**Regulamin**

**Ochrony Danych osobowych**

**w Szkole Podstawowej**

**im. W. Komara i T. Ślusarskiego**

**w Czarnogłowach**



**Wrzesień 2018 r.**

**REGULAMIN OCHRONY DANYCH OSOBOWYCH W SZKOLE PODSTAWOWEJ**

**IM. W. KOMARA I T. ŚLUSARSKIEGO**

**W CZARNOGŁOWACH**

Spis treści

[**I.** **POSTANOWIENIA OGÓLNE** 3](#_Toc514013103)

[**II.** **ZASADY KORZYSTANIA Z INTERNETU** 3](#_Toc514013104)

[**III.** **BEZPIECZNE UŻYTKOWANIE SPRZĘTU IT, PROGRAMÓW I DYSKÓW** 4](#_Toc514013105)

[**IV.** **ADMINISTROWANIE UPRAWNIENIAMI- ROZPOCZĘCIE, ZAWIESZENIE I ZAKOŃCZENIE PRACY** 5](#_Toc514013106)

[**V.** **POLITYKA HASEŁ** 5](#_Toc514013107)

[**VI.** **ZASADY KORZYSTANIA Z POCZTY ELEKTRONICZNEJ** 6](#_Toc514013108)

[**VII.** **ZASADY WYNOSZENIA NOŚNIKÓW Z DANYMI OSOBOWYMI POZA SZKOŁĘ** 7](#_Toc514013109)

[**VIII.** **ZASADY ZABEZPIECZANIA DOKUMENTACJI PAPIEROWEJ Z DANYMI OSOBOWYMI** 8](#_Toc514013110)

[**IX.** **POSTĘPOWANIE W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH** 8](#_Toc514013111)

[**X.** **POUFNOŚĆ I OCHRONA DANYCH OSOBOWYCH** 9](#_Toc514013112)

[**XI.** **CZYNNOŚCI DYSCYPLINARNE** 10](#_Toc514013113)

1. **POSTANOWIENIA OGÓLNE**

Regulamin stanowi wykaz podstawowych obowiązków z zakresu przestrzegania zasad ochrony danych osobowych w Szkole Podstawowej im. W. Komara i T. Ślusarskiego w Czarnogłowach.

 Regulamin ochrony danych osobowych jest wykazem obowiązków, które wynikają z zakresu przestrzegania zasad ochrony danych osobowych zgodnie z przepisami RODO. Obowiązki te dotyczą przede wszystkim: pracowników, współpracowników, innych pracowników, którzy posiadają dostęp do przetwarzanych danych przez Administratora/szkołę oraz użytkowników systemów informatycznych którzy posiadają dostęp do przetwarzanych danych przez Administratora/szkołę.

 Należy zapoznać każdą z tych osób z tym dokumentem, oraz zobowiązać ją do stosowania zawartych w nich zasad i procedur.

Regulamin zapewnia wiedzę wszystkim osobom, które przetwarzają dane osobowe. Wiedza ta opiera się na bezpiecznych zasadach przetwarzania danych. Po zapoznaniu się z zasadami bezpiecznego przetwarzania danych, każda osoba musi potwierdzić znajomość tych zasad, oraz złożyć deklaracja stosowania ich, podpisując własnoręcznie Oświadczenie woli.

Administratorem danych osobowych w Szkole Podstawowej im. W. Komara i T. Ślusarskiego w Czarnogłowach jest dyrektor szkoły.

