
e) bezpiecznych kanałów komunikacji,
f) zgłaszania incydentów i naruszeń ochrony danych osobowych.

Zasady wskazane w niniejszym Regulaminie wynikają z przyjętych w UMFC wewnętrznych regulacji składających się na system zarządzania bezpieczeństwem informacji, stanowią również środki organizacyjne stosowane przez Administratora w celu zapewnienia bezpieczeństwa przetwarzania danych osobowych w UMFC.

Słownik użytych pojęć i skrótów

DI – Dział Informatyki UMFC, oraz firmy zewnętrzne działające w imieniu i na rzecz UMFC w porozumieniu z DI w zakresie usług teleinformatyki

IOD – Inspektor ochrony danych UMFC

Licencja użytkownika – umowa o korzystanie z oprogramowania komputerowego, określająca warunki
i pola eksploatacji na jakich można korzystać z tego oprogramowania. Umowa, o której mowa w zdaniu poprzednim może być zawarta również w formie dokumentowej np. poprzez akceptację regulaminu.

Nośnik danych/mobilny nośnik danych – urządzenie elektroniczne lub dokument w wersji papierowej w którym/ na którym zawarte są informacje chronione, w tym dane osobowe (laptop, pendrive, przenośny, dysk zewnętrzny, telefon komórkowy, tablet, dokumenty papierowe itp.)

Praca zdalna - praca wykonywana całkowicie lub częściowo poza miejscem stałego wykonywania obowiązków służbowych, np. w miejscu zamieszkania lub w innym miejscu ustalonym przez pracownika i pracodawcę, w szczególności z wykorzystaniem środków

bezpośredniego porozumiewania się na odległość. Praca zdalna nie stanowi telepracy, o której mowa w art. 67^5 -67^{17} Kodeksu pracy (t.j. z dnia 16 maja 2019 r., Dz.U. z 2019 r. poz. 1040 z późn. zm.).

Pracodawca – Uniwersytet Muzyczny Fryderyka Chopina

Pracownik – wszystkie osoby świadczące pracę na rzecz UMFC zarówno na podstawie stosunku pracy jak i umowy cywilnoprawnej, posiadające status Użytkownika standardowego lub Użytkownika uprzywilejowanego.

Standardowa konfiguracja – ustawienia funkcjonalne i techniczne komputera lub laptopa wraz z zainstalowanym oprogramowaniem, przygotowane przez Dział Informatyki przed pierwszym ich wydaniem Pracownikowi.

Urządzenie – komputer stacjonarny i/lub laptop/telefon służbowy/tablet lub inne podobne urządzenie elektroniczne udostępnione przez UMFC Pracownikowi.

Urządzenie prywatne – komputer i/laptop/telefon /tablet lub inne podobne urządzenie elektroniczne nieudostępniane przez UMFC, wykorzystywane przez Pracownika lub współpracownika do wykonywania zadań służbowych na rzecz UMFC

Użytkownik standardowy – Pracownik posiadający dostęp do wewnętrznych i zewnętrznych systemów teleinformatycznych/ informatycznych wyłącznie na zasadzie korzystania z przyznanych mu przez administratorów tych systemów funkcjonalności i nadzorowanych przez DI.

Użytkownik uprzywilejowany – Pracownik lub współpracownik DI posiadający dostęp do wewnętrznych i zewnętrznych systemów teleinformatycznych/ informatycznych odpowiedzialny za ich pozyskanie, rozwój i utrzymanie, posiadający uprawnienia administratora na powierzonych przez UMFC stacjach roboczych oraz ponoszący całkowitą odpowiedzialność za prawidłowe funkcjonowanie systemów operacyjnych i zainstalowanych programów. Jeżeli wymagają tego ich obowiązki służbowe, Użytkownicy uprzywilejowani mogą posiadać podwyższone uprawnienia (również administracyjne) w wewnętrznych i zewnętrznych systemach teleinformatycznych / informatycznych UMFC .

Użytkownik – Użytkownik standardowy i Użytkownik uprzywilejowany.

I. ZASADY WYKONYWANIA PRACY ZDALNEJ

Zasady ogólne

1. Regulamin obowiązuje osoby, które wykonują pracę zdalną bez względu na formę zatrudnienia.
2. Naruszenie zasad wykonywania pracy zdalnej może stanowić naruszenie obowiązków pracowniczych, a w przypadku osób świadczących pracę na podstawie umów cywilnoprawnych stanowić naruszenie postanowień umownych skutkujące odpowiedzialnością kontraktową.

