Obraz zawierający godło, symbol, odznaka, herb

Opis wygenerowany automatycznie

**Właściwości dokumentu**

|  |  |
| --- | --- |
| Nazwa | Zasady bezpieczeństwa informacji |
| Zatwierdzanie i nadzór | Dyrektor Szkoły |
| Recenzja | Oficer Bezpieczeństwa Informacji w Szkole |
| Częstotliwość przeglądu | Raz w roku lub po każdej znaczącej zmianie w procesie |
| Lokalizacja przechowywania | Intranet / dedykowany folder na dysku sieciowym |

**Historia wersji**

|  |  |  |  |
| --- | --- | --- | --- |
| Wersja | Data | Autor | Opis zmian |
| 0.1 | 01.10.2024 | Coventry University | Przygotowanie projektu szablonu |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Spis treści**

[1 Ogólne wytyczne 3](#_Toc82346141)

[2 Praca zdalna 4](#_Toc82346142)

[3 Kontrola dostępu 4](#_Toc82346143)

[4 Bezpieczne logowanie i zarządzanie hasłami 5](#_Toc82346144)

[5 Korzystanie z Internetu, poczty elektronicznej,   
komunikatorów internetowych 6](#_Toc82346145)

[6 Sieć wewnętrzna 7](#_Toc82346146)

[7 Wymagania BYOD 7](#_Toc82346147)

[8 Monitorowanie 8](#_Toc82346148)

[9 Zabezpieczanie informacji 8](#_Toc82346149)

[10 Bezpieczne miejsce pracy 9](#_Toc82346150)

[11 Zgłaszanie incydentów i zdarzeń 9](#_Toc82346151)

[12 Sankcje dyscyplinarne 10](#_Toc82346152)

[Proszę pamiętać, że dokument musi być dostosowany do kontekstu Szkoły. Jeżeli jakieś zapisy uznacie za niemożliwie do realizacji, to oczywiście warto przemyśleć dlaczego tak jest a następnie usunąć/zmodyfikować/zastąpić innym zabezpieczeniem kompensującym ryzyko]

# Ogólne wytyczne

1. Użytkownik, oznacza, każdą osobę (Pracownika Szkoły oraz Ucznia) korzystającą z zasobów informatycznych, w tym Internetu, Szkoły.
2. Szkoła dostarcza Pracownikowi sprzęt informatyczny jako narzędzie umożliwiające wykonywanie pracy (zadań) na rzecz Szkoły.
3. Użytkownik ponosi odpowiedzialność za powierzony mu sprzęt i oprogramowanie oraz sposób ich działania.
4. Użytkownik ponosi konsekwencje finansowe i prawne posiadania nielegalnego oprogramowania na sprzęcie teleinformatycznym powierzonym mu przez Szkołę.
5. Surowo zabrania się testowania i/lub łamania zabezpieczeń urządzeń i systemu teleinformatycznego udostępnianego przez Spółkę.
6. Sprzęt powierzony przez Szkołę nie może być udostępniany osobom nieupoważnionym.
7. Zabronione jest samodzielne dokonywanie jakichkolwiek zmian w konfiguracji dostarczonych urządzeń lub oprogramowania, chyba że zmiana została zaakceptowana przez Oficera Bezpieczeństwa Informacji Szkoły. Dotyczy to w szczególności zmian w ustawieniach związanych z zabezpieczeniami.
8. Każdy użytkownik zobowiązany jest do zapoznania się ze wszystkimi regulacjami, instrukcjami i procedurami wewnętrznymi, które są wdrażane przez Dyrekcje Szkoły..