Funkcję Inspektora Ochrony Danych w Szkole Podstawowej im. W. Komara i T. Ślusarskiego w Czarnogłowach sprawuje p. Bartosz Kaniuk iodo.szczecin@gmail.com , tel. +48579979237

1. **ZASADY KORZYSTANIA Z INTERNETU**

|  |  |
| --- | --- |
| *a.* | Internetu należy używać tylko w sprawach służbowych; |
| *b.* | każdy, kto korzysta z Internetu ponosi odpowiedzialność za szkody, które powoduje oprogramowanie instalowane z Internetu; |
| *c.* | surowo wzbronione jest zgrywanie na dysk twardy komputera i korzystanie z nielegalnych programów. Ściąganie plików wymaga zgody osoby zajmującej się infrastrukturą IT w szkole; |
| *d.* | zabrania się korzystania ze stron, które mają charakter hackerski, lub zawierają treści niedozwolone (np. pornograficzne). Strony te najczęściej są zainfekowane i mają automatycznie zainstalowane szkodliwe oprogramowanie, które może zniszczyć zasoby znajdujące się w komputerze użytkownika; |
| *e.* | nie należy używać w przeglądarce opcji autouzupełniania formularzy zapamiętywania haseł; |
| *f.* | gdy używamy szyfrowanego połączenia w przeglądarce każdorazowo należy sprawdzić, czy pojawia się ikona "kłódki", a adres rozpoczyna się od "https"; |
| *g.* | szczególną uwagę należy zwrócić, gdy pojawia się podejrzane żądanie lub prośba logowania na stronę (bank, portal społecznościowy, e-sklep, poczta mailowa). Podejrzane powinno wydać się również, gdy strona wymaga podania loginu, hasła, PIN-u, numeru karty płatniczej przez Internet. Podawanie takich informacji jest zabronione zwłaszcza, gdy dokonujemy płatności przez stronę internetową banku. |

1. **BEZPIECZNE UŻYTKOWANIE SPRZĘTU IT, PROGRAMÓW I DYSKÓW**

|  |  |
| --- | --- |
| *a.* | osoba, która przetwarza dane osobowe i korzysta ze sprzętu IT (komputer stacjonarny, monitor, drukarka, skaner, ksero, laptop, tablet, smartfon) ma obowiązek zabezpieczenia go przed zniszczeniem lub uszkodzeniem; |
| *b.* | zgubienie, utrata lub zniszczenie powierzone sprzętu IT powinno być zgłoszone; |
| *c.* | zabrania się samowolnego instalowania sprzętu IT i dodatkowych urządzeń (twarde dyski, pamięć); |
| *d.* | zakazuje się podłączania niezatwierdzonych urządzeń do systemu informatycznego;e. należy uniemożliwić osobom niepowołanym[[1]](#footnote-1) wgląd do danych zawartych na monitorach (*polityka czystego ekranu*); |
| *e.* | czasowe opuszczenie miejsca pracy winno się wiązać z przywołaniem blokowanego hasłem wygaszacza ekranu (*WINDOWS+L*). Dozwolone jest całkowite wylogowanie się z systemu lub programu; |
| *f.* | po zakończeniu pracy należy wylogować się z systemu informatycznego, wyłączyć sprzęt komputerowy, zabezpieczyć stanowisko pracy (szczególnie nośniki, na których znajdują się dane osobowe); |
| *g.* | w trakcie wspólnego użytkowania komputera, użytkownicy zobowiązani są do usuwania plików, do których dostęp mają inni użytkownicy (nieuprawnieni do dostępu do takich plików); |
| *h.* | osoby uprawnione do niszczenia nośników mają obowiązek trwale zniszczyć nośnik lub trwale usunąć z niego dane (niszczenie płyt w niszczarce, niszczenie twardego dysku lub pendrive`a przy pomocy młotka). |

