KOMPENDIUM WIEDZY

dotyczące szkolenia pt. „Rozwój kompetencji cyfrowych – rozwiązania technologiczne w pracy pomocowej”

Warszawa, 03.10.2024 r.

Szkolenie jest finansowane ze środków Samorządu Województwa Mazowieckiego.
Usługa jest wykonywana w ramach zadań realizowanych przez Mazowieckie Centrum Polityki Społecznej.

Biuro Szkoleń Kadr Pomocy Społecznej, Mazowieckie Centrum Polityki Społecznej
ul. Grzybowska 80/82, 00-844 Warszawa, tel. 22 376 85 57, szkolenia@mcps.com.pl

Kompendium wiedzy dotyczące szkolenia pt. „Rozwój kompetencji cyfrowych – rozwiązania technologiczne w pracy pomocowej" zostało opracowane przez Pana Dariusza Adamczyka na podstawie treści zawartych w:

1. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.
2. Ustawa z dnia 18 listopada 2020 r. o doręczeniach elektronicznych.
3. Elektroniczna Platforma Usług Administracji Publicznej.

Spis treści:

1. Wprowadzenie do tematu kompetencji cyfrowych.
2. Technologie informacyjno-komunikacyjne.
3. Ważne pojęcia.
4. Praca w chmurze i wirtualne dyski.
5. Wiedza, trendy, komunikacja.
6. E-administracja.
7. Bezpieczeństwo w sieci.
8. Obszary rozwoju kompetencji cyfrowych.

Szkolenie jest finansowane ze środków Samorządu Województwa Mazowieckiego.
Usługa jest wykonywana w ramach zadań realizowanych przez Mazowieckie Centrum Polityki Społecznej.

1. Wprowadzenie do tematu kompetencji cyfrowych

Co to jest **INTERNET**? Jest to sieć komputerów połączonych ze sobą za pośrednictwem infrastruktury telekomunikacyjnej. Nazwa pochodzi od angielskich słów INTER (między) oraz NET lub NETWORK (sieć). Internet ma zasięg globalny, pozwala na wzajemną komunikację komputerów zlokalizowanych w dowolnym miejscu na Ziemi, gdzie tylko istnieje techniczna możliwość podłączenia komputera do sieci.

Smartfon - przenośne urządzenie telefoniczne integrujące w sobie funkcje telefonu komórkowego i komputera kieszonkowego. Smartfon to mieszczący się w kieszeni komputer, którego głównym przeznaczeniem jest komunikacja za pomocą połączeń głosowych, wiadomości tekstowych i wiadomości e-mail oraz przeglądanie stron WWW. Niezbędnym warunkiem uznania danego urządzenia za smartfon jest fakt, że działa ono pod kontrolą systemu operacyjnego umożliwiającego instalowanie dodatkowych aplikacji, rozszerzających jego funkcjonalność.

Blended search - zwracanie klasycznych wyników (linki, opisy) + video, zdjęcia, treści blogowe, aplikacje mobilne, social media.

2. Technologie informacyjno-komunikacyjne

Pod pojęciem **technologii informacyjnych i komunikacyjnych** (w skrócie **TIK**, z ang. Information and communication technologies (ICT)), zwane zamiennie **Technologiami informacyjno-telekomunikacyjnymi**, technikami informacyjnymi lub teleinformatycznymi) kryje się kompleksowy **zbiór technologii przetwarzających, gromadzących i przesyłających informacje w formie elektronicznej/online.**

Społeczeństwo informacyjne charakteryzuje się przygotowaniem i zdolnością do użytkowania systemów informatycznych i wykorzystuje usługi telekomunikacyjne do przekazywania i zdalnego przetwarzania informacji.

Przetwarzanie informacji z wykorzystaniem technologii informacyjnych i komunikacyjnych stanowi znaczącą wartość ekonomiczną, społeczną i kulturową.

