Moduły szkoleń w projekcie pt. „E-URZĘDNIK”

Temat: 1 Tworzenie i zarządzanie cyfrowymi dokumentami

Zajęcia zostaną poświęcone efektywnemu tworzeniu dokumentów cyfrowych z uwzględnieniem zasady prostego języka, oraz zarządzaniu nimi. Wiedza ta jest kluczowa z uwagi na rosnącą liczbę procedur administracyjnych realizowanych elektronicznie oraz potrzebę zapewnienia dostępności usług dla wszystkich użytkowników, w tym osób z niepełnosprawnościami.

Czas trwania: 7 x 60 min szkolenie online, 7 x 60 min szkolenie stacjonarne

Cele:

- Wykształcenie umiejętności efektywnego tworzenia i zarządzania dokumentami w formacie cyfrowym, w tym korzystanie z narzędzi biurowych i specjalistycznych aplikacji umożliwiających tworzenie dokumentów dostępnych i zgodnych z zasadami prostego języka.
- Wykształcenie umiejętności stosowania zasad higieny cyfrowej w codziennym życiu

Zagadnienia:

1. Rodzaje dokumentów

- Dokumenty tekstowe,
- Dokumenty PDF,
- Dokumenty prezentacyjne,
- Arkusze kalkulacyjne,
- Dokumenty graficzne,

2. Narzędzia do tworzenia dokumentów:

- Microsoft Office (Word, Excel, PowerPoint) – Jedno z najczęściej używanych narzędzi do tworzenia i edytowania dokumentów, arkuszy kalkulacyjnych, prezentacji.
- Google Workspace (Docs, Sheets, Slides) – Narzędzia do tworzenia dokumentów online z możliwością współpracy w czasie rzeczywistym.
- LibreOffice/OpenOffice – Bezpłatne oprogramowanie open-source do edytowania dokumentów, arkuszy kalkulacyjnych i prezentacji.
- Canva – Narzędzie do tworzenia graficznych dokumentów, prezentacji i materiałów marketingowych.

3. Narzędzia do tworzenia i edytowania multimediów:

- Obrazy: GIMP: Canva: Narzędzie online do projektowania grafik, plakatów, postów na media społecznościowe.
- Wideo: DaVinci Resolve: Darmowe oprogramowanie do edycji wideo i postprodukcji. Filmora: Łatwe w użyciu oprogramowanie do edycji wideo, które oferuje prostą obsługę. Beecut.
- Audio: Audacity: Darmowe oprogramowanie do nagrywania i edycji dźwięku.
- Animacje: Blender: Oprogramowanie open-source do tworzenia animacji 3D.

4. Platformy do publikowania i dystrybucji multimediów:

- YouTube: Platforma do udostępniania wideo.
- Vimeo: Alternatywa dla YouTube, skierowana do profesjonalistów.
- SoundCloud: Platforma do publikowania i dzielenia się plikami audio.
- Instagram, TikTok: Platformy społecznościowe do publikacji obrazów i filmów.

5. Elektroniczne formularze:

- Narzędzia pozwalające na elektroniczne składanie wniosków i formularzy przez obywateli, które są natychmiastowo przekazywane do odpowiednich urzędów.

6. Organizacja i przechowywanie dokumentów:

- Systemy zarządzania dokumentami (DMS): Systemy takie jak SharePoint, Google Workspace czy Microsoft OneDrive umożliwiają przechowywanie, organizowanie i współdzielenie dokumentów w sposób bezpieczny i uporządkowany.
- Cloud Computing: Usługi chmurowe takie jak Google Drive, Dropbox, OneDrive oferują przestrzeń do przechowywania dokumentów online, z dostępem z dowolnego miejsca.
- Struktura folderów: Ważne jest, aby dokumenty były przechowywane w logicznych folderach, ułatwiających późniejsze wyszukiwanie i dostęp.

7. Zarządzanie wersjami:

- W przypadku współpracy nad dokumentami istotne jest śledzenie różnych wersji i zmian. Większość narzędzi do edytowania dokumentów cyfrowych, takich jak Google Docs czy Microsoft Word, oferuje funkcję historii wersji, pozwalającą na przywracanie wcześniejszych edycji dokumentu.

8. Bezpieczeństwo dokumentów:

- Szyfrowanie: Ochrona dokumentów przed nieautoryzowanym dostępem jest kluczowa, szczególnie w przypadku wrażliwych informacji. Dokumenty mogą być szyfrowane zarówno na etapie przechowywania, jak i przesyłania.