3. Pracodawca w miarę posiadanych możliwości zapewnia sprzęt do wykonywania pracy zdalnej lub określa zasady korzystania ze sprzętu należącego do pracownika, .
4. Pracodawca dopuszcza użycie Urządzeń prywatnych pracownika pod warunkiem poszanowania i ochrony informacji poufnych i innych tajemnic prawnie chronionych, w tym danych osobowych, a także informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę.

II. ZASADY KORZYSTANIA Z URZĄDZEŃ W CELACH SŁUŻBOWYCH

Zasady ogólne

1. Zasady określone w niniejszym Regulaminie dotyczą wszystkich Użytkowników, chyba że w jego treści wyraźnie określono inaczej.
2. Urządzenia dla Użytkowników, przygotowuje i wydaje DI - w Standardowej konfiguracji oraz zgodnie
   z postanowieniami niniejszego Regulaminu.
3. Użytkownik korzysta z Urządzenia zgodnie z niniejszym regulaminem oraz dba o nie zgodnie z postanowieniami Rozdziału ***Bezpieczeństwo fizyczne Urządzeń***.
4. Każdy użytkownik stosuje hasła zgodnie z postanowieniami Rozdziału ***Tworzenie i korzystanie***
   z haseł.
5. Na Urządzeniach udostępnionych przez UMFC korzysta się wyłącznie z legalnego oprogramowania
   i na warunkach określonych w Licencji użytkownika.
6. Użytkownikowi standardowemu nie wolno samodzielnie dokonywać instalacji oprogramowania na Urządzeniu,
7. Użytkownik który samodzielnie pozyskał i uruchomił oprogramowanie na Urządzeniu ponosi odpowiedzialność za jego funkcjonowanie.
8. Zabrania się Użytkownikom, z zastrzeżeniem postanowień ust.9:
   a) omijania mechanizmów kontroli (np. używania serwerów proxy),
   b) testowania wdrożonych zabezpieczeń,
   c) skanowania urządzeń sieciowych, serwerów oraz stacji roboczych pod kątem badania świadczonych usług,
   d) wyłączania programów uruchamianych automatycznie przy starcie systemu,
   e) odinstalowania programów,
   f) podejmowania jakichkolwiek prób ingerencji w Urządzenia (np. samodzielna naprawa), poza czynnościami związanymi z codzienną eksploatacją,
   g) modyfikacji i zmian w konfiguracji sprzętowej urządzeń (np. wymiany dysków wewnętrznych, wymiana pamięci RAM). Użytkownicy w tym zakresie powinni zwracać się o pomoc do DI.
9. Postanowienia ust. 8 nie mają zastosowania do Użytkowników uprzywilejowanych, którzy w zakresie swoich obowiązków służbowych mogą wykonywać wskazane w tym ustępie czynności, jednak

w przypadku, o którym mowa w ust. 8 lit. e) nie mogą oni odinstalowywać programów zainstalowanych przez DI takich jak ESET (program antywirusowy) i Magik Info.

10. Zabrania się Użytkownikom samodzielnego dokonywania zmiany nazwy Urządzenia nadanej przez DI w ramach Standardowej konfiguracji.
11. Pomoc i wsparcie techniczne dla Użytkowników w zakresie konfiguracji, naprawy i serwisu realizują pracownicy DI. Zgłoszenia dokonuje się za pośrednictwem poczty elektronicznej lub osobiście.
12. Urządzenia wydawane są w DI, a ich odbiór potwierdzany jest pisemnie przez Pracownika.
13. Urządzenia stanowią własność UMFC i Pracownik jest zobowiązany na każde polecenie UMFC dokonać jego zwrotu.
14. Kończąc współpracę z UMFC Użytkownik ma obowiązek niezwłocznego przekazania Urządzenia wraz ze znajdującymi się na nim danymi do DI.

