

Standardy Ochrony Małoletnich w Grupie Mostostal Zabrze

Niniejsze Standardy ochrony małoletnich stanowią wzór postępowania dla Pracowników oraz Współpracowników Grupy Mostostal Zabrze podczas współpracy z osobami małoletnimi. Niezależnie od wieku, swoich współpracowników traktujemy z należyтым szacunkiem, zachowując przy tym wszelkie zasady bezpieczeństwa. Szczególną uwagę chcemy otoczyć osoby małoletnie, które mogą być szczególnie narażone na sytuacje zagrażające ich bezpieczeństwu i dobrostanowi, w myśl Ustawy o przeciwdziałaniu zagrożeniom przestępczością na tle seksualnym i ochronie małoletnich

§1 Definicje / Słowniczek pojęć

- 1. GMZ** – Grupa Mostostal Zabrze
- 2. Pracodawca** – Każda ze spółek wchodzących w skład Grupy Mostostal Zabrze, tj.:
 - Mostostal Zabrze S.A.,
 - Mostostal Zabrze Biprohut S.A.,
 - Mostostal Zabrze Konstrukcje Przemysłowe S.A.,
 - Mostostal Zabrze Realizacje Przemysłowe S.A.,
 - Mostostal Zabrze Gliwickie Przedsiębiorstwo Budownictwa Przemysłowego S.A.,
 - Mostostal Zabrze Nieruchomości Sp. z o.o.
 - Mostostal Zabrze Elektro Sp. z o.o.
 - Polwax S.A.
 - ModQ Solutions S.A.
- 3. Pracownik** – każda osoba zatrudniona u pracodawcy na podstawie stosunku pracy albo umowy cywilnoprawnej odpłatnej bądź nieodpłatnej, a także wykonująca działalność na rzecz pracodawcy.
- 4. Dyrektor Szkoły** – dyrektor szkoły, której uczeń realizuje praktyczną naukę zawodu lub staż uczniowski u pracodawcy, zgodnie z przepisami prawa oświatowego.
- 5. Małoletni** – każda osoba, która nie ukończyła 18. roku życia lub jest uczniem szkoły, która realizuje praktyczną naukę zawodu na podstawie umowy o praktyczną naukę zawodu lub umowy o pracę w celu przygotowania zawodowego lub staż uczniowski.
- 6. Opiekun prawny** – przedstawiciel ustawowy małoletniego, tj.: rodzic, rodzic zastępczy, opiekun tymczasowy.
- 7. Opiekun małoletniego** – opiekun wyznaczony przez pracodawcę do prowadzenia pod kierunkiem tej osoby praktyk zawodowych, stażu uczniowskiego lub wszelkiej innej dozwolonej formy zatrudnienia małoletniego.

8. **Instruktor praktycznej nauki zawodu** – pracodawca lub osoba zatrudniona przez pracodawcę, która posiada niezbędne kwalifikacje zawodowe i pedagogiczne do realizowania praktycznej nauki zawodu w zakładzie pracy.
9. **Przemoc fizyczna** - Działanie intencjonalne, którego skutkiem są obrażenia fizyczne u dziecka, takie jak popychanie czy szarpanie. Do możliwych objawów przemocy fizycznej należą m.in.: siniaki, ślady na ciele, obrzęki, złamania, zwichnięcia, oparzenia – w tym punktowe – a także przejawy lęku przed rozebraniem się, noszenie odzieży nieadekwatnej do warunków atmosferycznych (np. długi rękaw w upalne dni), zakrywanie oczu okularami przeciwsłonecznymi, apatia lub agresywne zachowania.
10. **Przemoc psychiczna** - Świadome działanie lub zaniechanie, które skutkuje niewłaściwą interakcją z dzieckiem, mającą negatywny wpływ na jego rozwój emocjonalny i psychiczny. Przykłady takich zachowań to: emocjonalna niedostępność, zaniedbywanie potrzeb emocjonalnych, szantażowanie, używanie obelg, grożenie, poniżanie czy zawstydzanie.
11. **Przemoc seksualna** - Włączanie dziecka w aktywności o charakterze seksualnym, na które – z uwagi na swój wiek i rozwój – nie jest w stanie wyrazić świadomej zgody. Przejawami przemocy seksualnej mogą być m.in.: prezentowanie treści pornograficznych, proponowanie bądź zmuszanie do podejmowania relacji intymnych, gwałt, a także inne formy przymuszania do czynności seksualnych. Objawy mogą obejmować dolegliwości somatyczne o niewyjaśnionym pochodzeniu, ślady przemocy fizycznej, trudności w poruszaniu się lub siadaniu, występowanie lęków, fobii, stanów depresyjnych, nadpobudliwość bądź agresję.
12. **Koordinator bezpieczeństwa w Internecie** – pracownik Działu IT, wyznaczony przez Pracodawcę, odpowiedzialny za zapewnienie bezpiecznych warunków korzystania z sieci informatycznych przez małoletniego na terenie Pracodawcy.
13. **Osoba odpowiedzialna na standardy ochrony małoletnich** – pracownik, wyznaczony do sprawowania nadzoru nad przestrzeganiem niniejszych standardów oraz ich bieżącą aktualizacją.
14. **Osoba odpowiedzialna za interwencję** – pracownik wyznaczony do przyjmowania zgłoszeń o zdarzeniach zagrażających małoletniemu, za podejmowanie interwencji, za opracowanie planu wsparcia małoletniego i zgłoszenie sprawy do właściwych organów i instytucji oraz prowadzenie rejestru interwencji.