- Zarządzanie dostępem: Współczesne systemy umożliwiają nadawanie różnych poziomów dostępu do dokumentów, co pozwala na kontrolowanie, kto może je edytować, przeglądać lub udostępniać.
- Podpisy elektroniczne: Wiele systemów umożliwia dodawanie podpisów elektronicznych, co jest niezbędne w kontekście podpisywania dokumentów formalnych w sposób zgodny z przepisami prawa.
- Backupy: Regularne tworzenie kopii zapasowych dokumentów jest kluczowe, aby zabezpieczyć dane przed ich utratą. Można to robić na nośnikach fizycznych lub w chmurze.

9. Edycja i współpraca nad dokumentami:

- Współpraca w czasie rzeczywistym: Narzędzia takie jak Google Docs, Microsoft 365, Notion czy Slack umożliwiają jednoczesną edycję dokumentów przez wielu użytkowników.
  Komentarze i śledzenie zmian: Funkcje komentarzy i śledzenia zmian w dokumentach umożliwiają łatwe zarządzanie procesem redakcyjnym i współpracę nad dokumentami w zespole.

10. Udostępnianie i dystrybucja dokumentów:

- Dokumenty cyfrowe mogą być łatwo udostępniane za pomocą e-maila, linków do plików w chmurze lub przez systemy zarządzania dokumentami.
- Istnieją również narzędzia umożliwiające publikowanie dokumentów na stronach internetowych lub platformach intranetowych.

11. Archiwizacja dokumentów:

- Archiwizacja: Przechowywanie dokumentów w sposób, który umożliwia ich długoterminowy dostęp, ale także przestrzega przepisów prawnych dotyczących przechowywania danych. Wymaga to uporządkowanego systemu i przestrzegania przepisów RODO lub innych regulacji.
- Usuwanie dokumentów: Ważne jest, aby po upływie określonego czasu usunąć dokumenty, które już nie są potrzebne, w sposób bezpieczny, aby uniknąć nieautoryzowanego dostępu.

12. Zgodność z przepisami i standardami:

- Wiele branż wymaga, by dokumenty cyfrowe były zgodne z określonymi standardami i przepisami prawnymi. Na przykład, w sektorze publicznym w Polsce istnieją wymogi związane z przechowywaniem dokumentów elektronicznych, zgodność z normami eIDAS dla podpisów elektronicznych oraz przepisy dotyczące ochrony danych osobowych (RODO).

13. Automatyzacja procesów związanych z dokumentami:

- OCR (Optical Character Recognition): Narzędzia do rozpoznawania tekstu w dokumentach skanowanych lub obrazach mogą pomóc w digitalizacji i organizowaniu fizycznych dokumentów.
- Workflow automation: Automatyzacja obiegu dokumentów, np. za pomocą platform takich jak DocuSign czy Trello, pomaga zautomatyzować procesy zatwierdzania, podpisywania i archiwizowania dokumentów.

14. Skanowanie dokumentów papierowych:

- Skanowanie dokumentów to proces przekształcania dokumentów papierowych w pliki cyfrowe za pomocą skanerów, które zapisują je w formatach takich jak JPEG, PNG, TIFF lub PDF. Skanowane dokumenty mogą być później przechowywane, udostępniane i przetwarzane w formie cyfrowej.

15. Dobre nawyki cyfrowe:

- Stosowanie zasad higieny cyfrowej w codziennej pracy

Korzyści dla uczestnika/uczestniczki:

Po zakończeniu szkolenia uczestnik/uczestniczka nabędzie praktyczne umiejętności w zakresie:

- Zwiększenia efektywności pracy
- Szybszego przetwarzania dokumentów
- Redukcji czasu na obieg dokumentów
- Oszczędności kosztów
- Zwiększenie bezpieczeństwa danych
- Ułatwienia dostępu do dokumentów
- Poprawy współpracy i komunikacji
- Ułatwienia archiwizacji i przestrzegania przepisów prawnych
- Zwiększenia przejrzystości i dostępności
- Transparentności działań administracji
- Łatwiejszego dostęp do informacji
- Łatwiejszej integracji z innymi systemami
- Stosowania higieny cyfrowej w codziennej pracy

Temat 2: Narzędzia e-administracji i e-usługi

Szkolenie obejmuje praktyczne zastosowanie narzędzi cyfrowych dostępnych w polskiej administracji, takich jak e-Puap, mObywatel, czy profil zaufany. Ten blok tematyczny

odpowiada na zapotrzebowanie urzędów na zwiększenie efektywności obsługi mieszkańców oraz dostępności usług publicznych.