Konfiguracja standardowa

1. Standardowo instalowanym systemem operacyjnym na Urządzeniach dla wszystkich Użytkowników jest system Windows z pełnym pakietem krytycznych aktualizacji oraz pakietem oprogramowania wskazanym w ust.2.
2. Instalowany pakiet oprogramowania w Standardowej konfiguracji zawiera:
   a) pakiet biurowy, w tym poczta elektroniczna,
   b) czytnik plików pdf.,
   c) oprogramowanie antywirusowe,
   d) stosowany przez UMFC oficjalny komunikator,
   e) oprogramowanie do kompresji i przesyłania zaszyfrowanych danych,
   f) VPN – w przypadku laptopa.
3. Urządzenie podłączane jest do domeny opartej na usłudze katalogowej Active Directory.
4. Każdy wydany Użytkownikowi laptop posiada szyfrowany dysk, jeżeli system i urządzenia umożliwiają taką funkcjonalność. W przypadku, gdy laptop posiada taką funkcjonalność Użytkownik nie może jej wyłączyć przez cały okres korzystania z tego urządzenia, bez zgody DI.
5. Każde Urządzenie posiada nazwę nadaną przez DI, której Użytkownik nie może zmienić.
6. Aktualny wykaz poszczególnych programów, o których mowa w ust. 2 jest prowadzony przez DI.
7. Każde Urządzenie wydane Użytkownikowi jest zabezpieczone hasłem oraz wdrożonym mechanizmem automatycznego wylogowania po 10 minutach nieaktywności.
8. DI dba o aktualizację Standardowej konfiguracji Urządzenia.

Korzystanie z systemu MacOS

1. DI prowadzi podstawowe wsparcie w zakresie obsługi systemu MacOS.
2. W ramach wsparcia podstawowego DI przed przekazaniem przygotowuje urządzenie do pracy:
   a) nadaje nazwę komputera zgodnie z przyjętym nazewnictwem UMFC ,
   b) tworzy konto „techniczne" użytkownika Admin (z wyłącznym dostępem dla DI),
   c) tworzy konto dla użytkownika,

d) instaluje program antywirusowy,
e) szyfruje dysk,
f) może udzielić użytkownikowi pomocy w instalacji niezbędnego oprogramowania.

3. W przypadku awarii systemu Mac OS, DI może zaproponować reinstalację systemu.
4. W przypadku awarii sprzętowej DI może (o ile to możliwe), zgłosić urządzenie do naprawy.
5. Użytkownikowi któremu zostaje powierzone Urządzenie marki Apple zabrania się deinstalacji oprogramowania, które zostało zainstalowane przez DI.
6. Jeśli zajdzie potrzeba skorzystania z konta Apple ID, użytkownik ma prawo utworzyć ww. konto wyłącznie przy użyciu służbowego adresu poczty elektronicznej.
7. W przypadku korzystania z konta Apple ID, na sprzęcie służbowym, użytkownikowi zabrania się przechowywania danych służbowych w usłudze iCloud Drive. Dane służbowe mogą być przechowywane jedynie na lokalnych nośnikach danych lub na udziałach sieciowych należących do UMFC .

Tworzenie i korzystanie z haseł przez Użytkownika

1. Zapisy niniejszego rozdziału dotyczą wszystkich Użytkowników bez względu na rodzaj używanego przez nich systemu operacyjnego.
2. Użytkownicy korzystający z Urządzeń zabezpieczają dostęp do nich za pomocą haseł.
3. Haseł używa się do:
   a) zabezpieczenia dostępu do systemu informatycznego,
   b) bezpiecznego funkcjonowania w Internecie (np. przy korzystaniu z prywatnej poczty, logowaniu do poczty służbowej przez przeglądarkę internetową, portale społecznościowe)
   c) przesyłania plików zawierających chronione informacje w sposób zaszyfrowany.
4. Użytkownik stosuje skomplikowane hasła (tzw. silne hasła), dbając o to, aby trudno było je odgadnąć. Hasło powinno składać się z **minimum 12 (dwunastu) znaków, w tym znaki specjalne, liczby, duże i małe litery**. Obowiązuje zasada: ***im dłuższe hasło i bardziej unikalne, tym lepiej.***
5. Silne hasła stosuje się w szczególności tam, gdzie zabezpieczamy dostęp do dużej ilość ważnych dla UMFC informacji obejmujących np.:
   a) dane kadrowe,
   b) dane osobowe nieudostępniane publicznie,
   c) dane finansowo - płacowe,
   d) informacje stanowiące tajemnicę przedsiębiorstwa,
   e) dane adresowe,
   f) dane przechowywane w utrzymywanych przez UMFC systemach teleinformatycznych,
   g) dane konfiguracyjne.
6. Nie należy używać w haśle trywialnych zwrotów oraz informacji, które łatwo można powiązać z Użytkownikiem (np. imię, nazwisko, data urodzenia) lub odgadnąć (np. aktualny miesiąc, rok). Przykłady trywialnego hasła: **UMFC1234, 1qaz@WSX, misiu102,**
7. Użytkownikowi nie wolno:
   a) udostępniać hasła – nikomu, nawet na wyraźne żądanie,
   b) zapisywać haseł w miejscach widocznych,
   c) przechowywać haseł w poczcie,
   d) zapamiętywać haseł na stronie.
8. Nie należy wykorzystywać tych samych haseł w kilku systemach jednocześnie, jeżeli mamy do czynienia z wrażliwością informacji, o której mowa w pkt 5 powyżej.