§2 Osoby odpowiedzialne

1. Koordynatorami bezpieczeństwa w Internecie są **Administrator Systemów Informatycznych - Marcin Bator** (marcin.bator@mz.pl) oraz **Kierownik Działu IT – Michał Kriger** (michal.kriger@mz.pl).
2. Osobą odpowiedzialną za standardy ochrony małoletnich jest **Dyrektor Biura Zarządzania Personelem Grupy Mostostal Zabrze - Aleksandra Brzoza** (aleksandra.brzoza@mz.pl).
3. Osobą odpowiedzialną za interwencję jest **Specjalista w Dziale Rozwoju Pracowników i Komunikacji - Martyna Samiec** (martyna.samiec@mz.pl).

S3 Obowiązki Pracodawcy

Pracodawca podejmuje następujące działania:

1. Ustalenie zasad zatrudniania Opiekunów Małoletnich i Instruktorów praktycznej nauki zawodu:

1.1. Przed powierzeniem Pracownikowi funkcji Opiekuna Małoletniego lub Instruktora praktycznej nauki zawodu, pracodawca dokona weryfikacji wskazanej osoby w Rejestrze Sprawców Przepięstw na Tle Seksualnym.

1.2. Pracownik ma obowiązek dostarczyć Pracodawcy informację z Krajowego Rejestru Karnego, w zakresie przestępstw określonych w rozdziale XIX (przestępstwa przeciwko życiu i zdrowiu) i XXV Kodeksu karnego (przestępstwo przeciwko wolności seksualnej i obyczajności), w art. 189a i art. 207 Kodeksu karnego oraz w ustawie z dnia 29 lipca 2005 r. o przeciwdziałaniu narkomanii (Dz. U. z 2023 r. poz. 1939), lub za odpowiadające tym przestępstwom czyny zabronione określone w przepisach prawa obcego. Pracownik ma obowiązek dostarczyć informację przed objęciem obowiązków związanych z opieką nad małoletnimi.

1.3. Wydruk z Rejestru oraz informacja z Krajowego Rejestru Karnego przechowywane są w aktach osobowych pracownika.

2. Ustanowienie zasad reagowania na wystąpienie sytuacji noszącej znamiona przemocy jakiegokolwiek rodzaju lub krzywdzenia małoletniego;

2.1. Kategorie zagrożeń

W ramach niniejszych Standardów wyróżnia się trzy kategorie zagrożeń wobec małoletnich:

- Podejrzenie przestępstwa (np. wykorzystanie seksualne, znęcanie się),
- Inne formy krzywdzenia niebędące przestępstwem (np. przemoc psychiczna, nadmierna presja),
- Zaniedbanie podstawowych potrzeb dziecka (np. brak opieki zdrowotnej, higieny, odpowiedniego odżywiania).

2.2. Zakres stosowania procedur interwencji

Procedury interwencji stosuje się w przypadku podejrzenia krzywdzenia przez:

- osoby dorosłe (np. pracowników, osoby trzecie),
- opiekunów prawnych,
- innych małoletnich.

2.3. Cel interwencji

Celem interwencji jest ochrona dziecka i zatrzymanie wszelkich form krzywdzenia.

2.4. Postępowanie w sytuacji bezpośredniego zagrożenia

W przypadku bezpośredniego zagrożenia życia lub zdrowia małoletniego należy natychmiast wezwać odpowiednie służby (Policję, pogotowie ratunkowe, Ośrodek Pomocy Społecznej) dzwoniąc pod numer 112 lub 998. Zgłoszenia dokonuje pracownik, który pierwszy uzyskał informację o zagrożeniu.

2.5. Obowiązek zgłoszenia do organów ścigania

Podejrzenie wykorzystania seksualnego dziecka poniżej 15. roku życia wymaga obowiązkowego zgłoszenia na Policję lub do prokuratury. Niewywiązanie się z tego obowiązku grozi karą pozbawienia wolności do 3 lat. W pozostałych przypadkach obowiązuje społeczny obowiązek zgłoszenia.

2.6. Dokumentowanie zgłoszeń

Każde podejrzenie lub zgłoszenie krzywdzenia (ze strony pracownika, małoletniego lub opiekuna) wymaga sporządzenia notatki służbowej i przekazania jej osobie odpowiedzialnej za interwencję. Notatka może mieć formę pisemną lub elektroniczną.

2.7. Osoba odpowiedzialna za interwencję

Osoba odpowiedzialna za interwencję informuje niezwłocznie pracodawcę o zgłoszeniu i podejmuje odpowiednie działania.

2.8. Postępowanie w przypadku konfliktu interesów

- Jeżeli zgłoszenie dotyczy osoby odpowiedzialnej za interwencję, interwencję prowadzi osoba wyznaczona przez Pracodawcę.
- Jeżeli sprawcą zgłoszonego krzywdzenia jest Członek Zarządu Spółki, Pracownik odpowiedzialny na Standardy Ochrony Młodości przekazuje zgłoszenie do członka Rady Nadzorczej Spółki, który podejmuje działania wskazane w pkt. 4.4. poniżej.

2.9. Zespół interwencyjny

Do zespołu interwencyjnego mogą zostać włączeni specjaliści, w szczególności psychologowie i pedagodzy ze szkoły ucznia.