1. **ADMINISTROWANIE UPRAWNIENIAMI- ROZPOCZĘCIE, ZAWIESZENIE I ZAKOŃCZENIE PRACY**

|  |  |
| --- | --- |
| *a.* | każdy użytkownik[[2]](#footnote-2) musi posiadać swój indywidualny identyfikator (*login*). Zabrania się umożliwiania innym osobom pracy na innym koncie niż swoje własne; |
| *b.* | przełożony wydaje polecenie do utworzenia konta wraz z uprawnieniami. Wykonywane jest to przez informatyków; |
| *c.* | użytkownik nie ma prawa do zmiany swoich uprawnień; |
| *d.* | użytkownik rozpoczyna pracę z użyciem identyfikatora (loginu) i hasła; |
| *e.* | jeśli system zasygnalizuje próby logowania się do systemu osoby nieupoważnionej, należy to niezwłocznie zgłosić informatykowi (administratorowi); |
| *f.* | w chwili zablokowania systemu podczas próby logowania, należy natychmiast powiadomić o tym informatyka (administratora); |
| *g.* | należy uniemożliwić osobom niepowołanym wgląd do danych zawartych na monitorach (*polityka czystego ekranu*); |
| *h.* | czasowe opuszczenie miejsca pracy winno się wiązać z przywołaniem blokowanego hasłem wygaszacza ekranu (*WINDOWS+L*). Dozwolone jest całkowite wylogowanie się z systemu lub programu. Brak tych działań, spowoduje że po upływie XX minut system automatycznie aktywuje wygaszacz. |
| *i.* | nie można uruchamiać aplikacji, które nie zostały zweryfikowane przez informatyka (szczególnie dotyczy to programów przesyłanych pocztą elektroniczną); |
| *j.* | po zakończeniu pracy użytkownik musi wylogować się z sytemu informatycznego i wyłączyć sprzęt komputerowy oraz zabezpieczyć stanowisko pracy (w szczególności dokumentację i nośniki, na których znajdują dane osobowe). |

1. **POLITYKA HASEŁ**

|  |  |
| --- | --- |
| *a.* | hasło musi zawierać określoną liczbę znaków, duże i małe litery oraz cyfrę (mogą też zawierać znaki specjalne). Hasło powinno być trudne do odgadnięcia. Nie może być powszechnie używanym słowem. Hasłem nie powinny być: imiona, daty urodzenia, nazwiska oraz typowe zestawy ( 1234..., qwerty); |
| *b.* | nie należy ujawniać haseł innym osobom, ani zapisywać ich na kartkach (w notesie, przy komputerze, na monitorze, pod klawiaturą); jeśli zaistnieje sytuacja ujawnienia hasła osobie trzeciej, należy je natychmiast zmienić; |
| *c.* | hasła muszą być zmieniane co 30/60/90 dni; jeśli nie jest to wymuszone przez system, należy samodzielnie o tym pamiętać; zmiany hasła można dokonać w trakcie pracy w aplikacji; |
| *d.* | pracownicy obowiązani są do zachowania hasła w tajemnicy, nawet po utracie przez nie ważności; |
| *e.* | nie można używać takich samych haseł w serwisach internetowych, jak w systemie komputerowym w szkole; |
| *f.* | jedno hasło nie może być używane jako zabezpieczenie do różnych systemów; |
| *g.* | zabronione jest generowanie haseł, w których jeden z członów zawsze pozostaje niezmienny, a drugi zmieniany jest według określonego wzorca (np. styczeń 2018, luty2018, marzec2018 itd.). |