Szkolenie jest finansowane ze środków Samorządu Województwa Mazowieckiego.
Usługa jest wykonywana w ramach zadań realizowanych przez Mazowieckie Centrum Polityki Społecznej.

3. Ważne pojęcia.

Domena kieruje internautów na żądaną stronę. Domena internetowa składa się z dwóch części - nazwy głównej oraz końcówki - rozszerzenia. Nazwę główną tworzy nazwa firmy/organizacji/akcji, nazwa działalności. Rozszerzenie jest odgórnie ustalone - można wybrać spośród możliwych propozycji. Każdy kraj posiada przypisane rozszerzenie. Domeny w większym uproszczeniu można podzielić na: narodowe (.pl, .de, .fr, co.uk.), funkcjonalne (.com.pl, .info.pl, .net.pl, .edu.pl), regionalne (.waw.pl, krakow.pl, .bydgoszcz.pl), globalne (.com, .net, .org).

URL (Uniform Resource Locator) to ujednolicony format adresowania zasobów (informacji, danych, usług) stosowany w Internecie i w sieciach lokalnych. URL służy do identyfikowania wszelkich zasobów dostępnych w Internecie. URL składa się z części określającej rodzaj zasobu/usługi (ang. *scheme*), dwukropka i części zależnej od rodzaju zasobu (ang. *scheme-specific part*).

Cookies - mały fragment tekstu, który serwis internetowy wysyła do przeglądarki i który przeglądarka wysyła z powrotem przy następnych wejściach na witrynę. Używane jest głównie do utrzymywania sesji np. poprzez wygenerowanie i odesłanie tymczasowego identyfikatora po logowaniu. Może być jednak wykorzystywane szerzej poprzez **zapamiętanie dowolnych danych**, które można zakodować jako ciąg znaków. Dzięki temu użytkownik nie musi wpisywać tych samych informacji za każdym razem, gdy powróci na tę stronę lub przejdzie z jednej strony na inną.

#Hashtag - słowo lub wyrażenie **bez spacji** poprzedzone symbolem **#** (ang. *hash*), będące formą znacznika (ang. *tag*). Krótkie wiadomości na blogach i serwisach społecznościowych (Facebook, Twitter, Instagram) mogą być oznaczone przez dodanie # przed ważnymi słowami albo wystąpić w zdaniu. Hasztagi umożliwiają grupowanie wiadomości, ponieważ można wyszukać komunikaty, w których zawarto dany hasztag. Wyszukiwanie obejmuje tylko jeden serwis internetowy, dlatego hasztag nie może być powiązany z wiadomościami z innego serwisu.

4. Praca w chmurze/dyski wirtualne.

- Dropbox, dysk google, one drive

Szkolenie jest finansowane ze środków Samorządu Województwa Mazowieckiego.
Usługa jest wykonywana w ramach zadań realizowanych przez Mazowieckie Centrum Polityki Społecznej.

Zalety pracy w chmurze: masz stały dostęp do wszystkich zasobów zgromadzonych w chmurze, osoby korzystające z tej samej chmury mogą pracować nad edycją tego samego dokumentu, chmura ukazuję historię zmian w dokumencie oraz informację kto wprowadził modyfikacje, możesz korzystać z chmury pracując w różnych systemach operacyjnych, kopie zapasowe plików tworzone są automatycznie i możesz je odzyskać w przypadku awarii komputera.

5. Wiedza, trendy, komunikacja

Serwis **OTWARTA NAUKA** powstał z myślą o wszystkich zainteresowanych problematyką otwartości w badaniach naukowych i edukacji. Oferuje przystępne i kompetentne wprowadzenie w podstawowe kwestie związane z otwartą nauką, aktualne informacje o dobrych praktykach, narzędziach i wydarzeniach, a także bazę wiedzy na temat otwartych modeli komunikacji naukowej. Serwis redagowany jest przez zespół Platformy Otwartej Nauki działającej w Interdyscyplinarnym Centrum Modelowania Matematycznego i Komputerowego Uniwersytet Warszawskiego.

