III LICEUM OGÓLNOKSZTAŁCĄCE
im. Juliusza Słowackiego
97-300 Piotrków Trybunalski
Al. Armii Krajowej 17
NIP 771-16-88-537 tel. 44/647 22 63
(*pieczęć szkoły*)

Piotrków Trybunalski, 17.09.2020 r.
(*miejscowość, data*)

ZARZĄDZENIE DYREKTORA NR 6/2020

z dnia 17.09.2020 r.

w sprawie wprowadzenia w III Liceum Ogólnokształcącym im. Juliusza Słowackiego

w Piotrkowie Trybunalskim (dalej Szkoła)

narzędzi komunikacji i nauki zdalnej opartych o usługi

Microsoft 365 (pakiet Microsoft Office 365)

1) Na podstawie:
   a) Rozporządzenia Ministra Edukacji Narodowej z 25 sierpnia 2017 r. w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji § 21.
   b) Rozporządzenie Ministra Edukacji Narodowej z dnia 20 marca 2020 r. w sprawie szczególnych rozwiązań w okresie czasowego ograniczenia funkcjonowania jednostek systemu oświaty w związku z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19.
   c) Rozporządzenie Ministra Edukacji Narodowej z dnia 20 marca 2020 r. zmieniające rozporządzenie w sprawie czasowego ograniczenia funkcjonowania jednostek systemu oświaty w związku z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19.

zarządzam:

§ 1

1. Z dniem 21.09.2020 r. wprowadzam w Szkole pakiet Office 365 firmy Microsoft, jako zestaw narzędzi służących do realizacji obowiązków pracy Nauczycieli w zakresie realizacji nauczania zdalnego i komunikacji z Rodzicami.
2. Do wykorzystywania pakietu Office 365 firmy Microsoft zobowiązani są również Uczniowie Szkoły oraz Opiekunowie Prawni (w tym Rodzice Uczniów) w zakresie realizowania nauki zdalnej oraz komunikacji w ramach realizowania programu nauczania.

3. W ramach pakietu wprowadzane są narzędzia określone w ramach Regulamin korzystania z usług Microsoft Office 365 dla Edukacji A1 w III Liceum Ogólnokształcącym im. Juliusza Słowackiego w Piotrkowie Trybunalskim, Al. Armii Krajowej 17, 97-300 Piotrków Trybunalski.

§ 2

1. Wprowadzam w Szkole Regulamin korzystania z usług Microsoft Office 365 dla Edukacji A1 w III Liceum Ogólnokształcącym im. Juliusza Słowackiego w Piotrkowie Trybunalskim, Al. Armii Krajowej 17, 97-300 Piotrków Trybunalski dalej zwanym Regulaminem.

§ 3

1. Zobowiązuję wszystkich Pracowników Szkoły w tym Nauczycieli do zapoznania się z Regulaminem.
2. Zobowiązuję Nauczycieli do zapoznania z Regulaminem Uczniów oraz ich Opiekunów prawnych (w tym Rodziców).
3. Każdy Pracownik może posiadać tylko jedno Konto umożliwiające dostęp do Usług.
4. Każdy Pracownik zobowiązany jest odebrać informację z loginem i hasłem od osoby Administratora Usług.
5. Każdy Pracownik winien znać i rozumieć Politykę Bezpieczeństwa Informacji.
6. Hasło powinno być zmienianie zgodnie z Polityką Bezpieczeństwa Informacji.
7. Każdy Pracownik zobowiązany jest do zgłaszania wszelkich nieprawidłowości Administratorowi Usługi niezwłocznie, nie dłużej jednak niż 24 godziny od ich zidentyfikowania.
8. Każdy Opiekun prawny w tym Rodzic Ucznia zobowiązany jest do wykorzystywania pakietu Office 365 firmy Microsoft w celu realizacji nauki zdalnej.

§ 4

Zarządzenie wchodzi w życie z dniem 21 września 2020 r.

