

TEST WIEDZY

do projektu pn. "Generator Cyfrowych Kompetencji", który jest finansowany ze środków Instrumentu na Rzecz Odbudowy i Zwiększania Odporności oraz Unii Europejskiej – NextGenerationEU w ramach Inwestycji C2.1.3. E-kompetencje Krajowego Planu Odbudowy i Zwiększania Odporności.

CZĘŚĆ I. DANE OSOBOWE UCZESTNIKA PROJEKTU

Dane identyfikacyjne	
Imię:	
Nazwisko:	
PESEL:	

TEST WIEDZY

Test składa się z 30 pytań jednokrotnego wyboru. Zaznacz X przy wybranej odpowiedzi.

CZĘŚĆ I ZARZĄDZANIE DANYMI I ANALIZA DANYCH

1. Czym są "dane osobowe"?

- Tylko dane o statusie cywilnym obywatela
- Każde informacje, które pozwalają na zidentyfikowanie osoby fizycznej
- Tylko dane dotyczące płac pracowników urzędów
- Dane dotyczące jedynie wieku i adresu zamieszkania

2. Które z poniższych działań jest elementem dobrego zarządzania jakością danych?

- Aktualizacja i sprawdzanie poprawności
- Kopia wyłącznie na urządzeniu przenośnym
- Praca w chmurze
- Zbieranie tylko danych dotyczących obywateli

3. Jakie dane są chronione zgodnie z RODO (Rozporządzenie o Ochronie Danych Osobowych)?

- Informacje przechowywane w chmurze
- Tylko dane przesyłane przy pomocy Internetu
- Każde dane, które mogą identyfikować osobę fizyczną
- Dane gromadzone w wersji papierowej

4. Co to jest Profil Zaufany w kontekście zarządzania danymi?

- Portal dla osób zakładających jednoosobową działalność gospodarczą
- Usługa umożliwiająca obywatelowi potwierdzenie swojej tożsamości
- Cyfrowy dowód osobisty

- System monitorowania pracy w administracji publicznej

5. Jakie dane są uważane za "dane wrażliwe" w kontekście RODO?

- PESEL
- Dane na temat orientacji seksualnej
- Stan cywilny obywatela
- Dane związane z zatrudnieniem

6. Kiedy dane gromadzone przez urzędników mogą być udostępniane publicznie?

- Zawsze, bez żadnych ograniczeń
- Tylko po uzyskaniu zgody konkretnej osoby
- Jeśli stanowią dane podatkowe
- W procesie rekrutacyjnym

CZĘŚĆ II ZAAWANSOWANE NARZĘDZIA DO ZDALNEJ PRACY I KOMUNIKACJI

1. Które z poniższych narzędzi jest najbardziej popularnym rozwiązaniem do wideokonferencji i spotkań online?

- TeamViewer
- Zoom
- AnyDesk
- Microsoft 365

2. Jakie zabezpieczenia powinny być stosowane w narzędziach do pracy zdalnej, aby zapewnić bezpieczeństwo danych?

- Uwierzytelnianie 2FA
- Przechowywanie haseł w przeglądarce internetowej
- Korzystanie z prywatnych sieci
- Komputer z systemem operacyjnym Windows

3. Co to jest VPN?

- Narzędzie umożliwiające zdalny dostęp do prywatnych plików w chmurze
- Rodzaj bezpiecznego połączenia internetowego
- Usługa synchronizacji danych między urządzeniami
- Regionalna blokada danych w systemach streamingowych

4. Które z poniższych narzędzi umożliwia wspólną pracę na dokumentach w czasie rzeczywistym?

- Google Docs
- Stormshield
- Microsoft Sway

- PotPlayer

5. Czym jest "time tracking"?

- Śledzenie postępów projektów w czasie rzeczywistym
- Monitorowanie czasu spędzonego nad zadaniami
- Przechowywanie danych o czasie pracy na lokalnych dyskach
- Narzędzie do mierzenia czasu prezentacji w PowerPoint

6. Co to jest 2FA?

- Protokół do szyfrowania dokumentów w chmurze
- Podwójna weryfikacja tożsamości, np. hasło i kod SMS
- Fizyczne zabezpieczenie karty płatniczej
- System rozpoznawania pisma odręcznego

CZĘŚĆ III CYBERBEZPIECZEŃSTWO I OCHRONA DANYCH

1. Czym jest phishing?

- Podsywanie się pod zaufaną osobę lub instytucję w celu uzyskania danych
- Rodzaj wirusa, który infekuje komputer i niszczy pliki systemowe
- Technika szyfrowania danych stosowana przez hakerów
- Metoda odzyskiwania danych z uszkodzonych nośników

2. Co oznacza skrót RODO?

- Rozporządzenie o Ochronie Danych Online
- Rozporządzenie o Ochronie Danych Osobowych
- Rozporządzenie o Obowiązках Działalności Online
- Rozporządzenie o Ochronie Dowodów Osobistych