Centrum Edukacji Obywatelskiej jest największą polską organizacją pozarządową działającą w sektorze edukacji. Od blisko 25 lat zmienia polską naukę i pracuje by ludzie uczyli się mądrzej i ciekawiej, a praca edukatorów była bardziej efektywna i satysfakcjonująca. Wprowadza nowoczesne metody nauczania oraz ocenianie kształtujące. Prowadzi programy, które pomagają ludziom zrozumieć świat, rozwijają krytyczne myślenie, wiarę we własne możliwości. Uczą przedsiębiorczości i odpowiedzialności, zachęcają do angażowania się w życie publiczne i działania na rzecz innych.

6. E-administracja

UPP – Urzędowe Poświadczenie Przedłożenia

Wystawiane jest automatycznie w momencie wpłynięcia dokumentu w postaci elektronicznej do elektronicznej skrzynki podawczej. Potwierdza jedynie poprawną formę wysłania dokumentu. UPP nie daje nam żadnego potwierdzenia, że dokument który wysłaliśmy został odebrany, nie wymaga jakiegokolwiek działania ze strony pracowników wskazanego podmiotu.

Szkolenie jest finansowane ze środków Samorządu Województwa Mazowieckiego.
Usługa jest wykonywana w ramach zadań realizowanych przez Mazowieckie Centrum Polityki Społecznej.

UPO – Urzędowe Poświadczenie Odbioru
Dokument potwierdzający o poprawnej weryfikacji i odbiorze wysłanego przez nas dokumentu. UPO jest także dowodem na rozpoczęcie procedowania sprawy użytkownika.

UPD – Urzędowe Poświadczenie Dostarczenia
Kierowane jest do osoby fizycznej (użytkownika sprawy) zawierające prośbę złożenia podpisu elektronicznego odbiorcy oraz podanie daty. Po podpisaniu i wysłaniu komunikatu UDP.xml otrzymamy w postaci elektronicznej pismo z urzędu (odpowiedź na nasz wniosek).
Na stronie BIP podmiot jest zobowiązany publikować informacje, które będą służyć odwiedzającym, między innymi: status prawny lub formę prawną, przedmiot działania i kompetencje, organy i osoby sprawujące funkcje i ich kompetencje, majątek, którym dysponuje, tryb działania, sposoby przyjmowania i załatwiania spraw, informacje o prowadzonych rejestrach, ewidencjach i archiwach oraz o sposobach i zasadach udostępniania danych w nich zawartych.

Dane podstawowe: nazwa podmiotu, logo podmiotu (opcjonalnie).

Dane strony podmiotowej BIP: adres URL (czyli adres internetowy strony podmiotowej BIP), imię i nazwisko redaktora/redaktorów, numer telefonu redakcji/ numer faksu redakcji.

Dane uzupełniające: kod pocztowy i miejscowość, ulica, numer domu, numer telefonu/ numer telefaksu, lokalizacja na mapie wskazująca położenie podmiotu.

DOKUMENT ELEKTRONICZNY

- W polskim prawodawstwie nie ma jednolitej definicji dokumentu. Zgodnie z ustawą o informatyzacji działalności podmiotów realizujących zadania publiczne rozumie się przez to „**stanowiący odrębną całość znaczeniową zbiór danych uporządkowanych w określonej strukturze wewnętrznej i zapisany na informatycznym nośniku danych" (art. 3 pkt 2 ustawy**).

- Wymagane jest zapisanie tego dokumentu na nośniku, nie mogą to być tylko przesłane dane. Za dokument elektroniczny uznaje się także dane elektroniczne, dane w postaci elektronicznej, dane w formie elektronicznej,

dane informatyczne i informacje w formie elektronicznej (art. 61 ust. 1 pkt 2 ustawy informatyzacji).