DYREKTOR
mgr Joanna Księżopolska - Szulc
(pieczęć i podpis dyrektora)

Regulamin korzystania z usług Microsoft Office 365 dla Edukacji A1 w III Liceum Ogólnokształcącym im. Juliusza Słowackiego w Piotrkowie Trybunalskim, Al. Armii Krajowej 17, 97-300 Piotrków Trybunalski

Słownik pojęć, skrótów i definicji

Lp.	Skrót/Definicja	Wyjaśnienie
1	Microsoft Office365 dla Edukacji A1 w skrócie O365 albo Usługa	Zbiór udostępnionych bezpłatnie aplikacji i usług dostępnych z serwerów Microsoft.
2	Placówka, Szkoła	III Liceum Ogólnokształcące im. Juliusza Słowackiego, Al. Armii Krajowej 17, 97-300 Piotrków Trybunalski, tel. 44 647 36 05, e-mail: liceum3@liceum3.piotrkow.pl
3	Użytkownik	Uczeń, Nauczyciel oraz Pracownik Administracji Placówki, który posiada imienne konto w O365 przypisane do wyłącznego użytku.
4	Dyrektor Placówki	Osoba zarządzająca placówką, odpowiedzialna za jej poprawne funkcjonowanie.
5	Domena internetowa albo domena	Unikalny adres, pod którym uruchomiono usługę O365 tu brzmiący: imie.nazwisko@liceum3pt.onmicrosoft.com
6	Identyfikator albo konto imienne albo konto	Utworzone dla każdego Użytkownika konto oraz hasło służące do logowania do O365. Po zalogowaniu się Użytkownik otrzymuje dostęp do danych oraz narzędzi O365.
7	Nieprawidłowość	Wszelkie odstępstwo od niniejszego regulaminu, naruszenie przepisów prawa, zaobserwowana anomalia. Nieprawidłowość winna być zgłoszona do Placówki telefonicznie lub pocztą elektroniczną.

§ 1 Postanowienia ogólne

2) Niniejszy regulamin określa zasady korzystania z O365 w szczególności w celu realizacji pracy i nauki zdalnej.

3) Usługa została wprowadzona jako jedyne narzędzie dla celów realizacji nauki i pracy zdalnej w Placówce.
4) Podstawą prawną dla podjęcia decyzji o użytkowaniu O365 jest:
   a) Rozporządzenie Ministra Edukacji Narodowej z dnia 20 marca 2020 r. w sprawie szczególnych rozwiązań w okresie czasowego ograniczenia funkcjonowania jednostek systemu oświaty w związku z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19.
   b) Rozporządzenie Ministra Edukacji Narodowej z dnia 20 marca 2020 r. zmieniające rozporządzenie w sprawie czasowego ograniczenia funkcjonowania jednostek systemu oświaty w związku z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19.
   c) Decyzja Dyrektora Placówki poprzedzona analizą dostępnych rozwiązań organizacyjnych i technicznych dla celów realizacji zdalnej nauki i pracy.
5) Wszelkie usługi dostarczane w ramach O365 świadczone są zgodnie z ustawą z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną.
6) Użytkownikami O365 są: uczniowie, nauczyciele oraz pracownicy administracyjni Placówki.
7) Korzystanie z O365 jest bezpłatne.
8) Zabrania się wykorzystywania O365 w celach zarobkowych.
9) Zabrania się wysyłania niechcianych informacji (SPAM-u) przy pomocy narzędzi udostępnianych w ramach Usługi.
10) Dostępność Usług jest bezpośrednio gwarantowana przez firmę Microsoft w ramach planu ciągłości działania. Placówka nie ponosi odpowiedzialności za brak dostępności Usług.
11) Każdy Użytkownik może posiadać tylko jedno Konto umożliwiające dostęp do Usług.

§ 2 Zakres świadczenia usług

1. Usługa dostarczana jest bezpłatnie przez firmę Microsoft w ramach zasobów udostępnianych przez tę firmę oraz zgodnie z regulaminem i zasadami określonymi przez firmę Microsoft.
2. Placówka wykorzystuje, zasila danymi, konfiguruje oraz utrzymuje usługi dostarczane przez firmę Microsoft.
3. Placówka dopuszcza do wykorzystania następujące narzędzia i usługi w ramach O365.