1. **ZASADY KORZYSTANIA Z POCZTY ELEKTRONICZNEJ**

|  |  |
| --- | --- |
| *a.* | dane osobowe przesyłane mailem poza szkołę może odbywać się tylko przez upoważnione do tego osoby. Pliki należy wysłać zaszyfrowane i spakowane[[3]](#footnote-3) oraz zahasłowane. Hasło należy przekazać odbiorcy inną drogą (telefonicznie lub smsem). Hasło powinno składać się z określonej liczny znaków, oraz zawierać małe i duże litery, cyfry lub znaki specjalne; |
| *b.* | należy dołożyć wszelkiej staranności przy wysyłce dokumentów z danymi osobowymi, poprzez kilkukrotne sprawdzenie poprawności adresu odbiorcy; |
| *c.* | doradza się, aby użytkownik, który przesyła dane osobowe zawarł informację z prośbą o potwierdzenie otrzymania wiadomości od odbiorcy; |
| *d.* | ZABRANIA SIĘ: otwierania załączników w mailach, które są wirusami infekującymi komputery w sieci (wiąże się to z bardzo wysokim ryzykiem utraty danych osobowych), klikania w hiperlinki w mailach (są to wirusy atakujące komputery w sieci, co wiąże się to z bardzo wysokim ryzykiem utraty danych osobowych); |
| *e.* | każdorazowo należy zgłaszać informatykowi podejrzane maile (!); |
| *f.* | nie należy wysyłać niezawodowych maili (np. życzeń świątecznych do wszystkich pracowników szkoły); |
| *g.* | wymaga sie kasowania niepotrzebnych maili na bieżąco; |
| *h.* | wysyłając maile do wielu adresatów powinno się stosować metodę UDW[[4]](#footnote-4); |
| *i.* | nie można łączyć firmowych kont pocztowych z prywatnymi; |
| *j.* | mail służbowy służy tylko do wykonywania obowiązków służbowych; obowiązuje zakaz wysyłania maili z poczty służbowej na prywatne adresy pocztowe pracowników lub innych osób; |
| *k.* | korzystanie z poczty mailowej do celów prywatnych powinno odbywać się okazjonalnie, i należy to ograniczyć do niezbędnego minimum; nie może to mieć wpływu na jakość pracy i wykonywanie przez niego obowiązków służbowych; |
| *l.* | nie wolno konfigurować kont pocztowych do automatycznego przekierowywania wiadomości na adres zewnętrzny; |
| *m.* | służbowej poczty mailowej nie można używać w celu rozpowszechniania treści o charakterze obraźliwym lub niemoralnym; |
| *n.* | użytkownik nie ma prawa bez zgody pracodawcy wysyłać za pośrednictwem poczty mailowej wiadomości, które zawierają dane osobowe dotyczące: pracodawcy, jego pracowników, klientów, kontrahentów , etc. |
| *o.*  | każdy użytkownik zobowiązany jest do skanowania programem antywirusowym plików, które wprowadza z dysków zewnętrznych. Obowiązuje zakaz wyłączania systemu antywirusowego, podczas gdy przetwarzamy dane osobowe w systemie informatycznym. Podczas stwierdzenia zainfekowania systemu należy natychmiast poinformować o tym fakcie informatyka. |

1. **ZASADY WYNOSZENIA NOŚNIKÓW Z DANYMI OSOBOWYMI POZA SZKOŁĘ**

|  |  |
| --- | --- |
| *a.* | pracownicy szkoły nie mogą wynosić na zewnątrz szkoły wymiennych nośników[[5]](#footnote-5) informacji z zapisanymi danymi osobowymi bez zgody pracodawcy; |
| *b.* | dane osobowe, które zostają wyniesione poza szkołę należy zaszyfrować; należy uzyskać na to zgodę ADO[[6]](#footnote-6); |
| *c.* | przewożenie dokumentacji papierowej w teczkach musi odbywać się w bezpieczny sposób (np. korzystanie z zaufanych firm kurierskich); |
| *d.* | jeśli przewiezienie dokumentów zawierających dane osobowe zostało powierzone pracownikowi szkoły, musi on w należyty i staranny sposób zabezpieczyć dokumenty przed kradzieżą lub zagubieniem; |
| *e.* | jeśli chcemy przekazać nośniki zawierające dane osobowe poza obszar szkoły należy zastosować odpowiednie środki bezpieczeństwa: powiadomić adresata o przesyłce, zaszyfrować dane, a hasło do ich odczytania przekazać inną drogą, zastosować koperty depozytowe oraz nadać przesyłkę przez kuriera. |

1. **ZASADY ZABEZPIECZANIA DOKUMENTACJI PAPIEROWEJ Z DANYMI OSOBOWYMI**

|  |  |
| --- | --- |
| *a.* | każdy pracownik powinien stosować się do *polityki czystego biurka.* Należy zabezpieczać, a w szczególności zamykać, dokumenty i nośniki (szafy, biurka, pomieszczenia zamknięte) przed kradzieżą, lub przed dostępem osób nieupoważnionych po godzinach pracy (lub podczas nieobecności w trakcie pracy); |
| *b.* | pracownicy, którzy przetwarzają dane osobowe są w obowiązku niszczyć dokumenty i wydruki w niszczarkach (ewentualnie utylizować je w specjalnych pojemnikach, które podlegają bezpiecznej utylizacji); |
| *c.* | nie należy pozostawiać dokumentów z danymi osobowymi poza zabezpieczonymi pomieszczeniami[[7]](#footnote-7); |
| *d.* | zakazuje się wyrzucanie niezniszczonych dokumentów na śmietnik lub porzucania ich na zewnątrz. |