2.10. Dokumentacja interwencji

Z każdej interwencji sporządza się kartę interwencji i dołącza ją do rejestru interwencji przechowywanego przez osobę odpowiedzialną za interwencję.

2.11. Informowanie szkół i opiekunów prawnych

W przypadku uczniów odbywających praktyki lub staże osoba odpowiedzialna za interwencję informuje szkołę ucznia oraz opiekunów prawnych o podjętej interwencji.

2.12. Obowiązek zachowania poufności

Osoby, które w związku z obowiązkami służbowymi uzyskały informacje o krzywdzeniu młodości, są zobowiązane do zachowania poufności – z wyjątkiem sytuacji przekazywania danych uprawnionym instytucjom.

2.13. Wsparcie eksperckie

W razie wątpliwości dotyczących dalszych działań, należy skonsultować się z Fundacją Dajemy Dzieciom Siłę (tel. 800 100 100).

3. Przeszkolenie pracowników pełniących funkcję opiekunów praktycznej nauki zawodu / stażów uczniowskich czy wszelkich innych dozwolonych form zatrudnienia nieletnich, w zakresie znajomości zapisów niniejszych Standardów Ochrony Młodości, poprzez szkolenia w wybranej formie.

4. Ustalenie zakresu odpowiedzialności pracowników w związku z niniejszymi Standardami;

4.1. Obowiązki pracodawcy:

- dbanie o tworzenie bezpiecznego środowiska w zakładzie pracy;
- wyznaczenie osoby/osób odpowiedzialnych za: standardy ochrony młodości, bezpieczeństwo w Internecie, prowadzenie interwencji,
- delegowanie zadań oraz odpowiedzialności związanych z realizacją standardów ochrony młodości.

4.2. Do obowiązków osoby **odpowiedzialnej za standardy ochrony młodości** należy:

- dbałość o udostępnienie standardów ochrony młodości na stronie internetowej pracodawcy (<https://mz.pl/firma/kodeks-etyki/>) oraz w systemie TQM.
- przygotowanie pracowników do stosowania standardów ochrony młodości,
- koordynowanie działań edukacyjnych,
- współpraca z innymi osobami wyznaczonymi w zakresie realizacji Standardów ochrony młodości,

- nadzór nad prowadzeniem przez Dział Zatrudnienia ewidencji pracowników, którzy zapoznali się ze Standardami ochrony małoletnich przed przystąpieniem do pracy albo po dokonaniu zmian w Standardach,
- monitorowanie realizacji wytycznych zawartych w standardach ochrony małoletnich, planowanie ewaluacji standardów z udziałem pracodawców, pracowników i małoletnich i ich aktualizacja,
- Przeprowadzenie ewaluacji stanu znajomości i przestrzegania standardów przez Pracowników,
- Oceny zgodności standardów z obowiązującymi przepisami prawnymi oraz sporządza raport zgodności.

4.3. Koordynator **bezpieczeństwa w Internecie** ma za zadanie zapewnić:

4.3.1. wytyczne w zakresie bezpiecznego korzystania z Internetu poprzez:

- monitoring przestrzegania zasad zawartych w Jednolitej polityce bezpieczeństwa teleinformatycznego, obowiązującej w GMZ,
- przedstawienie zasad bezpiecznego korzystania z Internetu małoletnim, i pracownikom oraz informowanie w przypadku jakichkolwiek aktualizacji ww. regulaminu (załącznik nr 1 do niniejszych Standardów Ochrony Małoletnich)

4.3.2. bezpieczne warunki korzystania z Internetu na urządzeniach pracodawcy poprzez:

- ustalenie zakresu blokowania dostępu do treści nielegalnych, szkodliwych i nieodpowiednich do wieku;
- instalację oraz regularną (przynajmniej raz w miesiącu) aktualizację sygnatur oprogramowania blokującego dostęp do treści nielegalnych, szkodliwych i nieodpowiednich do wieku małoletnich oraz aktualizację systemu operacyjnego urządzeń,
- ewaluację (co najmniej raz na rok) czy oprogramowanie zabezpieczające oraz blokujące i ustalony zakres jest adekwatny do potrzeb małoletnich oraz zmieniającego się otoczenia Internetu,
- sprawdzenie (co najmniej raz na miesiąc) czy na urządzeniach pracodawcy, użytkowanych przez małoletnie znajdują się treści nielegalne, szkodliwe i nieodpowiednie do wieku małoletnich.

4.4. Do osoby **odpowiedzialnej za interwencję** należy:

- przyjęcie zgłoszenia o wystąpieniu czynnika ryzyka zagrożenia dobra małoletniego;
- przyjęcie zgłoszenia o ujawnieniu symptomów krzywdzenia małoletniego lub krzywdzeniu małoletniego;
- przyjęcie zgłoszenia o incydentach lub zdarzeniach zagrażających dobru małoletniego;
- przekazanie zgłoszenia pracodawcy i dyrektorowi szkoły (jeśli małoletni uczęszcza do szkoły) lub gdy bezpośrednio zagrożone jest zdrowie lub życie małoletniego - niezwłoczne poinformowanie Policji i opiekunów prawnych (jeśli to nie oni stanowią zagrożenie);
- zainicjowanie interwencji zgodnie z opisanymi poniżej zasadami i monitorowanie współpracy ze szkołą,
- dokumentowanie zgłoszeń, ich weryfikacja oraz informowanie pracodawcy o wynikach poczynionych ustaleń
- prowadzenie rejestru interwencji w odpowiednio zabezpieczonym miejscu, do którego dostęp ma wyłącznie osoba odpowiedzialna za prowadzenie interwencji oraz pracodawca;
- współpraca w opracowaniu planu wsparcia małoletniego, uwzględniającego współpracę z dyrekcją szkoły, opiekunem prawnym małoletniego i innymi podmiotami,