Lp.	Nazwa Narzędzia	Opis narzędzia
1	Microsoft Teams (Web oraz Desktop)	Komunikator wykorzystywany jako podstawowe narzędzie dla celów nauki zdalnej. Można go używać zamiennie dla poczty elektronicznej do przesyłania plików oraz wiadomości tekstowych w sposób bezpieczny.
2	Microsoft Outlook Web	**Poczta elektroniczna (Outlook wersja dostępna przez przeglądarkę, bez możliwości instalacji na komputerze użytkownika)** –poczta e-mail, kalendarz i kontakty w jednym miejscu, aplikacja ta silnie integruje się aplikacjami Office, aby zwiększyć wydajność oraz usprawnić współpracę.
3	Microsoft Word Web	**Microsoft Word Web (wersja dostępna przez przeglądarkę, bez możliwości instalacji na komputerze użytkownika)** – aplikacja będzie podstawowym narzędziem pracy każdego pracownika, dzięki niej można tworzyć dokumenty, dodawać tekst, grafikę, udostępniać dokumenty i współpracować z innymi osobami.
4	Microsoft Excel Web	**Microsoft Excel Web (wersja dostępna przez przeglądarkę, bez możliwości instalacji na komputerze użytkownika)** – arkusz kalkulacyjny, w znacznym stopniu ułatwia pracę na liczbach.
5	Microsoft PowerPoint Web	**Microsoft PowerPoint Web (wersja dostępna przez przeglądarkę, bez**

		możliwości instalacji na komputerze użytkownika) – program umożliwiający tworzenie prezentacji biznesowych, a także multimedialnych.
6	Microsoft Sharepoint	**Microsoft Sharepoint (wersja dostępna przez przeglądarkę, bez możliwości instalacji na komputerze użytkownika)** – narzędzie do udostępniania plików, danych, wiadomości i zasobów w celu ułatwienia dostępu do informacji pracownikom. Sharepoint umożliwia współdzielenie informacji, kontrolę wersji, stałe informowanie o następujących zmianach w publikowanych informacjach. Sharepoint może służyć jako Intranet, lokalna i wewnętrzna tablica ogłoszeń.
7	Microsoft OneDrive	**Microsoft OneDrive** – wirtualny dysk, dzięki któremu istnieje możliwość dostępu do danych z każdego miejsca podłączonego do Internetu.
8	Microsoft Forms	**Microsoft Forms** – aplikacja umożliwiająca realizowanie ankiet i testów w celu weryfikacji opinii i posiadanej wiedzy.

4. Pozostałe narzędzia O365 będą uruchamiane i dopuszczane sukcesywnie wraz ze wzrostem wiedzy, wymagań oraz potrzeb Użytkowników.

§ 3 Dostęp oraz użytkowanie usługi

1) Dostęp do O365 realizowany jest z użyciem przeglądarki Microsoft Edge oraz Google Chrome.
2) W przypadku wykorzystania usługi Teams oraz OneNote Użytkownik ma prawo zainstalować na własnym komputerze i korzystać z aplikacji typu desktop.
3) W celu realizowania czynności wynikających z niniejszego regulaminu Użytkownik musi być zalogowany na swoje konto.
4) Każdy Użytkownik posiada przypisane wyłącznie do niego imienne konto (Identyfikator) w O365, przeznaczone do celów pracy i nauki zdalnej oraz innych zadań wskazanych przez Dyrektora Placówki na mocy wydanych przez niego zarządzeń.
5) Dostęp do usług oraz narzędzi możliwy jest poprzez zalogowanie się Użytkownika po podaniu identyfikatora w witrynie https://office.com.
6) Każdemu Użytkownikowi przypisywany jest indywidualny adres e-mail o składni: imię.nazwisko@domena albo i.nazwisko@domena (pierwsza litera imienia i nazwisko).
7) Adresy e-mail są jawne. Każdy użytkownik może je swobodnie przekazywać w celu realizowania czynności wynikających z niniejszego regulaminu.
8) Zabronione jest podejmowanie jakichkolwiek czynności mających na celu obrażanie, umniejszanie wartości innych osób lub utrudnianie im bądź uniemożliwianie wykorzystywania O365.
9) Dostęp do usługi realizowany jest z wykorzystaniem funkcji dwuskładnikowego logowania.
10) W celu poszerzania wiedzy na temat O365 Placówka zaleca wykorzystanie publicznie dostępnych informacji pochodzących z wiarygodnych źródeł. Informacje na temat źródeł informacji Placówka będzie przekazywała sukcesywnie Użytkownikom.
11) Zabronione jest przekazywanie hasła do logowania do Usług (Konta) innemu użytkownikowi.

§ 4 Prawa, obowiązki i odpowiedzialność Użytkownika

1) Każdy użytkownik może wykorzystywać O365 w pełnym zakresie wskazanym w niniejszym Regulaminie przestrzegając przepisów prawa, obowiązujących norm społecznych, z zachowaniem dobrych obyczajów.
2) Każdy użytkownik jest uprawniony do wykorzystywania O365 i realizacji czynności opisanych w niniejszym regulaminie z użyciem sprzętu prywatnego ze szczególnym uwzględnieniem własnego komputera (w tym laptopa) oraz smartfona.