1. **POSTĘPOWANIE W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH**

|  |  |
| --- | --- |
| *a.* | niezwłocznie i natychmiastowo należy powiadomić o zdarzeniu pracodawcę (nawet w przypadku, gdy istnieje tylko podejrzenie naruszenia ochrony danych osobowych). W szczególności, gdy zauważono nieprawidłowe: zabezpieczenie pomieszczeń, dokumentów i urządzeń, sprzętu IT i oprogramowania; lub gdy nie została zachowana zasada prawidłowej ochrony danych osobowych[[8]](#footnote-8); |
| *b.* | incydenty i zdarzenia, o których należy również powiadamiać to: zewnętrzne zdarzenia losowe (pożary, kradzieże, zalania, utrata łączności), wewnętrzne zdarzenia losowe (awarie sprzętu IT, pomyłki informatyków lub samych użytkowników, zgubienie danych) i umyślnie spowodowane incydenty (kradzież lub wyciek danych osobowych, ujawnienie informacji osobom nieupoważnionym, świadome niszczenie danych lub dokumentów oraz działanie wirusów i szkodliwego oprogramowania); |
| *c.* | w szczególności należy reagować, gdy: * zauważymy ślady na drzwiach wskazujące na próbę włamania i kradzieży,
* niszczona jest dokumentacja zawierająca dane osobowe bez użycia niszczarki,
* w szkole znajdują się osoby zachowujące się w podejrzany sposób,
* otwarte pozostają drzwi do szaf i pomieszczeń z danymi osobowymi,
* ustawienia monitorów wskazują na możliwość wglądu osób nieupoważnionych,
* dane osobowe są wynoszone na zewnątrz szkoły (w wersji papierowej i elektronicznej),
* udostępniane są dane osobowe osobom nieupoważnionych,
* odbywają się próby wyłudzenia danych osobowych przez telefon,
* dochodzi do kradzieży lub zagubienia komputerów i innego typu sprzętu, który zawiera dane osobowe,
* otrzymujemy maila z próbą wyłudzenia hasła i loginu,
* zauważymy działania wirusa w komputerze, zaobserwujemy zapisane hasła w pobliżu komputera
 |

.

1. **POUFNOŚĆ I OCHRONA DANYCH OSOBOWYCH**

|  |  |
| --- | --- |
| *a.* | osoba przetwarzająca dane osobowe jest zobowiązana do przetwarzania danych osobowych tylko w zakresie i celu, który został przewidziany w drodze powierzenia jej przez pracodawcę zadań. Użytkownik przetwarzający dane musi zachować tajemnicę danych osobowych do których ma wgląd i dostęp, w związku z obowiązkami, jakie nałożył na niego pracodawca. Dane osobowe nie mogą być wykorzystywane w celach niezgodnych z zakresem powierzonych zadań przez pracodawcę. W tajemnicy należy zachować sposób zabezpieczenia danych osobowych oraz chronić dane przed zniszczeniem, utratą, modyfikacją, nieuprawnionym ujawnieniem, dostępem i przetwarzaniem przez osoby do tego nieupoważnione; |
| *b.* | należy przeszkolić pracowników z zasad ochrony danych osobowym. Pracownicy, którzy przeszli szkolenie i zapoznali się z Regulaminem ochrony danych osobowych w szkole zobowiązane są podpisać oświadczenie o poufności; |
| *c.* | kategorycznie zabrania się przekazywania bezpośrednio lub drogą telefoniczną danych osobowych osobom nieupoważnionym, lub osobom, których tożsamość pozostaje trudna do zweryfikowania, lub gdy osoby nieupoważnione podszywają się pod kogoś innego. Instytucjom i osobom, które nie mogą wykazać jasnej podstawy prawnej do dostępu do danych osobowych, również nie dnależy przekazywać i ujawniać danych osobowych; |
| *d.* | zakaz przekazywania i ujawniania danych osobowych obowiązuje także w grupach dyskusyjnych, forach internetowych i blogach. |