- we współpracy z dyrekcją szkoły, do której uczęszcza małoletni, monitorowanie wsparcia udzielanego małoletniemu; w razie potrzeby skierowanie małoletniego i/lub jego opiekunów prawnych do instytucji oferujących: poradnictwo, konsultacje psychologiczne, terapię uzależnień, interwencje dla sprawców przemocy, grupy wsparcia, warsztaty umiejętności wychowawczych (będą to instytucje takie jak m.in. poradnie psychologiczno-pedagogiczne, ośrodki opieki psychologicznej i psychoterapeutycznej dla dzieci i młodzieży, ośrodki pomocy społecznej czy lokalne organizacje pozarządowe).

5. Ustalenie zasad współpracy, bezpiecznego traktowania oraz relacji między pracownikami, a małoletnimi.

Pracownik pełniący funkcję Opiekuna małoletniego oraz Instruktora praktycznej nauki zawodu zobowiązany jest do znajomości zapisów niniejszych Standardów, posiadania podstawowej wiedzy na temat czynników stanowiących zagrożenie dla osoby małoletniej oraz sposobów reagowania w sytuacji gdy zachodzi prawdopodobieństwo stosowania jakiegokolwiek formy przemocy wobec małoletniego.

§4 Podejrzenie krzywdzenia małoletniego

1. W przypadku podejrzenia krzywdzenia małoletniego, niezależnie od tego, czy sprawcą jest pracownik, opiekun prawny, czy inny małoletni, osoba odpowiedzialna za interwencję niezwłocznie przystępuje do zbierania informacji, przeprowadzając rozmowy z małoletnim, jego opiekunami prawnymi i /lub innymi osobami mającymi wiedzę o zdarzeniu. Celem tych działań jest ustalenie szczegółów incydentu i wpływu na zdrowie psychiczne i fizyczne małoletniego. Wszelkie ustalenia są zapisywane w karcie interwencji (załącznik nr 2 do niniejszych Standardów Ochrony Małoletnich).
2. W przypadku podejrzenia przestępstwa, osoba odpowiedzialna za interwencję sporządza zawiadomienie o możliwości popełnienia przestępstwa i kieruje je do odpowiednich służb (Policja, prokuratura). Jeśli zgłoszenie dotyczy innej formy krzywdzenia (np. przemoc domowa, zaniedbanie, krzywdzenie ze strony rówieśników), podejmowane są odpowiednie działania, w tym powiadomienie ośrodka pomocy społecznej lub wystąpienie do sądu rodzinnego.
3. Jeżeli sprawcą podejrzanym o krzywdzenie jest pracownik, zostaje on odsunięty od kontaktu z małoletnim, do czasu wyjaśnienia sprawy. W przypadku krzywdzenia niebędącego przestępstwem, rozważane są działania dyscyplinarne. Gdy sprawcą jest opiekun prawny, osoba odpowiedzialna za interwencję podejmuje działania zgodnie z opisanymi Standardami, które mogą obejmować interwencję w rodzinie lub powiadomienie odpowiednich instytucji.
4. W przypadku podejrzenia krzywdzenia rówieśniczego, przeprowadzana jest oddzielna rozmowa z osobami podejrzanymi o krzywdzenie oraz ich opiekunami prawnymi, a także z małoletnim będącym ofiarą. Ustalenia są zapisywane w karcie interwencji, a w razie potrzeby podejmowane są dodatkowe działania, w tym wsparcie ze strony szkoły lub instytucji.
5. W sytuacjach wymagających interwencji, osoba odpowiedzialna za interwencję podejmuje dalsze kroki zgodnie z zasadami wskazanym w §3, pkt. 4,4. oraz obowiązującym prawie.

§5 Upowszechnienie wiedzy o standardach ochrony małoletnich

1. Wszyscy Pracownicy mają obowiązek zapoznania się z niniejszym dokumentem, co potwierdzają pisemnie.

2. Wszyscy nowozatrudnieni Pracownicy potwierdzają zapoznanie się z dokumentem wraz z pozostałymi dokumentami udostępnianymi przez Dział Zatrudnienia w chwili podpisania umowy o pracę lub innej umowy cywilnoprawnej o współpracę.
3. Wszyscy małoletni, niezależnie od formy współpracy (praktyczna nauka zawodu / staż absolwencki / zatrudnienie małoletniego) potwierdzają na piśmie zapoznanie się z zapisami zawartymi w niniejszych Standardach.

§6 Indywidualny plan wsparcia małoletniego

1. W przypadku krzywdzenia małoletniego, osoba odpowiedzialna za interwencję opracowuje indywidualny plan działania, uwzględniający potrzeby dziecka, możliwości pracodawcy oraz – w razie potrzeby – współpracę z instytucjami lokalnymi. Może to obejmować kontakt ze szkołą, do której uczęszcza małoletni.
2. Plan powinien określać:
 - sposoby izolacji dziecka od sprawców i zapewnienie mu bezpiecznego funkcjonowania,
 - dostępne formy wsparcia, także poza miejscem praktyk czy pracy,
3. Plan należy tworzyć we współpracy z opiekunami prawnymi i omówić go z małoletnim. Jeśli sprawcą przemocy jest opiekun, plan ustala się z drugim, niekrzywdzącym opiekunem.
4. Indywidualny plan wsparcia opracowuje się również dla dzieci będących świadkami przemocy.