3) O365 można wykorzystywać wyłącznie, gdy system operacyjny komputera/smartfona/tabletu posiada bieżące wsparcie producenta.
4) Każdy Użytkownik zobowiązany jest do przestrzegania zasad netykiety https://pl.wikipedia.org/wiki/Netykieta oraz obowiązujących przepisów prawa
5) Każdy Użytkownik jest zobowiązany do zachowania poufności w zakresie udostępniania informacji przetwarzanych przez O365.
6) Każdy Użytkownik jest zobowiązany zgłaszać do Placówki wszelkie zidentyfikowane nieprawidłowości w Usłudze, telefonicznie na numer telefonu Placówki podany na stronach WWW albo pocztą elektroniczną, na adres e-mail Placówki.
7) Zabronione jest przekazywanie identyfikatora użytkownika innym użytkownikom. Wyjątek od tej reguły stanowi relacja opiekun prawny (rodzic) – uczeń, gdzie opiekun prawny powinien znać identyfikator ucznia.
8) Obowiązkiem Użytkownika jest zapisywanie wszelkich informacji przetwarzanych z użyciem O365 w OneDrive oraz Teams.
9) Użytkownik ponosi pełną odpowiedzialność za dane przetwarzane w ramach jego konta imiennego.
10) Użytkownik zobowiązany jest do zapewniania jak najlepszej ochrony danych przetwarzanych w ramach jego konta imiennego.
11) Każdy użytkownik winien zapoznać się i zrozumieć niniejszy Regulamin oraz:
    a) Załącznik nr 1 10 Zasad Użytkowania Haseł,
    b) Załącznik nr 2 10 Zasad Bezpieczeństwa,
    c) Załącznik nr 3 Lista czynności zabronionych,

    Które stanowią część niniejszego Regulaminu.

§ 5 Prawa, obowiązki i odpowiedzialność Placówki

1) Placówka zastrzega sobie prawo do komunikowania się z Użytkownikiem z wykorzystaniem adresu e-mail utworzonego w ramach O365.
2) Placówka ma prawo do zmiany zasad funkcjonowania O365 bez podania przyczyny i w każdym momencie, przy pomocy poczty elektronicznej.
3) Placówka zastrzega sobie prawo do:
    a) wprowadzania zmian w konfiguracji O365,
    b) rejestracji oraz wglądu do komunikacji Użytkownika prowadzonej z wykorzystaniem O365 ze szczególnym uwzględnieniem danych OneDrive, Teams oraz poczty elektronicznej,
    c) blokowania lub usuwania konta Użytkownika w przypadku, gdy przestanie on być Uczniem, Nauczycielem albo Pracownikiem Placówki,
    d) blokowania lub usuwania konta Użytkownika w przypadku naruszenia przez niego niniejszego Regulaminu albo obowiązujących przepisów prawa.
4) Placówka ma obowiązek dokładania wszelkich starań w zakresie utrzymania Usług oraz szerzenia wiedzy dotyczącej prawidłowego ich użytkowania.

§ 6 Bezpieczeństwo i Ochrona Danych Osobowych

1) Administratorem danych, w tym danych osobowych, przetwarzanych w ramach Usług jest Placówka reprezentowana przez Dyrektora.
2) Wszelkie informacje, w tym dane osobowe, są przetwarzane na podstawie:
    a) 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) dalej RODO,
        i) art. 6 ust. 1 lit. c na podstawie obowiązujących przepisów prawa,
        ii) art. 9 ust. 2 b czyli wypełnienia obowiązku, który ciąży na naszej Placówce.
    b) na postawie ustawy z 10 maja 2018 r. o ochronie danych osobowych,

c) rozporządzenia Ministra Edukacji Narodowej z dnia 20 marca 2020 r. w sprawie szczególnych rozwiązań w okresie czasowego ograniczenia funkcjonowania jednostek systemu oświaty w związku z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19,

d) rozporządzenia Ministra Edukacji Narodowej z dnia 20 marca 2020 r. zmieniające rozporządzenie w sprawie czasowego ograniczenia funkcjonowania jednostek systemu oświaty w związku z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19.