- Należy zauważyć, że podana definicja nie wymaga stosowania podpisu elektronicznego, mimo iż tradycyjnie uważa się go za element istotny dokumentu.

- **Naturalny dokument elektroniczny** – dokument będący od początku swojego istnienia zbiorem zapisanym w postaci elektronicznej, możliwym do odczytania wyłącznie za pośrednictwem odpowiednich urządzeń elektronicznych, nieposiadający pierwowzoru w postaci nieelektronicznej; (Dz.U.2011.14.67).

- **Wizualizacja** – prezentacja treści dokumentu elektronicznego w formie czytelnej dla człowieka, umożliwiającej zapoznanie się z tą treścią i jej zrozumienie. W szczególności wizualizacja może odbywać się przez wyświetlenie na monitorze ekranowym lub za pomocą wydruku; (Dz.U.2015.971).

- Wizualizacja dokumentu elektronicznego w postaci **wydrukowanego tekstu pisma** (pliku PDF) nie pozwoli na weryfikację, czy w rzeczywistości elektroniczny dokument naturalny został podpisany kwalifikowanym podpisem elektronicznym. Weryfikacji złożenia podpisu elektronicznego na dokumencie można dokonać jedynie za pomocą odpowiedniego programu komputerowego.

Środki komunikacji elektronicznej

- elektroniczna platforma usług administracji publicznej (ePUAP) lub regionalna platforma elektronicznych usług publicznych,
- Elektroniczna Skrzynka Podawcza poza ePUAP,
- poczta elektroniczna,
- dedykowany system, przeznaczony do komunikacji z usługodawcą i przez niego zarządzany (Zoom, MS Teams),
- SMS.

Szkolenie jest finansowane ze środków Samorządu Województwa Mazowieckiego.
Usługa jest wykonywana w ramach zadań realizowanych przez Mazowieckie Centrum Polityki Społecznej.

E-doręczenia mają swoją podstawę prawną w Ustawie z dnia 18 listopada 2020 roku o doręczeniach elektronicznych, która weszła w życie 1 lipca 2021 roku. Nakłada ona na administrację rządową oraz samorządową i przedsiębiorców szereg obowiązków. Jej podstawowym założeniem jest wprowadzenie nowoczesnego modelu korespondencji obywateli z samorządami i urzędami. Forma komunikacji jest bezpłatna.

Proces wdrażania przepisów ma trwać do 1 stycznia 2029 roku. Ich wprowadzenie ma na celu realizację standardów wskazanych w Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 910/2014 z 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym.

Z e-Doręczeń można korzystać na trzy sposoby:

- obywatele, firmy i urzędy – ze skrzynki na edoreczenia.gov.pl dla adresów, które tam założą,
- urzędy – z systemu elektronicznego zarządzania dokumentami (EZD), gdy urzędy zintegrują go z e-Doręczeniami – jeśli nie mają systemu klasy EZD, będą korzystać ze skrzynki na portalu Gov,
- obywatele i firmy – przez aplikacje firm, które będą dostarczać w przyszłości usługę e-Doręczeń.

Bezpłatna jest korespondencja:

- od obywateli i firm do urzędu,
- pomiędzy urzędami,
- urzędy płacą za wysyłkę do obywateli, firm i innych instytucji niepublicznych.

Publiczna usługa hybrydowa to **usługa** pocztowa świadczona przez operatora wyznaczonego, jeżeli nadawcą przesyłki listowej jest podmiot publiczny, natomiast operator wyznaczony to operator wyznaczony zgodnie z przepisami prawa pocztowego, czyli operator pocztowy obowiązany do świadczenia usług powszechnych.

Korzystanie z PURDE wymaga **posiadania adresu do doręczeń elektronicznych oraz skrzynki doręczeń**. Zarazem wpis adresu do doręczeń elektronicznych do bazy adresów elektronicznych jest równoznaczny z żądaniem doręczania korespondencji przez podmioty publiczne na ten adres.