Czas trwania: 7×60 min szkolenie online, 7×60 min szkolenie stacjonarne

Cele:

- Wykształcenie umiejętności praktycznego zastosowanie narzędzi cyfrowych dostępnych w polskiej administracji, takich jak e-Puap, mObywatel, czy profil zaufany.
- Wykształcenie umiejętności stosowania zasad higieny cyfrowej w codziennym życiu

Zagadnienia:

1. ePUAP (Elektroniczna Platforma Usług Administracji Publicznej)

- Składanie wniosków i pism elektronicznych do administracji publicznej.
- Dostęp do formularzy i deklaracji podatkowych, takich jak PIT.
- Możliwość podpisania dokumentów elektronicznych przy użyciu Profilu Zaufanego lub kwalifikowanego podpisu elektronicznego.
- Usługi dostępne dla obywateli, przedsiębiorców oraz instytucji publicznych.

2. Profil Zaufany (PZ)

- Umożliwia logowanie się do systemów administracji publicznej, takich jak ePUAP, ZUS, czy portal podatkowy.
- Możliwość składania podpisów elektronicznych w systemach rządowych i samorządowych.
- Bezpłatna rejestracja przez bankowość internetową lub w punkcie potwierdzającym.

3. e-Dowód

- Zawiera certyfikaty, które pozwalają na elektroniczne podpisywanie dokumentów
- Dostęp do usług publicznych (np. e-recepty, e-zwolnienia).
- Wspiera załatwianie spraw urzędowych bez konieczności osobistego stawiania się w urzędach.

4. e-ZUS

- Składanie deklaracji ubezpieczeniowych i ZUS DRA.
- Możliwość sprawdzenia stanu konta emerytalnego i historii składek.
- Wysyłanie dokumentów do ZUS online (np. wnioski o świadczenia).
- Wgląd w informacje o ubezpieczeniach zdrowotnych i emerytalnych.

5. e-Recepta

- Wystawianie i odbieranie e-recepty przez pacjentów.
- Możliwość realizacji recept w aptekach bez konieczności posiadania papierowej wersji.
- Ułatwia dostęp do leków i monitorowanie historii leczenia.

6. e-PIT (Elektroniczny Podatek dochodowy)

- Automatyczne wypełnianie formularzy PIT na podstawie danych od pracodawców oraz instytucji finansowych.
- Możliwość zatwierdzenia i wysłania PIT online bez konieczności wychodzenia z domu.
- Bezpieczne składanie deklaracji, z możliwością rozliczenia podatku lub uzyskania zwrotu.

7. Centralny Rejestr Elektronicznych Faktur (CRF)

- Wysyłanie faktur VAT w formie elektronicznej, zgodnie z wymogami polskiego prawa.
- Automatyczne przesyłanie faktur do administracji skarbowej w celu weryfikacji i archiwizacji.
- Zgodność z ustawą o VAT w zakresie przesyłania e-faktur.

8. System PESEL

- Wykorzystywany do identyfikacji obywateli w systemach administracji publicznej.
- Służy do wydawania dokumentów tożsamości, takich jak dowód osobisty.
- Wspiera administrację w procesie wydawania decyzji administracyjnych i realizacji e-usług.

9. Gov.pl – Portal usług publicznych

- Dostarczanie informacji o dostępnych usługach administracyjnych.
- Dostęp do formularzy, wniosków i instrukcji dotyczących załatwiania spraw urzędowych online.
- Możliwość logowania się do różnych systemów administracji publicznej za pomocą Profilu Zaufanego lub e-dowodu.

10. Bankowość elektroniczna i e-administracja

- Umożliwia opłacanie różnych zobowiązań finansowych bezpośrednio z poziomu portali administracyjnych.
- Przesyłanie potwierdzeń płatności do odpowiednich urzędów.
- Integracja z systemami rządowymi, takimi jak portal podatkowy.

11. e-WUŚ (Elektroniczna Weryfikacja Uprawnień Świadczeniobiorcy)

- Sprawdzanie statusu ubezpieczenia zdrowotnego pacjenta w systemie NFZ.