# Praca zdalna

[Uwaga, to dotyczy sprzętu zakupionego przez Szkołę a nie np. prywatnego laptopa nauczyciela wykorzystywanego do pracy. Do tej sytuacji będzie obnosił się punkt mówiący o pracy na prywatnych urządzeniach albo BYOD od angielskiego Bring Your Own Device]

1. Wynoszenie powierzonego sprzętu mobilnego poza siedzibę Szkoły musi być uzasadnione obowiązkami wykonywanymi przez użytkownika.
2. Użytkownik sprzętu mobilnego ma obowiązek go chronić. Należy unikać ryzykownych zachowań, które mogą obejmować m.in.:

* pozostawienie sprzętu bez nadzoru (w samochodzie, pokojach hotelowych itp.),
* pozostawienie torby z laptopem bez nadzoru,
* nie wylogowywanie się użytkownika w przypadku czasowej nieobecności lub braku aktywności,
* ustawienie monitorów umożliwiające podgląd zawartości ekranu osobom nieupoważnionym,

1. W przypadku zagubienia powierzonego sprzętu mobilnego używanego poza Spółką, użytkownik powinien zwłocznie zgłosić powyższy fakt do Oficera Bezpieczeństwa Informacji Szkoły, a w przypadku kradzieży dodatkowo, zgłosić ten fakt Policji.

# Bezpieczne logowanie i zarządzanie hasłami

[Informacja o identyfikatorach oczywiście do usunięcia dla szkół, które nie posługują się nimi

Polityka haseł powinna być zgodna z bieżącymi wytycznymi w tym obszarze: [Kompleksowo o hasłach | CERT Polska](https://cert.pl/posts/2022/01/kompleksowo-o-haslach/)

Popularna w wielu organizacjach polityka częstej zmiany, np. co 30 dni haseł oraz często stosowanie krótkich, zaledwie 8 znakowych haseł nie jest dobrym pomysłem]

1. Użytkownik ponosi odpowiedzialność za wszelkie czynności wykonywane przy użyciu jego identyfikatora i hasła.
2. Hasła użytkowników lub inne poświadczenia podlegają specjalnej ochronie.
3. Każdy użytkownik mający dostęp do systemu informatycznego Szkoły zobowiązany jest do:

* zachowania w tajemnicy wszystkich swoich haseł lub innych danych uwierzytelniających wykorzystywanych do pracy w systemie informatycznym Szkoły,
* niezwłocznej zmiany hasła w przypadku podejrzenia lub faktycznego ujawnienia hasła,
* używać haseł o minimalnej długości 12 znaków, hasło musi zawierać wielkie i małe litery oraz cyfry i/lub znaki specjalne,
* zaleca się stosowanie uwierzytelniania dwuskładnikowego wszędzie gdzie to możliwe,

1. Hasła nie mogą być zapisywane w żaden jednoznaczny sposób (np. pliki tekstowe, notatnik itp.).
2. Dozwolone jest korzystanie z zatwierdzonego systemu dedykowanego do bezpiecznego przechowywania haseł (menedżer haseł)
3. Zabronione jest logowanie się do systemu przy użyciu danych uwierzytelniających innego użytkownika.
4. Użytkownik zobowiązany jest do blokowania komputera, który nie jest obecnie używany, przed nieautoryzowanym dostępem, wymuszając chronioną hasłem blokadę ekranu (zasada czystego ekranu).