3) Dostęp do zarzadzania danymi posiadają osoby oraz podmioty upoważnione przez Administratora. Są to pracownicy Placówki oraz Inspektor Ochrony Danych. Microsoft Sp. z o.o. w Warszawie. Al. Jerozolimskie 195A 02-222 Warszawa jest podmiotem przetwarzającym dane osobowe.
4) Placówka dysponuje możliwościami zarządzania danymi Użytkownika oraz Usługami udostępnianymi przez firmę Microsoft.
5) Placówka przetwarza dane Użytkowników z poszanowaniem ich prywatności oraz obowiązujących przepisów prawa.
6) Każdy Użytkownik ma prawo:
   a) dostępu do treści swoich danych (art. 15 RODO),
   b) sprostowania (art. 16 RODO),
   c) ograniczenia przetwarzania (art. 18 RODO).

   Z tytułu nałożonego na ADO obowiązku prawnego dla przetwarzania ograniczone zostają prawa do:
   a) wniesienia sprzeciwu (art. 21 RODO),
   b) przenoszenia danych (art. 20 RODO),
   c) usunięcia danych (prawo do bycia zapomnianym) (art. 17 RODO).
1) W przypadku podejrzenia o niewłaściwym przetwarzaniu danych osobowych każda osoba może zgłosić skargę do Prezesa Urzędu Ochrony Danych Osobowych ul. Stawki 2, 00-193 Warszawa, tel. 22 531 03 00.
2) Dane osobowe oraz inne informacje przetwarzane w ramach usługi będą podlegały częściowemu profilowaniu oraz zautomatyzowanemu przetwarzaniu w celu analizy wyników oraz bieżących działań wykonywanych z użyciem Usługi.
3) Dane osobowe mogą być przetwarzane transgranicznie wyłącznie w sytuacjach nadzwyczajnych, np.: braku ciągłości działania i tylko w takim przypadku mogą być przesyłane poza obszar Unii Europejskiej.
4) Zgodnie z deklaracją firmy Microsoft wszystkie dane przetwarzane w ramach usługi znajdują się w obszarze Unii Europejskiej. Dane mogą być transferowane poza obszar Unii Europejskiej wyłącznie w uzasadnionych przypadkach.

§ 6 Postanowienia końcowe

1) Wszelkie uwagi, prośby, komentarze można zgłaszać do Dyrekcji Placówki pocztą elektroniczną na adres e-mail Placówki, listownie na adres tradycyjny Placówki albo osobiście w Sekretariacie. Zgłoszenie winno zawierać Imię, Nazwisko osoby zgłaszającej oraz opis merytoryczny zgłoszenia.
2) Odpowiedzi na zgłoszenia będą udzielane tą samą drogą, którą wpłynęły.
3) Kwestie sporne, które nie zostały ujęte w niniejszym Regulaminie będą rozstrzygane przez Dyrektora i/lub osoby przez niego upoważnione.
4) W sprawach nieuregulowanych niniejszym Regulaminem zastosowanie mają obowiązujące przepisy prawa.
5) Regulamin wchodzi w życie z dniem 1 września 2020 r.

Podpis Dyrektora

Załącznik nr 1 10 Zasad Użytkowania Haseł

1) Nie podawaj nikomu swojego hasła

Hasło jest Twoją własnością i nikomu go nie ujawniaj. Nie wysyłaj haseł mailem lub SMS-em (wyjątek stanowią hasła jednorazowe, ale nie wysyłaj ich w tej samej wiadomości wraz treścią).

2) Stosuj niestandardowe zdania jako hasła

Stosuj normalne, ale nieszablonowe, zdania złożone z kilku, np.: 5 wyrazów (passphrase), bo łatwiej je zapamiętać niż złożone hasła (password), a skuteczność ochrony wzrasta wraz z ilością zastosowanych znaków. Niech zdania-hasła będą nieszablonowe, np.: „Al1cja wcale nie ma p@pugi" (ilość znaków ze spacjami 26) albo „_Nie-znoszę trudnych h@seł" (ilość znaków ze spacjami 27).

3) Stosuj różne hasła

Dla każdego systemu informatycznego hasła powinny być różne. Stosowanie w wielu systemach tego samego hasła zdecydowanie podnosi prawdopodobieństwo jego ujawnienia.