9. Zalecane jest korzystanie z menagera hasła – (zasady korzystania opisano w rozdziale ***Korzystanie z menagera haseł***).
10. Hasła wymagają cyklicznych zmian co 9 miesięcy lub częściej jeżeli zajdzie okoliczność, o której mowa w pkt. 11.
11. Hasła zmieniamy niezwłocznie w sytuacji, gdy:
    a) mamy podejrzenie ataku na konto,
    b) konto nie funkcjonuje w sposób prawidłowy,
    c) dostaliśmy hasło domyślne (firmowe) lub jednorazowe,
    d) otrzymaliśmy komunikat o konieczności zmiany od DI lub IOD.
12. Przykład poprawnie wygenerowanego hasła prezentuje poniższy opis:

    Wymyślamy dłuższe zdanie i hasło tworzymy z pierwszych liter wyrazów tworzących to zdanie.

    Chwilę **p**o **8** **j**estem **p**o **3** **d**użych **k**awach **i** **n**adal **n**ie **m**ogę **$**ię **o**budzić !

    Hasło: Cp8jp3dkinnm$o!

Korzystanie z menagera hasła

1. W celu wygenerowania hasła Użytkownicy, niezależnie od rodzaju używanego systemu operacyjnego korzystają z menagera hasła. Zalecanym programem jest KeePassXc.
2. Użytkownicy mogą korzystać z innego, dowolnego oprogramowania do przechowywania i tworzenia haseł odpowiedniego dla danego systemu operacyjnego, lecz korzysta się wyłącznie z legalnego oprogramowania i na warunkach określonych w Licencji użytkownika.

Bezpieczeństwo fizyczne Urządzeń wykorzystywanych do celów służbowych

1. Użytkownik zobowiązany jest do zabezpieczenia Urządzenia w czasie jego transportu.
2. Nie wolno pozostawiać Urządzenia w miejscach publicznych bez nadzoru.
3. Podczas transportu Urządzenia samochodem nie zaleca się przewożenia go w widocznym miejscu (np. na siedzeniu pasażera lub tylnej kanapie), w celu zminimalizowania ryzyka kradzieży podczas postoju.
4. Podczas transportu Urządzenie powinno być wyłączone, a nie pozostawione w trybie uśpienia.
5. Zabronione jest wykonywanie zadań służbowych z wykorzystaniem Urządzenia podczas jazdy miejską komunikacją publiczną lub w takich miejscach publicznych, które powodują uzasadnione ryzyko naruszenia poufności danych.
6. Użytkownik dba o powierzone Urządzenie oraz chroni go przed szkodliwym wpływem warunków zewnętrznych m.in. nadmiernym nasłonecznieniem, przegrzaniem, zalaniem.
7. Urządzenia powinny być wykorzystywane przez Użytkowników zgodnie z ich przeznaczeniem
   i zasadami prawidłowej eksploatacji określonymi przez producenta.
8. W siedzibie pracodawcy należy stosować się do zasad instrukcji Ppoż., BHP oraz innych zaleceń związanych z bezpieczeństwem fizycznym i środowiskowym przekazywanych przez inspektorów ochrony przeciwpożarowej, BHP oraz DAG.

9. W miejscu wykonywanej pracy Użytkownik zabezpiecza Urządzenie, z należytą starannością i w miarę posiadanych możliwości, przed jego kradzieżą lub uszkodzeniem.
10. W przypadku kradzieży, zagubienia, zniszczenia Urządzenia lub utraty przechowywanych na nim danych należy niezwłocznie powiadomić o tym fakcie DI oraz IOD (w przypadku gdy w Urządzeniu przechowywane są dane osobowe). Kontakt realizowany jest następującymi kanałami:
    a) DI – serwis@chopin.edu.pl lub tel. na nr 22 278 9**3 38**
    b) IOD – iod@chopin.edu.pl