# Korzystanie z Internetu, poczty elektronicznej, komunikatorów internetowych w Szkole

1. Jeśli korzystasz z Internetu w Szkole, musisz bezwzględnie unikać ryzykownych zachowań, w tym:
   * + przeglądania stron internetowych zawierających treści niepożądane, w szczególności stron pornograficznych, rasistowskich, nawołujących do nienawiści, promujących sekty, hazardowych lub w jakikolwiek sposób obrażających uczucia innych osób lub naruszających szeroko rozumiane zasady współżycia społecznego,
     + przeglądanie stron internetowych zawierających wszelkiego rodzaju złośliwe oprogramowanie (np. malware, exploity itp.)
     + przeglądanie stron internetowych zawierających kody umożliwiające złamanie lub ominięcie ochrony praw autorskich,
     + pobieranie z Internetu, instalowanie, przechowywanie lub rozpowszechnianie oprogramowania, które nie jest autoryzowane przez Spółkę.
2. Zabronione jest uzyskiwanie dostępu do stron internetowych, które są wykorzystywane do nielegalnej dystrybucji treści (utworów) z naruszeniem przepisów o ochronie praw autorskich.
3. Skrzynki pocztowe z podanym przez Szkołę adresem e-mail mogą być wykorzystywane wyłącznie do korespondencji związanej z działaniem Szkoły.
4. Zabrania się przekazywania poczty do skrzynek niezwiązanych ze Szkołą, w szczególności prywatnych. [Ten zapis oznacza, że np. Nauczyciel nie może wysyłać sobie materiałów na prywatną skrzynką – Szkoła musi rozważyć czy może sobie pozwolić na zabronienie tego w praktyce]
5. W przypadku wysyłania załączników stanowiących tajemnicę Szkoły lub chronionych odpowiednimi przepisami prawa (np. zawierających dane osobowe), załącznik taki musi być zaszyfrowany hasłem spełniającym wymagania określone w punkcie trzecim zasad. Hasło nie może zostać wysłane tym samym kanałem komunikacyjnym co wiadomość.

# Wymagania dotyczące korzystania do pracy lub nauki w Szkole z urządzeń prywatnych użytkowników (BYOD)

1. Można stosować wyłącznie urządzenia i systemy wspierane przez producenta (dla których dostarczane są poprawki bezpieczeństwa).
2. W przypadku:
   * + utraty prywatnego sprzętu (np. w wyniku utraty lub kradzieży) służącego do przetwarzania poufnych danych Szkoły,
     + podejrzenie ujawnienia poufnych danych Spółki

użytkownik niezwłocznie informuje o wystąpieniu takiego zdarzenia Oficera Bezpieczeństwa Informacji Szkoły.

1. W przypadku zagubienia prywatnego urządzenia użytkownika, jego sprzedaży lub zakończenia współpracy ze Szkołą, użytkownik wyraża zgodę na usunięcie przez Szkołę wybranych lub wszystkich (w zależności od możliwości technicznych) danych należących do Szkoły.
2. W przypadku zakończenia współpracy ze Szkołą, zaprzestania korzystania z urządzenia na potrzeby BYOD lub utylizacji prywatnego urządzenia służącego do przetwarzania danych na rzecz Szkoły, użytkownik zobowiązuje się do skontaktowania się z Oficerem Bezpieczeństwa Informacji Szkoły w celu trwałego usunięcia z niego danych będących własnością Szkoły.

# Zabezpieczanie informacji

1. Obowiązkiem użytkownika jest podjęcie kroków w celu zabezpieczenia informacji, które opracowuje lub tworzy. Użytkownik ma następujące opcje zabezpieczania informacji (plików):
   * zaleca się umieszczanie danych w katalogu wskazanym przez Oficera Bezpieczeństwa Informacji Szkoły,
   * korzystanie z zaakceptowanego przez Szkołę rozwiązania do przechowywania danych.
2. Inne rozwiązania do przechowywania danych Szkoły są zabronione.
3. Zabronione jest przetwarzanie informacji na zewnętrznych nośnikach danych (np. pendrive, dysk przenośny), które nie są własnością Szkoły i nie zostały zabezpieczone kryptograficznie.
4. Zabronione jest ujawnianie informacji (danych, plików) należących do Szkoły osobom nieupoważnionym.

# Bezpieczne miejsce pracy

1. W celu ograniczenia ryzyka nieuprawnionego dostępu, utraty lub uszkodzenia informacji w godzinach pracy i poza ich godzinami, użytkownik zobowiązany jest:
   * przestrzegać zasady nie pozostawiania otwartych i niezabezpieczonych drzwi umożliwiających dostęp do pomieszczenia,
   * zabezpieczyć kartę dostępu lub, a w przypadku zgubienia niezwłocznie poinformować o tym fakcie ochronę obiektu i Oficera Bezpieczeństwa Informacji Szkoły,
   * przechowywać dokumenty papierowe i wymienne nośniki informacji w odpowiednio zabezpieczonych meblach biurowych,
   * po zakończeniu pracy zorganizować swoje miejsce pracy, zapobiegając nieautoryzowanemu dostępowi do dokumentów zawierających chronione informacje (zasada „czystego biurka”).