Szkolenie jest finansowane ze środków Samorządu Województwa Mazowieckiego.
Usługa jest wykonywana w ramach zadań realizowanych przez Mazowieckie Centrum Polityki Społecznej.

E-przesyłki pochodzące za pomocą rejestrowanego doręczenia elektronicznego od urzędów będą zawierały podpis elektroniczny lub pieczęć elektroniczną urzędu. Dzięki temu, osoba, która otrzyma dokument elektroniczny, będzie mogła się nim posługiwać jako oryginałem i udowodnić jego autentyczność i integralność przed urzędami i sądami.

Przesyłka hybrydowa (drukowana): zawiera informację, że dokument został podpisany lub opieczętowany. Przepisy nie precyzują żadnych zabezpieczeń pozwalających na udowodnienie autentyczności wydrukowanego pisma, które zostało przekazane usługą hybrydową.

7. Bezpieczeństwo w sieci

DANE OSOBOWE

Dane zwykłe: Imię, Nazwisko, Adres zamieszkania, PESEL, NIP, Numer i seria dowodu osobistego, Wykształcenie, Zawód, Płeć, Nr telefonu.

Dane wrażliwe: Pochodzenie rasowe lub etniczne**,** Poglądy polityczne**,** Przekonania religijne lub filozoficzne**,** Przynależność wyznaniowa, partyjna, Stan zdrowia**,** Kod genetyczny**,** Nałogi**,** Życie seksualne**,** Skazania; orzeczenia o ukaraniu**,** Mandaty, orzeczenia wydane przed sądem lub urzędem.

RODO – 6 prostych zasad

- Zidentyfikuj, w jaki sposób dane są wykorzystywane.
- Upewnij się, że dane są bezpiecznie przechowywane.
- Upewnij się, że możesz udowodnić zgodność RODO.
- Zidentyfikuj jakie dane przechowujesz.
- Pozyskaj zgody.
- Upewnij się, że możesz monitorować zgodność z RODO na bieżąco.

ZASADY BEZPIECZNEJ PRACY W SIECI

- ochrona fizyczna w sieci komputerowej i stacji roboczej – utrudnienie dostępu osobom niepowołanym do serwera i stacji roboczych poprzez zamki z szyfrem lub kartami magnetycznymi,
- bezpieczeństwo systemu operacyjnego – mechanizm kontroli dostępu do plików,
- bezpieczeństwo danych – postęp pracownika tylko do danych przeznaczonych do jego poziomu kompetencji,

- bezpieczeństwo przesyłu danych – szyfrowanie danych, kontrola dostępu do sieci nieupoważnionych użytkowników,
- bezpieczeństwo dostępu do Internetu – różnego rodzaju firewale,
- zdrowy rozsądek – unikanie haseł typu imię, data urodzenia, zapisywanie ich na biurku itp.

Internet Protocol address – IP address) to unikatowy **numer** przyporządkowany urządzeniom w sieciach komputerowych, protokołu **IP**. Adresy **IP** są wykorzystywane w Internecie oraz sieciach lokalnych. Adres **IP** zapisywany jest w postaci czterech oktetów w postaci dziesiętnej oddzielonych kropkami.

ZAGROŻENIA W INTERNEICE

- cyberprzemoc, uzależnienie, niebezpieczne treści (przemoc), łamanie prawa (hazard), kradzież danych osobowych, włamania komputerowe, zagrożenia techniczne (wirusy), wyłudzenia poufnych informacji.

