Regulamin korzystania z usługi dostępu VPN

w ramach infrastruktury IT będącej własnością Centrum Onkologii - Instytutu im. Marii Skłodowskiej - Curie w Warszawie

Rozdział 1
Cel regulaminu.
§ 1

Celem niniejszego regulaminu jest wskazanie zasad oraz reguł korzystania ze zdalnego dostępu do sieci komputerowej poprzez połączenia Virtual Private Network (VPN) w technologii L2TP, IPSec oraz SSL.

Rozdział 2
Zakres regulaminu.
§ 1

Niniejszy regulamin dotyczy wszystkich pracowników, współpracowników, podwykonawców, konsultantów, pracowników czasowych oraz innych pracowników firm trzecich korzystających z zasobów wewnętrznych COI za pomocą połączeń VPN, zwanych dalej Użytkownikami.

Rozdział 3
Polityka dostępu
§ 1

1. Polityka dostępu do sieci VPN stanowi, iż użytkownicy są odpowiedzialni za bezpieczeństwo korzystania z usługi, w szczególności za zachowanie zasad opisanych w §2 niniejszego rozdziału.
2. Użytkownicy korzystający z prywatnych urządzeń dostępowych takich jak: komputery, laptopy, palmtopy, tablety itp. w czasie połączenia z siecią VPN również podlegają niniejszym zapisom regulaminu i regułom jakie obowiązują w sieci lokalnej COI.

§ 2

1. Tylko autoryzowani użytkownicy mogą korzystać z połączeń VPN.
2. Obowiązkiem każdego Użytkownika korzystającego z sieci VPN i co za tym idzie zasobów sieciowych jest bezwzględne przestrzeganie reguł opisanych poniżej:

a) dopilnowanie by żaden inny nieautoryzowany podmiot/użytkownik nie korzystał z praw przydzielonych Użytkownikowi.
b) wykorzystanie imiennego certyfikatu, silnego hasła do certyfikatu, loginu do konta oraz hasła do konta.
c) wykorzystanie tzw. „silnych haseł" składających się minimalnie z:
   - co najmniej 10 znaków alfanumerycznych,
   - co najmniej 2 cyfr,
   - co najmniej 2 znaków specjalnych takich jak „!@#$%^&*()_+=-|",
   - co najmniej 2 dużych liter,
d) upewnienie się, iż w tym samym czasie urządzenie dostępowe nie jest podpięte do innej sieci w szczególności sieci typu p2p (peer to peer) oraz m2m (mail to mail)
e) korzystanie z loginu, który musi mieć postać email'a firmowego i nie będącego emailem ogólnodostępnych usług hostingowych, np. „@wp.pl"
f) posiadanie na sprzęcie służącym do połączeń VPN oprogramowania antywirusowego z uaktualnionymi definicjami bazy wirusów, przy czym system antywirusowy musi być podczas całego połączenia włączony.

3. Zabronione jest:

a) przechowywanie certyfikatu dostępowego VPN w/na komputerze w miejscach publicznych takich jak: kafejki internetowe, komputery w hotelu, etc.
b) przechowywanie certyfikatu w usługach online takich jak np. dropbox, mesh, etc.

c) przechowywanie hasła oraz login w postaci niezaszyfrowanej np. w pliku tekstowym, na kartce, etc.
d) podwójne szyfrowanie za wyjątkiem usług RDP oraz usług SSH
e) korzystanie z zasobów sieci Internet poprzez sieć VPN
f) korzystanie z połączeń, adresów, lokalizacji i technologii nie zaaprobowanych przez Dział Informatyki
g) wykorzystanie sieci VPN do innych czynności niż wykonywanie zadań służbowych

4. Użytkownicy korzystający z sieci VPN są limitowani maksymalnie do 24 godzinnego połączenia ciągłego, a w wypadku wykrycia nieaktywności połączenie zostanie automatyczne rozłączone po 20 minutach.
5. Użytkownicy połączeń VPN są zobowiązani do zgłaszania do Działu Informatyki COI zauważonych nieprawidłowości w działaniu usług.

§ 3

Użytkownik korzystający z połączenia VPN zgadza się na:

a) monitorowanie zachowania użytkownika w sieci włączając w to takie elementy jak: poczta, dostęp do zasobów plikowych, dostęp do zasobów teleinformatycznych np. sesje SSH, sesje RDP, itp.
b) przeszkolenie z zasad prawidłowego korzystania z sieci VPN.
c) cykliczną zmianę hasła do konta dostępowego, nie rzadziej niż co 90 dni.
login do konta będzie składał się z emaila firmowego.

Rozdział 4

§ 1

Naruszenie regulaminu

Każdy Użytkownik, któremu udowodni się niestosowanie do niniejszego regulaminu lub omijanie jego zapisów może być pociągnięty do odpowiedzialności dyscyplinarnej , zgodnie z obowiązującymi przepisami.

§ 2

Odpowiedzialność

Użytkownik ponosi pełną odpowiedzialność za wszelkie szkody przez niego spowodowane w odległych lub lokalnych systemach komputerowych oraz za wszelkie inne straty lub nadużycia popełnione przy użyciu udostępnionych mu zasobów i programów użytkowych.