III. DOSTĘP DO SIECI I CHMURY

1. Podczas wykonywania pracy zdalnej należy korzystać tylko z zaufanego dostępu do sieci lub chmury oraz przestrzegać wszelkich zasad i procedur organizacyjnych dotyczących logowania i udostępniania danych.
2. Zabrania się korzystania z internetowych sieci publicznych w celu zdalnego wykonywania zadań służbowych.
3. Dostęp do dysków sieciowych UMFC możliwy jest jedynie przy wykorzystaniu łącza VPN oraz przy wykorzystaniu służbowego laptopa.
4. Należy odpowiednio stopniować dostęp i uprawnienia do dysków sieciowych (nie wszyscy do wszystkiego, tylko zgodnie z zasadą konieczności, nadanych upoważnień i w celu wykonania obowiązków służbowych).
5. Jeśli praca nie jest wykonywana w chmurze lub pracownik nie ma dostępu do sieci, należy zadbać o bezpieczną archiwizację danych.

IV. BEZPIECZEŃSTWO DOKUMENTÓW W WERSJI PAPIEROWEJ (TRADYCYJNE NOŚNIKI DANYCH)

1. Należy unikać przenoszenia poza organizację dokumentów zawierających dane osobowe lub inne informacje chronione w formie papierowej. W przypadku konieczności wykonywania pracy zdalnej z wykorzystaniem dokumentacji papierowej jej przenoszenie może odbywać się jedynie za zgodą bezpośredniego przełożonego.
2. Jeżeli istnieje uzasadniona konieczność wykonywania pracy poza siedzibą organizacji wymagająca wykorzystania papierowej formy dokumentu należy zapewnić im bezpieczeństwo podczas transportu oraz w miejscu wykonywania pracy.
3. Nie wolno pozostawiać dokumentów w miejscu wykonywania pracy bez nadzoru, dokumenty muszą być zabezpieczone przed ich przypadkowym zniszczeniem, zalaniem lub zabrudzeniem oraz kradzieżą bądź zagubieniem.
4. Podczas transportu nie wolno pozostawiać dokumentów w widocznym miejscu w samochodzie np. na siedzeniach. Zalecane jest schowanie ich np. do bagażnika.
5. Nie wolno wyrzucać żadnych dokumentów (błędnych wydruków, niepotrzebnych projektów, notatek itp.) zawierających dane chronione lub nazwę instytucji do kosza. Ich niszczenie powinno odbyć się z wykorzystaniem niszczarki do dokumentów, a w przypadku jej braku w

miejscu wykonywania pracy zdalnej niszczenia należy dokonać w siedzibie pracodawcy, zgodnie z obowiązującymi w organizacji zasadami.
6. Dokumenty w formie papierowej należy chronić przed dostępem do nich osób nieuprawnionych.
7. Drukowanie dokumentów należy ograniczyć jedynie do tych niezbędnych.
8. Nie wolno korzystać z ogólnodostępnych punktów kserograficznych lub drukowania w celu kserowania lub drukowania dokumentów zawierających dane osobowe lub inne informacje chronione.

V. BEZPIECZEŃSTWO ZDALNEJ KOMUNIKACJI

Praca zdalna w UMFC realizowana jest za pośrednictwem ustalonych kanałów komunikacji:
a) służbowej poczty elektronicznej,
b) Microsoft Teams, Zoom,
c) Zdalnych połączeń grupowych,
d) W kontakcie telefonicznym.

Zdalne nauczanie realizowane jest za pośrednictwem MS Teams. Zasady dotyczące zdalnego nauczania określa UMFC w odrębnych komunikatach i procedurach.

Poczta służbowa

1. Do zadań służbowych należy wykorzystywać przede wszystkim służbowe konta poczty elektronicznej. Jeśli przy pracy wymagającej przetwarzania danych osobowych musi zostać wykorzystany prywatny adres poczty elektronicznej należy upewnić się, że treść i załączniki są właściwie szyfrowane.
2. Należy unikać używania danych osobowych lub poufnych informacji w temacie wiadomości.
3. Przed wysłaniem wiadomości e-mail należy upewnić się, że jest on wysyłany do właściwego adresata, zwłaszcza jeśli wiadomość zawiera dane osobowe lub dane wrażliwe.
4. W przypadku kierowania korespondencji do wielu odbiorców spoza organizacji należy bezwzględnie stosować opcję UDW, BCC (ukryte do wiadomości, blind carbon copy).
5. Należy dokładnie sprawdzić nadawcę otrzymanej wiadomości e-mail. Nie wolno otwierać wiadomości od nieznanych adresatów, a zwłaszcza nie otwierać załączników i nie klikać w linki zawarte w treści wiadomości od nieznanych nadawców z uwagi na realne zagrożenie atakiem phishingowym.
6. Należy czytać wszystkie komunikaty przesyłane przez DI i/lub IOD gdyż mogą zawierać dodatkowe zalecenia dotyczące zasad bezpieczeństwa nieujęte w niniejszym Regulaminie i/lub informacje o aktualnych zagrożeniach i niebezpieczeństwach.