§7 Zasady bezpiecznego korzystania z Internetu

1. Pracodawca zapewniając małoletnim sprzęt komputerowy oraz dostęp do Internetu podejmuje działania zabezpieczające małoletnich przez dostępem do treści szkodliwych.
2. Środki bezpieczeństwa podnoszące bezpieczeństwo korzystania z Internetu stosowane w GMZ:
 - 2.1. Sprzęt komputerowy wydawany pracownikom oraz osobom małoletnim wyposażony jest w system antywirusowy, który jest automatycznie aktualizowany oraz monitorowany,
 - 2.2. Sprzęt komputerowy wydawany osobom małoletnim posiada mechanizmy ograniczające dostęp do Internetu. Blokowane są strony m.in. dotyczące:
 - poczty elektronicznej,
 - sklepów internetowych,
 - portali społecznościowych,
 - pornografii,
 - platform streamingowych.
 - 2.3. Sprzęt komputerowy wydawany osobom małoletnim posiada mechanizmy monitorujące przeglądane treści w Internecie. Osoba małoletnia otrzymując sprzęt komputerowy z dostępem do Internetu wyraża zgodę na takie monitorowanie.
 - 2.4. Sprzęt komputerowy wydawany osobom małoletnim ma zablokowaną możliwość korzystania z zewnętrznych nośników danych.
 - 2.5. Udzielenie dostępu do Internetu wymaga zapoznania się i akceptacji regulaminu przez małoletniego.

3. Warunkiem dopuszczenia małoletniego do korzystania ze sprzętu komputerowego jak i sieci internetowej jest zapoznanie się z zasadami bezpiecznego korzystania z Internetu, co małoletni potwierdza na piśmie.
4. W przypadku gdy dojdzie do naruszenia zasad bezpiecznego korzystania z Internetu lub ujawnienia treści nielegalnych, szkodliwych lub nieodpowiednich dla wieku, Pracodawca:
 - 4.1. Rejestruje, analizuje oraz dokumentuje każdy przypadek. Raport ze zdarzenia powinien zawierać dokładny opis zdarzenia, wskazanie uczestników i podjętych działań.
 - 4.2. Pracodawca zabezpiecza dowody zdarzenia (datę zdarzenia, treści wiadomości, dane nadawcy / adres stron www). Jeżeli nastąpiło naruszenie prawa, pracodawca ma obowiązek poinformowania Policji oraz przekazania materiału dowodowego.
 - 4.3. Żadne z powyższych działań nie może naruszać praw małoletniego, w tym prawa do prywatności.
5. Kolejność podejmowanych działań została ustalona i przedstawiona poniżej:
 - 5.1. Rozmowa z uczestnikiem zdarzenia, dostosowana do charakteru i wagi zdarzenia oraz roli uczestnika w zdarzeniu.
 - 5.2. Powiadomienie opiekuna prawnego uczestników zdarzenia oraz o podjętych przez Pracodawcę działaniach.
 - 5.3. W zależności od wagi sytuacji, Pracodawca powiadamia Policję lub sąd w przypadku popełnienia przestępstwa.
6. Działania naprawcze podejmowane przez Pracodawcę:
 - 6.1. W przypadku nielegalnych lub szkodliwych treści w Internecie, należy poinformować opiekunów małoletniego o możliwości ich usunięcia poprzez Dyżurnet.pl lub formularz na stronie, gdzie je opublikowano.
 - 6.2. Małoletni powinien zostać poinformowany o prawie do bycia zapomnianym – umożliwia ono usunięcie linków z Google na podstawie unijnego RODO.
 - 6.3. Jeśli naruszono prywatność małoletniego, można skorzystać ze strony <https://stopncii.org/> w celu usunięcia intymnych materiałów publikowanych bez zgody.

S8 Monitoring

1. Osoba odpowiedzialna za standardy ochrony małoletnich, raz na 2 lata przeprowadza wśród pracowników ewaluację stanu znajomości i przestrzegania standardów oraz potrzeby wprowadzenia zmian w tych standardach. Dopuszcza się osobne sprawdzenie stanu znajomości wśród małoletnich.
2. Na podstawie ewaluacji, o której mowa w ust. 1 powyżej oraz oceny zgodności standardów z obowiązującymi przepisami prawnymi, osoba odpowiedzialna za standardy ochrony małoletnich, sporządza raport, który następnie przekazuje pracodawcy. Część raportu stanowi ocena znajomości standardów przez pracowników, zestawienie zgłaszanych naruszeń standardów ochrony małoletnich oraz propozycje zmian.
3. Pracodawca w terminie jednego miesiąca od otrzymania raportu, o którym mowa w ust. 2 powyżej, podejmuje decyzje co do wprowadzenia zmian do standardów ochrony małoletnich i powierza przygotowanie zaktualizowanego dokumentu osobie odpowiedzialnej za standardy ochrony małoletnich.
4. Jeśli na podstawie raportu zostanie ustalone, że stopień znajomości standardów ochrony małoletnich jest niewystarczający, osoba odpowiedzialna za standardy ochrony małoletnich ma

obowiązek przeprowadzić szkolenie uzupełniające z zakresu standardów ochrony małoletnich dla pracowników.