4) Komplikuj zapis hasła

Zamiast litery „A" i „a" stosuj znak „@" (małpa); zamiast „E" i „e" stosuj cyfrę 3; zamiast litery „l" i „i" stosuj cyfrę 1; zamiast litery „L" i „l" stosuj znak „!" (wykrzyknik). Stosuj znaki specjalne: @#{]|%^&* i inne.

5) Stosuj menadżera haseł

W celu zapanowania nad hasłami stosuj menadżera haseł, czyli oprogramowanie, które zapamiętuje Twoje hasła i umożliwia ich stosowanie bezpośrednio w różnych systemach. Zalecanym menadżerem haseł jest KeePass, ponieważ jest rozwijany przez społeczność międzynarodową, najlepiej przetestowany, stabilnie rozwijany. Można go ściągnąć ze strony (https://keepass.info/).

6) Zmieniaj hasło minimum co 90 dni

W przypadku zastosowania 20 znakowego hasła (zdania zamiast hasła) nie ma potrzeby zmiany hasła co 30 dni. Zmiana co 90 dni (4 razy w roku) wystarczy dla zachowania bezpieczeństwa informacji.

7) Zmień hasło natychmiast po wykrytym naruszeniu

Jeżeli dowiesz się o naruszeniu haseł, np.: z prasy, radia, telewizji, od innej osoby lub podejrzewasz, że mogło do tego naruszenia dojść, natychmiast zmień hasła do systemów, których naruszenie dotyczy.

8) Nie zapisuj haseł w przeglądarce internetowej

NIGDY NIE ZAPAMIĘTUJ (ZAPISUJ) HASEŁ W PRZEGLĄDARCE INTERNETOWEJ. Bez logowania każdy może wejść na Twoje konto uzyskując dostęp do komputera.

9) Nie korzystaj z nieznanego sprzętu oraz nieznanego Wi-Fi

Nie wykorzystuj, w celu logowania się do systemów chronionych Twoim hasłem, nieznanego komputera lub smartfonu przypadkowej osoby, ponieważ możesz to hasło pozostawić zapisane na tym urządzeniu. Nieznane sieci bezprzewodowe mogą rejestrować wszystkie wpisywane przez Ciebie hasła.

10) Nie podawaj hasła Policji, Bankowi, sklepowi internetowemu

Hasło należy do Ciebie i żadna odpowiedzialna organizacja nie będzie prosić o jego podanie. Jeżeli ktoś prosi o podanie hasła w wiadomości e-mail, SMS to na pewno jest próba jego wyłudzenia.

Załącznik nr 2 10 Zasad Bezpieczeństwa

1) Podnoszenie świadomości

Uczyń swoim obowiązkiem podnoszenie świadomości wśród znajomych osób. Zawsze zakładaj, że inni wiedzą mniej o RODO i ochronie informacji.

2) Ogranicz fizyczny dostęp do informacji

Jeżeli Twoja szafa ma zamek, zamykaj ją. Jeśli szafa nie ma zamka, przemyśl czy powinien zostać zamontowany. Jeżeli wykorzystujesz szafki z zamkami i bez, przełóż dokumenty wymagające lepszej ochrony do szafek zamykanych na klucz. Nie pokazuj osobom nieuprawnionym danych osobowych. Nie zostawiaj gości lub osób postronnych bez opieki.

Jeżeli współużytkujesz komputer z innymi osobami załóż na nim konto do własnego użytku oraz zaszyfruj dane za pomocą oprogramowania tj. np.: Veracrypt albo Cryptomator.

3) Wiedz, jakie dane przechowujesz (przetwarzasz)

Przechowywanie to przetwarzanie, posiadanie to również przetwarzanie. Musisz wiedzieć jakie dane przechowujesz na swoim komputerze, pendrivie, telefonie, dysku sieciowym lub w chmurze. Musisz również wiedzieć, dlaczego je przechowujesz, skąd je masz, jak długo możesz je mieć i czy możesz je mieć, czy pozwala Ci na to prawo, Twój przełożony lub Klient. Zastanów się czy musisz mieć dostęp do danych, które Ci udostępniono.

4) Utrzymuj porządek

Usuń dane (pliki Word, Excel, PDF i inne, zbędne maile), które zawierają dane osobowe i inne wartościowe informacje, których nie potrzebujesz. Ustalaj najniższe możliwe uprawnienia do danych, usług, pomieszczeń, systemów informatycznych. Pamiętaj, że mniej znaczy więcej i lepiej zgodnie z zasadą minimalizacji

5) Pytaj, jeśli czegoś nie wiesz

Jeżeli nie wiesz lub nie jesteś pewien zapytaj innych, może Ci pomogą szczególnie w przypadku niepewnych maili lub nieznanych plików.