3. Co to jest firewall?

- Urządzenie lub oprogramowanie, które monitoruje i kontroluje ruch sieciowy
- Nazwa programu antywirusowego
- Złośliwe oprogramowanie, które przechwytuje dane logowania
- Oprogramowanie do pracy zdalnej

4. Jakie jest podstawowe zadanie szyfrowania danych?

- Utrudnienie nieautoryzowanego dostępu do danych
- Skuteczne usunięcie danych z nośników
- Możliwość przechowywania danych w chmurze
- Zwiększenie prędkości transferu danych

5. Co to jest MFA?

- Uwierzytelniani wieloskładnikowe
- Technika szyfrowania danych za pomocą wielu algorytmów
- Proces przyznawania dostępu do systemu na podstawie lokalizacji użytkownika
- Sposób tworzenia haseł o dużej długości i skomplikowanej strukturze

6. Jakie są główne zasady w ochronie danych osobowych zgodnie z RODO?

- Zbieranie danych w sposób zgodny z prawem, ich przetwarzanie w sposób przejrzysty, ograniczenie do niezbędnego minimum
- Zbieranie danych w celu stworzenia pełnego profilu użytkownika
- Przechowywanie danych wrażliwych
- Udostępnianie danych osobowych zainteresowanym podmiotom

CZĘŚĆ IV NARZĘDZIA E-ADMINISTRACJI I E-USŁUGI

1. Co to jest ePUAP?

- Platforma do komunikacji z administracją publiczną
- System do wymiany dokumentów między urzędami państwowymi
- Narzędzie do zarządzania sprawami podatkowymi obywateli
- Usługa pozwalająca na zakładanie firm online

2. Jakie technologie są wykorzystywane do zapewnienia autentyczności i integralności dokumentów w e-administracji?

- Podpis elektroniczny
- Podpis odręczny
- Przechowywanie dokumentów w formacie PDF\
- Algorytmy kompresji plików

3. Jakie są wymogi techniczne, aby móc korzystać z platformy ePUAP?

- Tylko dostęp do Internetu
- Odpowiednie oprogramowanie antywirusowe
- System operacyjny Windows
- Przeglądarka internetowa obsługująca technologię SSL/TLS

4. Czy Profil Zaufany można wykorzystać w usługach komercyjnych?

- Tak, ale tylko w wybranych bankach
- Nie, jest ograniczony wyłącznie do administracji publicznej
- Tak, ale tylko w Polsce
- Tak, w usługach komercyjnych zgodnych z eIDAS

5. Jakie systemy w Polsce są kluczowe dla funkcjonowania e-administracji?

- ePUAP
- CEIDG
- e-KRS
- Wszystkie powyższe

6. Czy e-administracja jest dostępna dla osób z niepełnosprawnościami?

- Tak, systemy muszą spełniać standardy dostępności WCAG
- Tak, ale tylko w wybranych usługach
- Nie, brakuje regulacji prawnych w tym zakresie
- Nie, korzystanie wymaga dodatkowych urządzeń

CZĘŚĆ V TWORZENIE I ZARZĄDZANIE CYFROWYMI DOKUMENTAMI

1. Jakie oprogramowanie można wykorzystać do zarządzania dużą ilością dokumentów cyfrowych w firmie?

- Google Meet
- Microsoft SharePoint
- Microsoft Sway
- Google Keep

2. Co oznacza „wersjonowanie dokumentów”?

- Tworzenie kopii zapasowych dokumentu
- Tworzenie różnych wersji dokumentu w celu śledzenia zmian i edycji
- Ochrona dokumentu przed edytowaniem i zmianami
- Dodawanie cyfrowej pieczęci do plików PDF

3. Które z poniższych technologii służą do zapewnienia integralności dokumentów cyfrowych poprzez zapewnienie ich autentyczności i niezmienności?

- HTML
- Blockchain
- OCR
- JSON

4. Jakie są podstawowe formaty cyfrowych dokumentów wykorzystywanych w pracy biurowej?

- PDF, DOCX, XLSX
- JPG, PNG, GIF
- MP3, MP4, AVI
- TXT, RTF, ZIP

5. Jakie są zasady bezpieczeństwa przy udostępnianiu dokumentów w zewnętrznych systemach współpracy (np. Google Drive, Dropbox)?

- Udostępnianie dokumentów powinno odbywać się tylko za pomocą silnych haseł i uwierzytelniania dwuskładnikowego
- Udostępnianie dokumentów powinno być oparte na linkach do folderów
- Należy zawsze udostępniać dokumenty tylko w formacie PDF
- Współdzielenie dokumentów w zewnętrznych systemach jest zawsze bezpieczne, niezależnie od zastosowanych zabezpieczeń.

6. Jaki protokół powinien być używany do zapewnienia bezpiecznego przesyłania dokumentów przez Internet?

- SSL/TLS
- FTP
- http
- VPN