1. **CZYNNOŚCI DYSCYPLINARNE**

W sytuacji, gdy nastąpi nieuzasadnione zaniedbanie obowiązków wynikających z regulaminu ochrony danych osobowych w szkole, będzie to traktowane jako ciężkie naruszenie obowiązków pracowniczych i zasad współpracy. Sprzeczne działania z zobowiązaniami zawartymi w tym dokumencie może zostać uznane przez pracodawcę jako naruszenie przepisów karnych zawartych w Rozporządzeniu o ochronie danych UE z dnia 27.04.2016 r.

Regulamin ochrony danych osobowych w szkole obowiązuje od 25 maja 2018 roku.

Czarnogłowy, 05.09.2018 r …………………………….

miejscowość, data podpis Dyrektora

**Załączniki do regulaminu ochrony danych osobowych w szkole:**

|  |  |  |
| --- | --- | --- |
| 1. Oświadczenie woli | .................... | załącznik nr 1 |

**Z REGULAMINEM OCHRONY DANYCH OSOBOWYCH W SZKOLE PODSTAWOWEJ IM. W. KOMARA I T. ŚLUSARSKIEGO W CZARNOGŁOWACH ZAPOZNAŁAM/EM SIĘ:**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Imię i Nazwisko** | **Czytelny podpis** |
| 1. | Grażyna Kamińska |  |
| 2. | Magdalena Fiłkowska |  |
| 3. | Wioletta Wójcik |  |
| 4. | Agnieszka Suleja |  |
| 5. | Waldemar Majewski |  |
| 6. | Emilia Kowalewska |  |
| 7. | Urszula Maciejewska |  |
| 8. | Agnieszka Mikuła |  |
| 9. | ks. Krzysztof Jęczmionka |  |
| 10. | Ewa Majewska |  |
| 11. | Katarzyna Grześkowiak |  |
| 12. | Monika Tomczyk |  |
| 13. | Beata Świerczyńska |  |
| 14. | Joanna Pajestka |  |
| 15. | Elżbieta Chadaś |  |
| 16. | Bożena Mańczak |  |
| 17. | Danuta Kazimierczuk |  |
| 18. | Jolanta Grześkowiak |  |
| 19. | Dorota Gębicz |  |
| 20. | Stanisław Inglot |  |
| 21. | Małgorzata Rapa |  |
| 22. | Romualda Kozak |  |
| 23. | Ewa Rabikowska |  |
| 24.  | Genowefa Ogórek |  |
| 25. | Halina Docenko |  |

1. klient, inny pracownik, pracownik innego działu [↑](#footnote-ref-1)
2. komputera stacjonarnego, laptopa, dysku sieciowego, programów, na których pracownik pracuje, poczty elektronicznej [↑](#footnote-ref-2)
3. PROGRAM ZIP, WINZIP, WINRAR [↑](#footnote-ref-3)
4. UDW- ukryte do wiadomości [↑](#footnote-ref-4)
5. wymienne dyski twarde, pedndrive`y, płyty CD i DVD [↑](#footnote-ref-5)
6. ADO- Administrator Danych Osobowych [↑](#footnote-ref-6)
7. korytarz, toaleta, kserokopiarka, skaner, sala konferencyjna, pomieszczenie socjalne [↑](#footnote-ref-7)
8. niestosowanie zasady czystego ekranu/biurka, nienależyta ochrona haseł, niezamykanie szaf i biurek, w których dostępne są dokumenty zawierające dane osobowe. [↑](#footnote-ref-8)