- Weryfikacja, czy osoba ma prawo do świadczeń zdrowotnych w ramach ubezpieczenia.
- Automatyczne przesyłanie zapytań do NFZ o uprawnienia pacjenta.

12. e-KRS (Elektroniczny Krajowy Rejestr Sądowy)

- Rejestracja nowych podmiotów gospodarczych oraz zmian w istniejących firmach.
- Weryfikacja danych firm i organizacji, takich jak dane kontaktowe, przedstawiciele prawni itp.
- Dostęp do publicznych informacji o zarejestrowanych podmiotach.

13. Dobre nawyki cyfrowe

- Stosowanie zasad higieny cyfrowej w codziennej pracy

Korzyści dla uczestnika/uczestniczki:

Po zakończeniu szkolenia uczestnik/uczestniczka nabędzie praktyczne umiejętności w zakresie:

- Zwiększenia kompetencji cyfrowych: Szkolenie pozwoli na zdobycie lub pogłębienie umiejętności korzystania z nowoczesnych platform cyfrowych, które są kluczowe w codziennej pracy urzędniczej.
- Usprawnienia procesów administracyjnych: Nauka efektywnego wykorzystania narzędzi takich jak e-Puap czy mObywatel pozwoli na szybsze załatwianie spraw obywateli, co przekłada się na wzrost zadowolenia mieszkańców.
- Zabezpieczania danych osobowych
- Rozumienia funkcjonowania i zarządzania e-usługami
- Zmniejszenia błędów proceduralnych
- Szybkiego reagowania na zmiany w przepisach
- Efektywne zarządzanie czasem pracy.
- Stosowania higieny cyfrowej w codziennej pracy

Temat 3: Zarządzanie danymi i analiza danych

Umiejętności efektywnego zarządzania danymi i otwierania danych (open data) jest niezbędna dla poprawy jakości usług publicznych oraz zwiększenia transparentności działań administracji.

Czas trwania: 7 x 60 min. szkolenie online, 7 x 60 min. szkolenie stacjonarne

Cele:

- Wykształcenie umiejętności przetwarzania i analizowania danych w sposób, który wspiera decyzje strategiczne i operacyjne urzędów.
- Wykształcenie umiejętności stosowania zasad higieny cyfrowej w codziennym życiu

Zagadnienia:

1. Cechy danych otwartych:

- Dostępność: Muszą być dostępne w sposób bezpłatny i bezbarierowy.
- Przejrzystość: Dane muszą być opublikowane w sposób przejrzysty i zrozumiały, aby mogły być wykorzystywane przez jak najszersze grono użytkowników.
- Ponowne wykorzystanie: Dane mogą być używane w dowolny sposób, zarówno komercyjnie, jak i niekomercyjnie.
- Formaty: Dane otwarte są publikowane w otwartych formatach (np. CSV, JSON, XML, GeoJSON), które można łatwo analizować i przetwarzać.
- Licencja: Wiele zbiorów danych otwartych jest udostępnianych na licencjach, które zezwalają na ich dowolne wykorzystywanie, np. Creative Commons.

2. Przykłady danych otwartych:

- Dane rządowe: Statystyki gospodarcze, dane o zdrowiu publicznym, dane meteorologiczne, dane z ewidencji ludności.
- Dane o transporcie: Rozkłady jazdy, dane o ruchu drogowym, dane o trasach lotniczych, dane o stanie dróg.
- Dane geograficzne: Mapy, dane GIS (Geographic Information Systems), dane o powierzchni gruntów, dane o terenie.
- Dane o edukacji: Dane o szkołach, kursach, programach nauczania, wynikach matur.
- Dane o środowisku: Dane o jakości powietrza, poziomach zanieczyszczenia wody, dane o bioróżnorodności.