BEZPIECZNA INSTALACJA OPROGRAMOWANIA/POBIERANIE PLIKÓW

- Instalacja najnowszej wersji używanego na urządzeniu oprogramowania (plus wtyczki, sterowniki).
- Usunięcie starszych wersji oprogramowania.
- Ustawienia odpowiednich poziomów zabezpieczeń.
- Monity zabezpieczeń wyświetlane podczas korzystania z oprogramowania w używanej przeglądarce (Mozilla, Edge, Chrome…).
- Okresowe przywracanie ukrytych monitów zabezpieczeń.
- Włączenie automatycznych aktualizacji programu i systemu.
- Regularne czyszczenie pamięci podręcznej środowiska.
- Niezezwalanie na uruchamianie aplikacji od nieznanych wydawców.
- Ustawienie poziomu bezpieczeństwa w użytkowanej przeglądarce.
- Instalacja i zabezpieczenie VPN.

BEZPIECZNA POCZTA ELEKTRONICZNA

- Dokładne sprawdzenie, weryfikacja nadawcy.
- Pisownia. Styl emaila, błędy.
- Spakowane załączniki – nie pobieramy ZIP, RAR.
- Linki, Załączniki.

Szkolenie jest finansowane ze środków Samorządu Województwa Mazowieckiego.
Usługa jest wykonywana w ramach zadań realizowanych przez Mazowieckie Centrum Polityki Społecznej.

- SPAM.
- Dwustopniowa weryfikacja.
- Rozdzielenie konta: prywatne vs. Służbowe.
- Polityka haseł.
- Udostępnianie danych, w szczególności szczególnej kategorii danych.

BEZPIECZNA BANKOWOŚĆ ELEKTRONICZNA

Wyłudzanie danych (phishing) – podszywanie się pod bank w celu wyłudzenia pożądanych informacji lub skłonienia do określonych działań. Hakerzy usiłują poznać nasze dane do logowania do serwisów transakcyjnych. Wysyłają fałszywe maile lub podszywają się pod osobę z banku. Pod pretekstem bezpieczeństwa proszą o podanie danych do bankowości elektronicznej czy też kliknięcia w link podany w e-mailu.

Złośliwe oprogramowanie – zainstalowanie na komputerze wirusów czy programów szpiegujących, które śledzą informacje pojawiające się na ekranie komputera, czytają znaki wprowadzane na klawiaturze, przejmują kontrolę nad urządzeniem. Wirusy mogą np. podmienić numer konta adresata przelewu na inny w momencie wypełniania formatki wysyłania przelewu.

- Nie podawaj danych logowania do bankowości elektronicznej przez e-mail/telefon.
- Bank nigdy nie prosi klienta o login/ hasło do konta internetowego ani telefonicznie, ani mailowo.
- Zabezpiecz komputer i telefon – legalne i aktualizowane oprogramowanie; programy antywirusowe; firewall (zapora sieciowa) do ochrony przed atakami z zewnątrz.
- Nie otwieraj podejrzanych e-maili i załączników.
- Sprawdzaj zabezpieczenia strony banku – połączenie szyfrowane; Certyfikat SSL.
- Stwórz silne, unikalne hasło do konta.
- Weryfikuj kody SMS oraz numer rachunku odbiorcy.
- Korzystaj z bezpiecznych sieci WI-FI.
- Korzystaj z zaufanych sklepów internetowych.
- Sprawdzaj bankomaty.
- Włącz powiadomienia.
- Ustaw limity dla transakcji kartami płatniczymi.
- Dbaj o swój smartfon – wylogowanie; aplikacje (Facebook, TikTok…).

Szkolenie jest finansowane ze środków Samorządu Województwa Mazowieckiego.
Usługa jest wykonywana w ramach zadań realizowanych przez Mazowieckie Centrum Polityki Społecznej.