# Zgłaszanie incydentów i zdarzeń

1. W przypadku zauważenia zdarzenia, które może być świadectwem lub dowodem naruszenia bezpieczeństwa, nieprawidłowego działania oprogramowania, błędów lub awarii systemu, użytkownik powinien:
   * zaprzestać pracy na komputerze,
   * niezwłocznie poinformować Oficera Bezpieczeństwa Informacji Szkoły/Informatyka i/lub bezpośredniego przełożonego/Dyrekcję o zajściu, który podejmuje analizę w zakresie konieczności odłączenia komputera od sieci.
2. Zgłoszenie można wykonywać:
   * Pocztą elektroniczną na adres zgloszenia-it@szkola.pl
   * Osobiście do Oficera Bezpieczeństwa Informacji Szkoły/Informatyka i/lub bezpośredniego przełożonego/Dyrekcję
3. Wniosek powinien zawierać:
   * wskazanie użytkownika lub obszaru, który był świadkiem/uczestnikiem zdarzenia,
   * wskazanie lub identyfikacja systemu, którego dotyczy incydent,
   * przybliżony czas wystąpienia incydentu,
   * opis okoliczności i miejsc, w których doszło do zdarzenia oraz symptom /opis zdarzenia.

# Sankcje dyscyplinarne

1. Nieprzestrzeganie zasad określonych w niniejszych Zasadach może prowadzić do odpowiednich sankcji dyscyplinarnych.
2. W przypadku, gdy naruszenie określonych zasad doprowadzi do podejrzenia naruszenia prawa, Dyrekcja przekaże wszelkie dowody organom ścigania do dalszego postępowania.
3. Każdy użytkownik zobowiązany jest do trzymania się na bieżąco wszelkich regulaminów, instrukcji i procedur wewnętrznych, które są wprowadzane przez Dyrekcje Szkoły. Wszystkie przepisy są przechowywane na Dysku Google/OneDrive/Sharepoint/Dysku sieciowym.
4. W przypadku wprowadzenia nowego dokumentu (regulamin, procedura, instrukcje itp.), Oficer Bezpieczeństwa Informacji i/lub Bezpośredni Przełożony jest odpowiedzialny za zapewnienie skutecznego sposobu komunikowania powyższych przepisów użytkownikom.
5. Brak znajomości aktualnych przepisów bezpieczeństwa nie będzie podstawą do jakiegokolwiek rozpatrzenia niewinności użytkownika i może prowadzić do postępowania dyscyplinarnego.

Więcej informacji o projekcie   
  
Sfinansowane ze środków UE. Wyrażone poglądy i opinie są jedynie opiniami autora lub autorów i niekoniecznie odzwierciedlają poglądy i opinie Unii Europejskiej lub Europejskiej Agencji Wykonawczej ds. Edukacji i Kultury (EACEA). Unia Europejska ani EACEA nie ponoszą za nie odpowiedzialności.

Wszystkie rezultaty wypracowane w ramach niniejszego projektu udostępniane są na zasadzie otwartych licencji (CC BY-NC 4.0). Można z nich korzystać bezpłatnie i bez ograniczeń. Kopiowanie lub przetwarzanie tych materiałów w całości lub w części bez zgody autora jest zabronione. W przypadku wykorzystania rezultatów niezbędne jest podanie źródła finansowania oraz jego autorów.

**PROJEKT NR. 2023-2-PL01-KA210-VET-000176822**

* [https://www.coventry.ac.uk/wroclaw/](https://www.coventry.ac.uk/wroclaw/%20)
* <https://kreatywnidlabiznesu.pl/cyber-sec-edu-check/>
* <https://eccedu.net/>

Obraz zawierający tekst, design, Czcionka, Grafika

Opis wygenerowany automatycznie