3. Zarządzanie danymi otwartymi (Open Data Management)

- Publikacja danych, Platformy Open Data: Wiele rządów i organizacji udostępnia dane otwarte za pośrednictwem dedykowanych platform, takich jak data.gov.pl w Polsce, data.gov w USA, EU Open Data Portal w Unii Europejskiej, World Bank Open Data.
- Formaty danych: Udostępnianie danych w otwartych, znormalizowanych formatach (np. CSV, JSON, GeoJSON), które umożliwiają ich łatwe pobieranie i przetwarzanie.
- Zbieranie danych: Urzędnicy często zbierają dane poprzez formularze, wnioski, ankiety, a także systemy informatyczne. Ważne jest, aby dane były zbierane w sposób zgodny z obowiązującymi przepisami prawa (np. RODO w Unii Europejskiej).
- Przechowywanie danych: Dane muszą być przechowywane w sposób bezpieczny, z zachowaniem poufności, integralności i dostępności. Systemy informacyjne muszą być odpowiednio zabezpieczone przed nieautoryzowanym dostępem.
- Udostępnianie danych: Urzędnicy muszą zapewnić, aby dane były dostępne dla innych pracowników administracji publicznej, a także dla obywateli, o ile jest to zgodne z przepisami prawa. Przykładem może być udostępnianie danych publicznych na portalach ePUAP czy BIP (Biuletyn Informacji Publicznej).

4. Analiza danych otwartych (Open Data Analytics)

Eksploracja danych (Data Exploration):

- Tworzenia raportów: Na podstawie danych urzędnicy opracowują raporty, które są następnie wykorzystywane przez decydentów, np. w przypadku oceny skutków polityki publicznej.
- Prognozowania: Analiza danych może również dotyczyć prognozowania, np. przewidywania liczby obywateli korzystających z usług publicznych, które mogą wpłynąć na planowanie zasobów lub rozwoju infrastruktury.
- Analiza statystyczna: Urzędnicy często korzystają z narzędzi takich jak Excel, Power BI, R, Python lub specjalistyczne oprogramowanie do analizy danych w celu obliczania wskaźników, wykresów i analiz statystycznych. Dzięki temu możliwe jest wyciąganie wniosków dotyczących np. trendów społecznych, demograficznych, gospodarczych.

Wizualizacja danych:

- Mapy i wykresy: Wizualizacja danych geograficznych, jak i liczbowych za pomocą wykresów i map.

5. Bezpieczeństwo danych

Szyfrowanie danych

- Zabezpieczenie dostępu (autoryzacja i autentykacja)

6. Przykłady zastosowań

- Ewidencja ludności i inne rejestry publiczne: Urzędnicy odpowiedzialni za utrzymywanie ewidencji ludności muszą zarządzać ogromnymi zbiorami danych, które są następnie wykorzystywane do planowania polityki publicznej, organizowania wyborów, czy wnioskowania o świadczenia socjalne.
- Analiza budżetu: W przypadku budżetu państwowego lub samorządowego, analiza danych pozwala na monitorowanie wydatków i przychodów, identyfikowanie oszczędności lub obszarów wymagających dodatkowych inwestycji.
- Zarządzanie kryzysowe: W sytuacjach kryzysowych, takich jak pandemie, urzędnicy wykorzystują dane z różnych źródeł (np. dane medyczne, dane o mobilności ludności) w celu podejmowania decyzji w sprawie ograniczeń czy dystrybucji zasobów.

7. Dobre nawyki cyfrowe

- Stosowanie zasad higieny cyfrowej w codziennej pracy

Korzyści dla uczestnika/uczestniczki:

Po zakończeniu szkolenia uczestnik/uczestniczka nabędzie praktyczne umiejętności w zakresie:

- Lepszego podejmowania decyzji
- Lepszej jakość usług publicznych
- Zwiększenia przejrzystości i odpowiedzialności
- Lepszego zarządzanie zasobami

- Wspierania innowacji i reform
- Lepszej współpracy i wymiany informacji
- Zwiększenia satysfakcji obywateli
- Umiejętności analitycznych
- Wykorzystania nowoczesnych narzędzi
- Stosowania higieny cyfrowej w codziennej pracy

Temat 4: Cyberbezpieczeństwo i ochrona danych

Temat wynika bezpośrednio z narastającej liczby ataków cyfrowych, które mogą paraliżować działanie instytucji publicznych i narażać na szwank wizerunek i bezpieczeństwo państwa oraz jego obywateli.