BEZPIECZNA INSTYTUCJA – PRZYKŁADOWE ZABEZPIECZENIA TECHNICZNE

- sieć komputerowa/WIFI zabezpieczona silnym hasłem,
- brak dostępu do sieci osób nieupoważnionych,
- dostęp do sieci Internet za pośrednictwem hasła udostępnionego przez Administratora lub osobę upoważnioną,
- blokada mediów społecznościowych i serwisów z grami, brak dostępu za pośrednictwem sieci WIFI,
- komputery i laptopy zabezpieczone silnym hasłem,
- włączona opcja geolokalizacji, zdalnego unieruchomienia w urządzeniach technicznych (komputer, laptop, smartfon),
- aktualizacja danych dostępowych do systemów informatycznych (login, hasło) w okresie 1 x miesiąc,
- wysyłanie korespondencji email tylko i wyłącznie z adresu służbowego, domeny urzędu administracji publicznej,
- szyfrowanie nośników danych (laptop, pendrive, płyta CD).

POLITYKA BEZPIECZNEGO HASŁA

- Używanych identyfikatorów i haseł nie należy udostępniać innym osobom, a w przypadku podejrzenia, że osoba postronna weszła w ich posiadanie, należy dokonać zmiany zgodnie z obowiązującymi procedurami.
- Logowanie do systemu pocztowego przy pomocy internetowej przeglądarki powinno być przeprowadzone na komputerze, laptopie z zabezpieczeniem antywirusowym.
- Hasła dostępowe do konta pocztowego, systemów IT należy chronić przed dostępem osób trzecich. Nie zaleca się zapamiętywania w przeglądarkach internetowych.
- Po zakończeniu pracy należy wylogować się ze wszystkich systemów.
- Adres konta pocztowego należy udostępniać i wykorzystywać wyłącznie w celach służbowych. Przy wysyłaniu informacji drogą elektroniczną konieczne jest dokładne zweryfikowanie jego adresata oraz treści przesyłanych dokumentów.

Szkolenie jest finansowane ze środków Samorządu Województwa Mazowieckiego.
Usługa jest wykonywana w ramach zadań realizowanych przez Mazowieckie Centrum Polityki Społecznej.

RODZAJE INCYDENTÓW

Incydent krytyczny - skutkujący znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi.

Incydent poważny - powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości działania świadczonej usługi kluczowej.

Incydent istotny - incydent, który ma istotny wpływ na świadczenie usługi cyfrowej.

Incydent w podmiocie publicznym - powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny.

Incydent zwykły - zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo – ten incydent nie podlega zgłoszeniu, ale też należy go obsługiwać.

JAK CHRONIĆ DANE I PRYWATNOŚĆ W SOCIAL MEDIA?

- Zastanów się czy chcesz posługiwać się swoim prawdziwym **imieniem i nazwiskiem**.
- Adres skrzynki pocztowej, numer telefonu pozwalają na łatwą identyfikację oraz powiązanie profilu z innymi kontami.
- Podczas **rejestracji** nie podawaj więcej informacji niż wymaga tego portal.
- Silne hasło (zawierające m.in. wielkie i małe litery, cyfry, znaki specjalne). Jeśli to możliwe – włącz uwierzytelnianie dwuskładnikowe.
- W przypadku pytań dotyczących **odzyskiwania hasła** nie podawaj odpowiedzi łatwych do odgadnięcia

8. Obszary rozwoju kompetencji cyfrowych

PROGRAM ROZWOJU KOMPETENCJI CYFROWYCH

Kompetencje informatyczne obejmujące posługiwanie się komputerem i innymi urządzeniami elektronicznymi, bezpieczne korzystanie z Internetu, aplikacji i oprogramowania, nowych inteligentnych technologii cyfrowych oraz umiejętność stosowania metod pochodzących z informatyki przy programowaniu i tworzeniu rozwiązań informatycznych dla problemów z różnych dziedzin (myślenie komputacyjne).

Szkolenie jest finansowane ze środków Samorządu Województwa Mazowieckiego.
Usługa jest wykonywana w ramach zadań realizowanych przez Mazowieckie Centrum Polityki Społecznej.

Kompetencje informacyjno-komunikacyjne, polegające na umiejętności wyszukiwania informacji, rozumienia jej, a także selekcji i oceny krytycznej, jak również komunikowania się na odległość za pomocą technologii cyfrowych.