5. Pracodawca wprowadza do standardów ochrony małoletnich niezbędne zmiany i ogłasza nowe brzmienie standardów.

§9 Zasady bezpiecznych relacji

Wszyscy Pracownicy GMZ traktują małoletnich z szacunkiem oraz uwzględniając ich godność i potrzeby. Stosowanie przemocy w jakiegokolwiek formie jest działaniem niedopuszczalnym. Zasady współpracy przebiegają zgodnie z obowiązującymi przepisami prawa, z treścią przepisów wewnętrznych oraz zgodnie z posiadanymi kompetencjami.

Zasady te dotyczą wszystkich pracowników oraz współpracowników, gości oraz każdej osoby dorosłej mającej kontakt z małoletnim na terenie Pracodawcy.

Każda osoba jest zobowiązana do zachowania profesjonalnej relacji oraz utrzymania odpowiedniego stylu komunikacji z małoletnim, tak by komunikaty były adekwatne do sytuacji, bezpieczne i uzasadnione.

Zasady postępowania z małoletnimi:

1. Traktuj wszystkich równo i z szacunkiem, niezależnie od tożsamości czy pochodzenia.
2. Unikaj faworyzowania dzieci i młodzieży.
3. Rozmawiaj z szacunkiem i cierpliwością.
4. Słuchaj uważnie i dostosuj odpowiedzi do wieku dziecka.
5. Dostosuj komunikację do potrzeb psychofizycznych małoletniego.
6. Zwracaj się po imieniu, zgodnie z preferencją dziecka.
7. Nie zawstydzaj, nie krzycz, nie lekceważ. Reaguj spokojnie, chyba że chodzi o bezpieczeństwo.
8. Zachowuj się odpowiednio. Unikaj wulgaryzmów, żartów seksualnych, zastraszania.
9. Informuj dziecko o decyzjach jego dotyczących, uwzględniaj jego zdanie.
10. Daj dziecku przestrzeń do mówienia o trudnych sytuacjach – zapewnij wsparcie.
11. Chronь prywatność dziecka – nie ujawniaj jego danych osobom nieuprawnionym.
12. Szanuj prywatność. Jeśli musisz złamać poufność, wyjaśnij dlaczego.
13. Działaj w widocznym miejscu. W razie spotkania sam na sam – powiadom innych.
14. Zakazane są jakiegokolwiek relacje seksualne lub intymne z małoletnimi, także komentarze, żarty i udostępnianie treści erotycznych.
15. Nie nagrywaj ani nie fotografuj małoletnich dla celów prywatnych bez zgody pracodawcy, opiekunów i dziecka.
16. Nie oferuj ani nie używaj alkoholu, papierosów czy narkotyków w obecności małoletnich.
17. Nie przyjmuj prezentów ani pieniędzy od małoletnich lub ich opiekunów; unikaj relacji zależności.
18. Zgłaszaj sytuacje zauroczenia między pracownikiem a małoletnim – reaguj z szacunkiem i rozważą.

Kontakt fizyczny z małoletnimi:

1. Przemoc fizyczna wobec małoletniego jest absolutnie niedopuszczalna.
2. Fizyczny kontakt jest dopuszczalny tylko wtedy, gdy wynika z potrzeb dziecka, jest stosowny do jego wieku, sytuacji i odbywa się za jego zgodą.
3. Każdy kontakt powinien być jawny, adekwatny i dobrze uzasadniony.
4. Nie dotykaj dziecka w sposób nieprzyzwoity ani nieodpowiedni.
5. Unikaj łaskotania, „zapasów”, brutalnych zabaw – mogą być źle odebrane.
6. Zawsze pytaj dziecko o zgodę, np. przed przytuleniem.
7. Zachowuj szczególną ostrożność w kontaktach z dziećmi, które doświadczyły przemocy – mogą szukać niewłaściwego kontaktu fizycznego. Reaguj stanowczo, ale z empatią.
8. Jeśli jesteś świadkiem niewłaściwego kontaktu fizycznego (swojego lub innej osoby), natychmiast zgłoś to zgodnie z procedurą.

Kontakty poza pracą i w Internecie

1. Kontakty z dziećmi powinny odbywać się wyłącznie w ramach obowiązków zawodowych.
2. Nie zapraszaj dzieci do swojego domu, nie spotykaj się z nimi prywatnie i nie kontaktuj przez prywatne kanały (telefon, social media).
3. W razie potrzeby kontaktuj się służbowo (telefon, e-mail), jawnie i za zgodą pracodawcy oraz opiekunów.
4. W kontaktach online zawsze powinien uczestniczyć jeszcze jeden dorosły.
5. W relacjach prywatnych (np. rodzinnych) obowiązuje poufność wobec informacji o innych dzieciach.
6. W sytuacji zagrożenia dziecka można odstąpić od powyższych zasad – należy wówczas niezwłocznie poinformować pracodawcę i sporządzić notatkę służbową.

Kontakty z małoletnimi Online:

1. Zachowuj świadomość, że Twoja aktywność w sieci może być widoczna dla dzieci i ich opiekunów.
2. Nie dodawaj dzieci do znajomych w mediach społecznościowych.
3. W komunikacji edukacyjnej online zapewnij obecność drugiej dorosłej osoby.