Praca zdalna w zespołach – połączenia grupowe

1. Dopuszcza się wykorzystywanie następujących aplikacji do połączeń grupowych: Microsoft Teams oraz Zoom lub innych programów rekomendowanych przez UMFC.

2. Podczas grupowych połączeń należy zapewnić brak dostępu do wymienianych informacji osobom nieuprawnionym.
3. Nie wolno przesyłać linków do spotkań służbowych za pośrednictwem portali społecznościowych.

Rozmowy telefoniczne

1. Nie należy ujawniać danych osobowych oraz żadnych informacji poufnych, dopóki nie istnieje pewność kim jest rozmówca.
2. Nie należy ufać nieznanemu rozmówcy, który prosi o podanie poufnych danych (w szczególności hasła, kody, PIN'y), np. pod pretekstem rozpracowywania grupy przestępczej (tzw. metodą „na policjanta"), aktualizacji systemu lub dokonania innej czynności wymagającej podania haseł, kodów, PIN'ów.
3. Nie należy prowadzić służbowych rozmów telefonicznych w miejscach publicznych np. komunikacji miejskiej, w kawiarniach, restauracjach lub na balkonie w miejscu zamieszkania bez gwarancji zachowania poufności wymienianych informacji.

VI. INCYDENTY I AWARIE. ZGŁASZANIE NARUSZEŃ OCHRONY DANYCH.

1. W przypadku wykrycia zainfekowania wirusem i niemożności usunięcia go przez oprogramowanie antywirusowe, zarażony komputer przenośny powinien zostać niezwłocznie odłączony z sieci komputerowej i pozostać wyłączony do momentu usunięcia wirusa. W takiej sytuacji należy niezwłocznie zawiadomić Dział Informatyki.
2. Wystąpienie zainfekowania wirusem systemu operacyjnego komputera równoważne jest z wystąpieniem incydentu dotyczącego bezpieczeństwa informacji i podlega zgłoszeniu zgodnie z zasadami postępowania w przypadku naruszenia ochrony danych (Kierownictwo UMFC oraz Inspektor Ochrony Danych).
3. Osoby zapewniające bezpieczeństwo teleinformatyczne UMFC przechowują osobną kopię oprogramowania antywirusowego w celu możliwości wykonania tzw. skanowania off- line.
4. W przypadku zagubienia lub kradzieży urządzenia, na którym była wykonywana praca lub przechowywane materiały z nią związane, należy natychmiast podjąć odpowiednie kroki w celu – o ile jest to możliwe – zdalnego wyczyszczenia jego pamięci. W takiej sytuacji należy niezwłocznie zawiadomić Dział Informatyki.
5. W przypadku zagubienia lub kradzieży przenośnego nośnika danych, w tym dokumentów w wersji papierowej należy natychmiast zawiadomić o tym fakcie Kierownictwo UMFC oraz inspektora ochrony danych.
6. Wykaz kontaktów w przypadku zaistnienia sytuacji kryzysowej stanowi załącznik nr 1 do niniejszego Regulaminu.

VII. POSTANOWIENIA KOŃCOWE

1. Zapisy Regulaminu podlegają przeglądowi co najmniej raz w roku pod kątem adekwatności stosowanych zabezpieczeń do zagrożeń i występującego ryzyka.

2. W przypadku ujawnienia konieczności niezwłocznego zastosowania dodatkowych, nieuwzględnionych w niniejszym Regulaminie zasad lub zmiany istniejących wszyscy Użytkownicy zostaną o tym fakcie poinformowani w sposób przyjęty w UMFC.
3. Regulamin wchodzi w życie z dniem ogłoszenia Zarządzenia.
4. Z uwagi na opis stosowanych środków zabezpieczeń w UMFC niniejszy Regulamin stanowi akt wewnętrzny i nie podlega publikacji w BIP.