Kompetencje funkcjonalne, czyli realne wykorzystanie powyższych kompetencji w różnych sferach codziennego życia, takich jak finanse, praca i rozwój zawodowy, utrzymywanie relacji, zdrowie, hobby, zaangażowanie obywatelskie, życie duchowe itd., zgodnie z zasadami bezpiecznego korzystania z technologii cyfrowych.

PROGRAM ROZWOJU KOMPETENCJI CYFROWYCH ADMINISTRACJA PUBLICZNA

- umiejętność korzystania z informacji i danych,
- komunikowanie się i współpraca wirtualna,
- umiejętność korzystania z mediów,
- tworzenie treści cyfrowych (w tym programowanie),
- bezpieczeństwo (w tym komfort cyfrowy i kompetencje związane z cyberbezpieczeństwem),
- kwestie dotyczące własności intelektualnej,
- rozwiązywanie problemów,
- krytyczne myślenie.

Platforma edukacyjna jest systemem IT umożliwiającym zarządzanie procesem kształcenia i służącym do realizacji. Platforma spełnia rolę repozytorium materiałów dydaktycznych, jak również stanowi medium komunikacyjne pomiędzy uczestnikami procesu edukacyjnego. Konstrukcja platformy zapewnia uczącym się wirtualną osobistą przestrzeń kształcenia (wraz z narzędziami pracy, nauki i komunikacji), a prowadzącym zajęcia umożliwia zarządzanie materiałami dydaktycznymi, grupami użytkowników i procesem kształcenia.

Podręcznik elektroniczny (e-Podręcznik, e-Book) jest narzędziem e-edukacji służącym przede wszystkim do samodzielnej nauki osoby szkolonej. Współczesne podręczniki elektroniczne mają formę multimedialną (tekstu, dźwięk, obraz) i interaktywną (różnego typu ćwiczenia do wykonania przez użytkownika) i są dostępne online. Przy korzystaniu z nich wskazane jest połączenie z Internetem (z uwagi na zawartość łączy do dodatkowych zasobów edukacyjnych).

Szkolenie jest finansowane ze środków Samorządu Województwa Mazowieckiego.
Usługa jest wykonywana w ramach zadań realizowanych przez Mazowieckie Centrum Polityki Społecznej.

Metody podające – służą przekazywaniu uczącym się w możliwie dostępny sposób wiedzy deklaratywnej. Podstawą i głównym źródłem wiedzy jest nauczyciel/ edukator.

Przykład: nagranie video; pliki audio; plik tekstowy; podcast

Metody problemowe – służą przekształceniu wiedzy biernej osób uczących się w wiedzę czynną oraz odkrywaniu nowych wiadomości i stosowanie ich w praktyce. Istotą tego typu metod jest postawienie uczestnika w sytuacji trudności i konkretnego problemu, którą należy przezwyciężyć, opracowując samodzielnie lub w grupie pewne rozwiązanie.

Przykład: forum dyskusyjne; zadanie otwarte; dokument współdzielony

Metody eksponujące – polegają na wywołaniu w uczestniku zajęć przeżycia emocjonalnego i eksponowaniu wartości, według których kształtuje potem swoje oceny i poglądy.

Przykład: projekcja materiału filmowego

Metody praktyczne – służą umożliwieniu bezpośredniego poznania rzeczywistości i rozwijaniu umiejętności przydatnych w codziennej praktyce życiowej.

Przykład: ćwiczenia praktyczne; integracja ze spotkaniem stacjonarnym

Metoda programowana – utrwalanie wiadomości kolejnymi powtórzeniami, praca indywidualna.

Szkolenie jest finansowane ze środków Samorządu Województwa Mazowieckiego.
Usługa jest wykonywana w ramach zadań realizowanych przez Mazowieckie Centrum Polityki Społecznej.