Czas trwania: 7 x 60 min szkolenie online, 7 x 60 min szkolenie stacjonarne

Cele:

- Zapoznanie uczestników z aspektami przestrzegania prawa i zasad bezpieczeństwa w sieci. Respektowanie prywatności informacji i ochrony danych, praw własności intelektualnej, etykiety w komunikacji i norm współżycia społecznego.
- Ocena zagrożeń związanych z technologią i ich uwzględnienie dla bezpieczeństwa swojego i innych.
- Wykształcenie umiejętności stosowania zasad higieny cyfrowej w codziennym życiu

Zagadnienia:

1. Zabezpieczenie sieci:

- Zapory ogniowe (firewalle): Blokują nieautoryzowany dostęp do sieci, filtrując ruch przychodzący i wychodzący.
- Wirtualne sieci prywatne (VPN): Tworzą bezpieczne połączenie między użytkownikami a siecią, zapewniając prywatność przesyłanych danych.
- Systemy wykrywania i zapobiegania włamaniom (IDS/IPS): Monitorują sieć w celu wykrycia prób nieautoryzowanego dostępu lub innych podejrzanych aktywności.

2. Ochrona urządzeń i systemów:

- Antywirusy: Programy, które wykrywają i neutralizują złośliwe oprogramowanie (wirusy, trojany, ransomware, spyware).
- Zarządzanie łatanie oprogramowania: Regularne aktualizowanie systemów operacyjnych i aplikacji, aby zabezpieczyć je przed znanymi lukami bezpieczeństwa.

3. Zarządzanie tożsamościami:

- Single Sign-On (SSO): Umożliwia użytkownikom logowanie się do wielu systemów za pomocą jednej pary poświadczeń, zmniejszając ryzyko związane z zarządzaniem hasłami.

4. Tworzenie silnych i unikalnych haseł:

- Silne hasło: Hasło powinno składać się z co najmniej 12 znaków, zawierać małe i wielkie litery, cyfry oraz znaki specjalne.
- Unikalne hasło dla każdego konta: Używanie tego samego hasła do wielu kont stwarza poważne ryzyko w przypadku wycieku danych. Warto korzystać z menedżerów haseł, które pomagają przechowywać silne i unikalne hasła dla różnych kont.

5. Używanie uwierzytelniania wieloskładnikowego (MFA):

- MFA to technika zabezpieczająca, która wymaga dwóch lub więcej metod weryfikacji tożsamości użytkownika, np. hasła i kodu wysłanego na telefon lub aplikację. Używanie MFA znacznie zwiększa bezpieczeństwo nawet w przypadku kradzieży hasła.

6. Aktualizacja oprogramowania:

- Regularne aktualizowanie systemów operacyjnych, aplikacji oraz oprogramowania antywirusowego jest kluczowe w zabezpieczeniu przed nowymi zagrożeniami. Producenci oprogramowania często wydają poprawki (tzw. „łatki"), które zamykają luki bezpieczeństwa.

7. Szyfrowanie danych:

- Szyfrowanie w ruchu (np. HTTPS na stronach internetowych) i szyfrowanie danych w spoczynku (np. na urządzeniach, w chmurze) zapewniają, że dane są chronione przed nieautoryzowanym dostępem, nawet jeśli ktoś przechwyci je w trakcie transmisji lub uzyska dostęp do przechowywanych plików.

8. Zarządzanie prywatnością w Internecie:

- Kontrola prywatności na stronach internetowych: Regularne sprawdzanie ustawień prywatności na swoich profilach w mediach społecznościowych oraz na innych stronach, aby ograniczyć dostęp do swoich danych osobowych.
- Używanie pseudonimów: Warto rozważyć używanie pseudonimów lub aliasów zamiast swoich prawdziwych danych w sieci, szczególnie w mniej wiarygodnych miejscach (np. forach internetowych).

9. Unikanie podejrzanych linków i załączników:

- Phishing to popularna metoda oszustwa, w której atakujący podszywają się pod wiarygodne źródła (np. banki, instytucje rządowe) w celu wyłudzenia danych osobowych lub pieniędzy.
- Załączniki: załączniki od nieznanych nadawców mogą zawierać złośliwe oprogramowanie (np. wirusy, ransomware).

10. Bezpieczne korzystanie z publicznych sieci Wi-Fi:

- Logowanie do kont wrażliwych (np. bankowych) w publicznych sieciach Wi-Fi.

11. Regularne tworzenie kopii zapasowych danych:

- Backup: Regularne tworzenie kopii zapasowych danych, szczególnie ważnych plików, pomaga uniknąć utraty danych w przypadku awarii systemu, ataku ransomware lub innych incydentów.

12. Uważność na aplikacje i uprawnienia:

- Zezwalanie na uprawnienia: dostęp do danych, zwłaszcza do lokalizacji, zdjęć, kontaktów czy mikrofonu, uprawnienia wymagane przez aplikacje.
- Aplikacje z nieznanych źródeł: Pobieranie aplikacji tylko z oficjalnych sklepów (Google Play, Apple App Store).