6) Świadomie używaj urządzeń komputerowych

Wykorzystuj wszystkie urządzenia służące do przetwarzania danych, szczególnie prywatne urządzenia do celów służbowych, świadomie. Nie konfiguruj konta poczty elektronicznej Twojej organizacji na smartfonie i/lub komputerze, z którego korzysta Twoje dziecko. Nie zostawiaj tych urządzeń bez nadzoru. Nie używaj nieznanych sieci Wi-Fi.

7) Szyfruj dane

Dowiedz się jak szyfrować dane i zaszyfruj swój smartfon oraz komputer przenośny. Jeżeli je zgubisz lub zostaną Ci skradzione, nikt nie będzie mógł odczytać tych danych. Szyfruj dane przesyłane mailem w załączniku i nie przesyłaj danych osobowych w treści wiadomości.

8) Nie otwieraj nieznanych treści i nie podłączaj nieznanych pendrive'ów

Jeżeli nie wiesz co jest na wymiennym nośniku lub przenośnym urządzeniu lub w mailu nie podłączaj go do komputera. To uchroni Cię przed działaniem złośliwego oprogramowania.

9) Nie włączaj makr w oprogramowaniu biurowym

Makro to program, który bywa dołączany do plików pakietu biurowego (Microsoft Office). Taki program może uszkodzić lub/i wykraść informacje, o ile ktoś go napisał w złej intencji. Nie uruchamiaj go.

10) Aktualizuj oprogramowanie

Pamiętaj, aby zawsze mieć aktualne oprogramowanie. To umożliwi załatanie istniejących dziur i utrudni wyciek danych.

Załącznik nr 3 Lista czynności zabronionych

1) Co nie jest dozwolone jest zabronione

Jest to zasada przewodnia, która zabrania wykonywania czynności, wykorzystywania środków oraz stosowania zaleceń, które nie są jawnie dozwolone. Jeżeli masz wątpliwości co jest dozwolone a co nie zapytaj w Placówce.

2) Nigdy nie podawaj hasła

Twoje hasła należą wyłącznie do Ciebie, nie podawaj ich nikomu.

3) Nie wysyłaj niezaszyfrowanych danych osobowych

Nie wysyłaj danych osobowych oraz innych ważnych informacji w postaci niezaszyfrowanej. W ogóle ogranicz wysyłanie danych osobowych do minimum.

4) Nie zostawiaj odblokowanego ekranu komputera

Niezablokowany ekran umożliwia skorzystanie z komputera w dowolny sposób. Wygaszacz ekranu powinien wymuszać podanie hasła po jego uruchomieniu.

5) Nie zapisuj haseł

Nie zapisuj haseł na karteczkach, które trzymasz w zamkniętej szafie (chyba, że to sejf i hasła mają charakter masterpassword). Do celu bezpiecznego przechowywania haseł używaj menadżera haseł KeePass (https://keepass.info/).

6) Nie uruchamiaj nieznanego oprogramowania

Jeżeli ktoś prosi Cię o uruchomienie oprogramowania, którego nie znasz nie rób tego. Prośba może być wyrażona mailem, osobiście lub telefonicznej.

Nie instaluj nieznanego oprogramowania na swoim smartfonie, bo może ono spowodować wyciek danych. Najlepiej ogranicz listę aplikacji do minimum.

7) Nie wykorzystuj nieznanych nośników wymiennych (pendrive lub płyta CD)

Nie podłączaj do komputera nośników znalezionych na ulicy lub otrzymanych od znajomego, bo mogą zawierać szkodliwe oprogramowanie.

8) Nie uruchamiaj programów typu MAKRO (MACRO)

Makro stanowi integralną część plików oprogramowania biurowego (Microsoft Office, Libre Office), ale jednocześnie najczęściej jest powodem wycieku danych. Jeżeli Word, Excel, Power Point ostrzegają przed uruchomieniem makro, nie rób tego.

9) Nie polegaj całkowicie na innych

Twoje bezpieczeństwo to Twoje zadanie. Inspektor Ochrony Danych, Administrator Danych Osobowych, Nauczyciel, Rodzic, Kolega albo Koleżanka zawsze pomogą, ale nie będzie ich z Tobą cały czas.