Ochrona małoletnich

1. W pracy z dzieckiem, które doznało krzywdzenia, zachowaj ostrożność i ucz je granic.
2. Gdy podejrzewasz krzywdzenie lub dziecko się zwierza:
 - Daj mu przestrzeń do wypowiedzenia się.
 - Wyraź, że mu wierzysz.

- Powiedz, że dobrze zrobili, mówiąc o tym.
- Podkreśl, że nie ponosi winy.
- Jasno potęp każdą formę przemocy.
- Poinformuj, że sprawą zajmą się odpowiednie osoby i zostaną podjęte działania w celu jego ochrony.

PREZES ZARZĄDU

Dariusz Pietyszuk



MOSTOSTAL ZABRZE



Regulamin dla osób małoletnich dotyczący bezpiecznego korzystania z sieci teleinformatycznych, w tym Internetu

1. Dostęp do sieci teleinformatycznej Grupy Mostostal Zabrze (zwanej dalej GMZ) jest możliwy tylko i wyłącznie z urządzeń służbowych.

Dostęp do gościnnej sieci Internet jest możliwy z dowolnego urządzenia – wymagane jest podanie hasła zabezpieczającego. Dodatkowo osoba korzystająca z dostępu do gościnnej sieci Internet musi potwierdzić swoją pełnoletność. Osoby niepełnoletnie nie mogą korzystać z tej sieci.

Sprzęt służbowy może być wykorzystywany tylko w miejscu pracy i nie powinien opuszczać wskazanego stanowiska pracy.

2. Osoba małoletnia uzyskując dostęp do sieci teleinformatycznej GMZ, w tym do Internetu musi przestrzegać zasad bezpieczeństwa opisanych w dokumentach systemu zarządzania GMZ. Są to w szczególności wytyczne dotyczące rozpoczęcia, zawieszenia i zakończenia pracy ze sprzętem mającym dostęp do sieci teleinformatycznej GMZ:

- użytkownik loguje się do systemu operacyjnego i programów z wykorzystaniem indywidualnego przyporządkowanego do niego identyfikatora i hasła,
 - każdorazowe wprowadzanie danych autoryzacyjnych winno odbywać się w sposób uniemożliwiający ich ujawnienie osobom postronnym,
 - w sytuacji tymczasowego zaprzestania pracy na skutek nieobecności przy stanowisku komputerowym użytkownik zobowiązany jest uruchomić wygaszacz ekranu chroniony hasłem (np. poprzez kombinację klawiszy „WIN” + ”L” w przypadku systemu operacyjnego Windows),
 - zabrania się instalowania jakiegokolwiek oprogramowania na służbowym sprzęcie komputerowym bez konsultacji z Działem Informatycznym GMZ,
 - po zakończeniu przetwarzania danych osobowych, użytkownik systemów zobowiązany jest do zamknięcia otwartych dokumentów i ewentualnie zapisanie zmian, poprawne wylogowanie się ze wszystkich programów i z systemów teleinformatycznych. Stacja robocza powinna być odłączona od źródła zasilania pod nadzorem osoby sprawującej pieczę nad małoletnim.
- W przypadku osób małoletnich zabronione jest podłączanie nośników zewnętrznych do służbowego sprzętu komputerowego – wprowadza się blokadę portów USB.

3. Zasady bezpiecznego korzystania z Internetu:

3.1. Chroń swoje dane.

Podstawą bezpieczeństwa w sieci jest ochrona swoich danych. Dlatego nie podawaj nikomu numeru PESEL, danych do logowania oraz informacji osobistych. Nawet, jeśli ufasz danej osobie, to nie przekazuj takich danych przez Internet. Zarówno poczta, jak i konta społecznościowe mogą zostać przejęte przez oszustów. Jeśli uważasz, że odpowiednio chronisz się podczas korzystania z Internetu, to nigdy nie masz pewności jak robią to inne osoby.

3.2. Zadbaj o hasła.

Wciąż wiele osób w zły sposób przechowuje swoje hasła. Nigdy nie zapisuj ich na swoim dysku, mailu, a nawet chmurze. Możesz mieć je zapisane w notesie lub wykorzystać do ich przechowywania specjalistyczne programy. Niezwykle istotne jest także to, aby hasła się nie powtarzały. Jeśli na przykład robisz zakupy w jakimś sklepie internetowym, a hasło do niego jest takie samo, jak do maila, banku i innych kont, to jesteś bardzo narażony na przechwycenie tych danych. Wystarczy, że sklep online będzie miał wyciek danych – hakerzy wykorzystają je do tego, aby Cię okraść. Ponadto konstruuj hasła, których złamanie jest bardzo ciężkie. Nie powinny one składać się ze słów słownikowych, muszą mieć różne znaki, a także cyfry oraz duże i małe litery. Każde hasło powinno być długie – im dłuższe, tym trudniej je rozszyfrować (zaleca się minimum 12 znakowe).

