Załącznik nr 2
do Zarządzenia nr 12/2020
z dnia 24 marca 2020r.

INFORMACJA DLA SŁUCHACZA DOTYCZĄCA BEZPIECZEŃSTWA INFORMACJI PRZY NAUCZANIU ZDALNYM W SZKOLE POLICELALNEJ - MEDYCZNYM STUDIUM ZAWODOWYM W CHEŁMIE

1. Używaj tylko zaufanego dostępu do sieci lub chmury, unikaj sieci ogólnodostępnych.
2. Do autoryzacji we wszystkich systemach używaj haseł o długości min 8 znaków zawierających kombinację małych i dużych znaków, cyfr i znaków specjalnych; hasło zmieniaj regularnie co najmniej raz na 30 dni; nie stosuj tych samych haseł do różnych systemów.
3. Stosuj oprogramowanie zabezpieczające komputer np. programy antywirusowe, zaporę sieciową (FireWall).
4. Aktualizuj oprogramowanie urządzeń, na których pracujesz.
5. Po zakończeniu pracy wyloguj się z programów, z których korzystałeś; blokuj komputer, na którym pracujesz w razie oddalenia się od miejsca pracy w ramach pracy zdalnej.
6. Korzystając z zasobów pamiętaj o przestrzeganiu przepisów prawa autorskiego i praw pokrewnych.

Stosuj się do przyjętych standardów w zakresie bezpieczeństwa.
Pamiętaj, o następujących zagrożeniach:

Fałszywe wiadomości e-mail (phishing)

Od dłuższego czasu użytkownicy Internetu otrzymują e-maile łudząco podobne do wysyłanych przez Pocztę Polską, firmy kurierskie czy telekomunikacyjne. **Phishing może dotyczyć również aktualnej sytuacji związanej z koronawirusem. To oznacza, że atakujący może podszyć się pod służby sanitarne.** Spreparowane wiadomości często zawierają załącznik z oprogramowaniem lub link do niego. Otworzenie takiego załącznika powoduje zainfekowanie komputera, a w konsekwencji – wyłudzenie np. danych uwierzytelniających do kont bankowych czy zaszyfrowanie zawartości komputera lub serwera służbowego (bywa, że pojawia się żądanie zapłaty okupu w zamian za odszyfrowanie). Fałszywe wiadomości e-mail (phishing) **Dlatego zwracaj baczną uwagę na otrzymywane wiadomości:**

1. Przeczytaj uważnie treść e-maila, przyjrzyj się jego formie – jeśli masz wątpliwości, porównaj wiadomość z innymi e-mailami od tego samego nadawcy.
2. Zachowaj czujność w przypadku otrzymania wiadomości w jakikolwiek sposób związanej z kwestiami finansowymi.
3. Przed kliknięciem w link sprawdź, dokąd prowadzi – jeśli odsyła do formularza, w którym trzeba podać ważne dane, zachowaj ostrożność.
4. Szczególnie uważaj na e-maile, w których nadawca straszy Cię konsekwencjami lub zbyt wiele obiecuje.
5. Nie otwieraj załączników, które budzą Twoją wątpliwość.
6. Patrz na treść wiadomości, jej styl oraz poprawność językową – błędy mogą być sygnałem ostrzegawczym, gdyż teksty tworzone przez profesjonalne podmioty są co do zasady prawidłowo sformułowane.

Przeglądanie zasobów Internetu

Podczas korzystania z przeglądarek internetowych należy zwracać uwagę na nietypowe rzeczy, które dzieją się w trakcie pracy. Najczęstsze nieautoryzowane zmiany mogą być powodowane przez: wyświetlające się okienka z reklamami, zmianę wyglądu strony, podejrzane linki, reklamy wyświetlające się na stronach internetowych bez możliwości ich zamknięcia. W ostatnim czasie w sieci można natrafić na portale, które służą do wyłudzania danych osobowych oraz haseł. Najważniejsze, aby pamiętać o niepodawaniu tego typu informacji na stronach, których pochodzenia nie jesteśmy pewni. **O braku wiarygodności portalu może świadczyć np. brak szyfrowania SSL (kłódka z lewej strony adresu WWW) lub pojawianie się okienek reklamowych, których nie można zamknąć.**