13. Bezpieczne korzystanie z chmury:

- Przechowywanie danych w chmurze: Korzystanie z chmurowych usług przechowywania danych, które oferują odpowiednie zabezpieczenia (szyfrowanie, kontrola dostępu), aby dane były bezpieczne. Przechowywanie danych w chmurze z certyfikatami bezpieczeństwa (np. ISO 27001) jest bardziej bezpieczne niż przechowywanie ich na niezaszyfrowanych urządzeniach.
- Udostępnianie dokumentów: Bezpieczne udostępnianie dokumentów i informacji w chmurze z zachowaniem odpowiednich uprawnień i zabezpieczeń, aby tylko uprawnione osoby miały dostęp do wrażliwych danych.

14. Bezpieczne usuwanie danych:

- Trwałe usuwanie plików, oprogramowanie.

15. Dobre nawyki cyfrowe:

- Stosowanie zasad higieny cyfrowej w codziennej pracy

16. Przykłady ataków sieciowych:

- Ataki ransomware: Złośliwe oprogramowanie, które szyfruje dane ofiary i żąda okupu za ich odszyfrowanie.
- Phishing: Oszustwo polegające na podszywaniu się pod zaufane źródło, aby wyłudzić dane logowania, dane osobowe lub pieniądze.
- Włamania: Nieautoryzowany dostęp do systemów informatycznych w celu kradzieży danych, ich modyfikacji lub usunięcia.
- Ataki DDoS (Distributed Denial of Service): Przeładowanie serwera lub sieci ogromną ilością ruchu, co prowadzi do jej przeciążenia i zablokowania.
- Błąd ludzki: Nieostrożność lub nieuwaga pracowników, która może prowadzić do wycieku danych (np. wysyłanie poufnych informacji na niewłaściwy adres e-mail).

Korzyści dla uczestnika/uczestniczki:

Po zakończeniu szkolenia uczestnik/uczestniczka nabędzie praktyczne umiejętności w zakresie:

- Ochrony wrażliwych danych i informacji
- Bezpieczeństwa danych osobowych
- Ochrony danych wrażliwych i poufnych
- Zwiększania zaufania obywateli
- Minimalizacji ryzyka cyberataków i incydentów bezpieczeństwa
- Ochrony przed cyberatakami

- Zwiększenia odporności systemów IT
- Zabezpieczenia procesów pracy i obiegu dokumentów
- Zwiększenia efektywności operacyjnej
- Bezpiecznej automatyzacji procesów
- Ochrony przed utratą danych
- Ochrony przed nadużyciami i oszustwami
- Utrzymania ciągłości pracy i zarządzania kryzysowego
- Stosowania higieny cyfrowej w codziennej pracy

Temat 5: Zaawansowane narzędzia do zdalnej pracy i komunikacji

Zajęcia zostaną poświęcone najskuteczniejszym narzędziom i platformom, takim jak video konferencje, współdzielone dokumenty czy bezpieczne przesyłanie danych, które umożliwiają efektywne funkcjonowanie zespołów rozproszonych.

Czas trwania: 7 x 60 min. szkolenie online, 7 x 60 min. szkolenie stacjonarne

Cele:

- Wykształcenie umiejętności skutecznego korzystania z cyfrowych narzędzi, platform i strategii w celu komunikowania się, współpracy i wydajnej pracy z innymi.
- Wykształcenie umiejętności stosowania zasad higieny cyfrowej w codziennym życiu

Zagadnienia:

1. Narzędzia do komunikacji

- Microsoft Teams
- Czaty indywidualne oraz grupowe.
- Spotkania wideo z możliwością nagrywania.
- Integracja z Microsoft 365 (Word, Excel, PowerPoint).
- Współdzielenie plików w chmurze (OneDrive).
- Automatyczne tłumaczenie wiadomości.
- Wsparcie dla aplikacji trzecich.
- Slack
- Kanały do komunikacji w zespołach i projektach.
- Integracje z aplikacjami (Google Drive, Trello, Jira, Asana).
- Możliwość wysyłania wiadomości głosowych i wideo.
- Bots automatyzujące zadania i procesy.