3.3. Zwracaj uwagę na strony, jakie odwiedzasz.

Zawsze weryfikuj czy dana witryna posiada certyfikat SSL (jeśli nie posiada wówczas pojawia się komunikat, że strona jest niezabezpieczona). Ponadto sprawdzaj czy adres URL jest poprawny. Oszuści często tworzą strony niezwykle podobne do oryginalnych, których adres delikatnie się różni. Oszuści cyfrowi często tworzą witryny, które wyglądają identycznie, jak strony banków, portali społecznościowych czy portali pocztowych i wyłudniają dane osób, które zrobią literówkę w adresie. To jednak nie jest jedyny sposób, aby przez pomyłkę przekazać dane do hakerów. Możesz kliknąć w link do płatności na stronie internetowej z ogłoszeniami, przejść do fałszywej witryny przez wiadomość e-mail albo SMS. Dlatego zawsze wpisuj adres banku ręcznie. Nie korzystaj z bankowości internetowej na służbowym sprzęcie.

3.4. Uważaj na spam i phishing

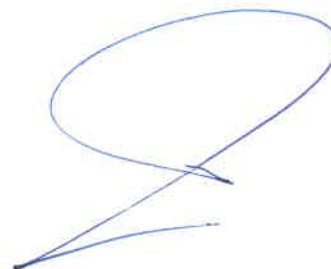
Wiadomości mailowe to źródło wielu ataków. Niekiedy przypominają maile od operatora komórkowego, banku, firmy energetycznej. Zawierają faktury albo linki. Zawsze sprawdzaj takie wiadomości przed kliknięciem. Pierwszym krokiem powinno być przeskanowanie maila systemem antywirusowym (niekiedy dzieje się to automatycznie). Potem sprawdź adres mailowy, z którego otrzymałeś wiadomość. Następnie przeczytaj tekst i zobacz, czy nie ma on rażących błędów, na przykład gramatycznych. Nigdy nie wchodź w podejrzone linki i nie pobieraj załączników. Zawsze możesz skontaktować się z nadawcą telefonicznie, aby upewnić się, że wiadomość pochodzi od niego.

3.5. Bądź ostrożny podczas zawierania znajomości

Coraz powszechniejsze jest korzystanie z Internetu w celu nawiązywania nowych znajomości. Fora internetowe, grupy dyskusyjne, społeczności na Facebooku, aplikacje randkowe. To wszystko narzędzia, dzięki którym można zyskać przyjaciół. Jednak są to miejsca, w których jest wielu oszustów, jacy chcą wyłudzić od Ciebie dane. Mogą przestać link lub plik ze szkodliwym oprogramowaniem lub podchwytliwie nakłonić Cię do tego, abyś sam wystąpił te dane w wiadomości. Dlatego bądź uważny i zawsze zwracaj uwagę na próby wyłudzenia danych oraz nie klikaj w podejrzone linki.

4. Środki bezpieczeństwa podnoszące bezpieczeństwo korzystania z Internetu stosowane w GMZ:

- 4.1. Sprzęt komputerowy wydawany pracownikom oraz osobom małoletnim wyposażony jest w system antywirusowy, który jest automatycznie aktualizowany oraz monitorowany,
- 4.2. Sprzęt komputerowy wydawany osobom małoletnim posiada mechanizmy ograniczające dostęp do Internetu. Blokowane są strony m.in. dotyczące:
- poczty elektronicznej,
 - sklepów internetowych,
 - portali społecznościowych,
 - pornografii,
 - platform streamingowych.
- 4.3. Sprzęt komputerowy wydawany osobom małoletnim posiada mechanizmy monitorujące przeglądane treści w Internecie. Osoba małoletnia otrzymując sprzęt komputerowy z dostępem do Internetu wyraża zgodę na takie monitorowanie.
- 4.4. Sprzęt komputerowy wydawany osobom małoletnim ma zablokowaną możliwość korzystania z zewnętrznych nośników danych.
- 4.5. Udzielenie dostępu do Internetu wymaga zapoznania się i akceptacji regulaminu przez małoletniego.



KARTA INTERWENCJI W PRZYPADKU PODEJRZENIA KRZYWDZENIA MAŁOLETNIEGO

1. DANE OSOBY ZGŁASZAJĄCEJ SYTUACJĘ (pracownika placówki):

Imię i nazwisko: _____

Stanowisko: _____

Data zgłoszenia: _____

Podpis: _____

2. DANE MAŁOLETNIEGO:

Imię i nazwisko dziecka: _____

Wiek / klasa / grupa: _____

Placówka: _____

3. OPIS SYTUACJI / ZDARZENIA / OBJAWÓW WSKAZUJĄCYCH NA MOŻLIWOŚĆ KRZYWDZENIA:

(opis faktów, obserwacji, zachowania dziecka, wypowiedzi, sygnałów fizycznych lub emocjonalnych, itp.)

4. PIERWSZE DZIAŁANIA PODJĘTE W PLACÓWCE:

Rozmowa z małoletnim

Rozmowa z rodzicami / opiekunami

Poinformowanie osoby odpowiedzialnej za procedury ochrony małoletnich

Inne (jakie?): _____

Nie podjęto działań (dlaczego?): _____

5. DECYZJA O DALSZYCH KROKACH:

- Zgłoszenie do dyrektora placówki
- Powiadomienie Policji
- Powiadomienie Ośrodka Pomocy Społecznej
- Wszczęcie procedury „Niebieskiej Karty”
- Konsultacja z psychologiem / pedagogiem
- Dokumentacja przekazana do zespołu interdyscyplinarnego
- Inne: _____

6. OSOBY ZAANGAŻOWANE W INTERWENCJĘ (wymienić imię, nazwisko, funkcję):

7. DATA I PODPISY OSÓB SPORZĄDZAJĄCYCH KARTĘ:

Data: _____

Podpis: _____