- Wyszukiwarka w wiadomościach, plikach i dokumentach.
- Możliwość współdzielenia plików i dokumentów.
- Zoom
- Wideokonferencje z możliwością udostępniania ekranu.
- Nagrywanie spotkań.
- Pokój wirtualny z możliwością podziału na mniejsze grupy (breakout rooms).
- Wirtualne tła i filtracja hałasu.
- Integracja z kalendarzami i aplikacjami do zarządzania zadaniami.
- Możliwość zapraszania uczestników bez konieczności rejestracji.
- Google Meet
- Wideokonferencje zintegrowane z ekosystemem Google Workspace.
- Możliwość prowadzenia spotkań wideo, czatów, współdzielenia ekranów i plików.
- Discord
- Narzędzie do komunikacji zespołowej
- Tekstowe i głosowe czaty,
- Możliwość tworzenia kanałów tematycznych oraz integrację z innymi aplikacjami.

2. Narzędzia do zarządzania projektami i zadaniami

- Trello
- Wizualne zarządzanie projektami z kartami i listami.
- Dodawanie terminów, przypomnienia i komentarzy do zadań.
- Integracje z aplikacjami (Slack, Google Drive, Dropbox).
- Możliwość współpracy w czasie rzeczywistym.
- Śledzenie postępu prac i aktualizowanie statusu zadań.
- Tablice publiczne i prywatne.
- Asana
- Tworzenie projektów z zadaniami, terminami, podzadaniami i przypisaniem do osób.
- Możliwość używania widoku listy, tablicy lub kalendarza.
- Integracje z narzędziami takimi jak Slack, Microsoft Teams, Google Drive.
- Automatyzacja procesów i przypomnienia.
- Raportowanie postępu projektu i mierzenie wyników.
- Zadania do delegowania z odpowiednimi terminami i priorytetami.

3. Narzędzia do współdzielenia plików i pracy w chmurze

- Google Drive
- Przechowywanie plików, zdjęć i dokumentów w chmurze.
- Współpraca nad dokumentami Google (Google Docs, Sheets, Slides).
- Synchronizacja plików na różnych urządzeniach.
- Integracja z Google Meet do wideokonferencji.
- Wersjonowanie dokumentów, możliwość komentowania.
- Dostęp do plików offline.
- Dropbox
- Szerokie możliwości przechowywania i synchronizacji plików w chmurze.
- Współdzielenie plików i folderów z innymi użytkownikami.
- Zabezpieczenie plików za pomocą szyfrowania.
- Wersjonowanie plików.
- Integracja z narzędziami takimi jak Slack i Zoom.
- OneDrive
- Przechowywanie i synchronizacja plików w chmurze.
- Integracja z aplikacjami Microsoft 365 (Word, Excel, PowerPoint).
- Współpraca w czasie rzeczywistym nad dokumentami.
- Wysokiej jakości szyfrowanie danych.
- Możliwość pracy offline i automatyczna synchronizacja po ponownym połączeniu.
- SharePoint
- Zarządzanie dokumentami,
- Tworzenie baz danych i współpraca w zespole,
- Wysoka użyteczność w administracji publicznej,
- Oferuje wysoki poziom kontroli dostępu, integrację z systemami rządowymi i przestrzeganie regulacji prawnych.

4. Dobre nawyki cyfrowe

Stosowanie zasad higieny cyfrowej w codziennej pracy

Korzyści dla uczestnika/uczestniczki:

Po zakończeniu szkolenia uczestnik/uczestniczka nabędzie praktyczne umiejętności w zakresie:

- Wydajność i organizacji pracy

- Skutecznej komunikacji przy pomocy cyfrowych komunikatorów i platform
- Zwiększenia dostępności i responsywności
- Współpracy w zespole
- Zwiększenie bezpieczeństwa danych i dokumentów
- Zwiększanie satysfakcji obywateli
- Optymalizacji kosztów
- Stosowania higieny cyfrowej w codziennej pracy

Temat 6: Elektroniczna obsługa procesów back-office

Podniesienie umiejętności elektronicznej obsługi procesów back-office oraz wykorzystania stanowiskach w urzędach (najczęściej pojawiających się potrzeb urzędów). Ostateczny Odbiorca Wsparcia (OOW) powinien w porozumieniu z urzędem wybrać kierunki szkoleń odpowiadające potrzebom urzędu. Katalog cyfrowych usług polskiej administracji dostępny jest pod adresem: https://www.gov.pl/web/cyfryzacja/katalog-cyfrowych-uslug-polskiej-administracji.