ZESPÓŁ SZKÓŁ Nr 1
im. gen. Stefana Roweckiego "Grota"
18-300 ZAMBRÓW
Aleja Wojska Polskiego 31
tel. (086) 271 23 50, tel./fax 271 65 90
NIP 723-10-20-638 Regon 000188396

Załącznik nr 1 do Polityki bezpieczeństwa
w Zespole Szkół nr 1 w Zambrowie

Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych przetwarzanych w Zespole Szkół Nr 1 im gen. Stefana Roweckiego „Grota" w Zambrowie

I. Postanowienia ogólne

§ 1. 1. Niniejszy regulamin określa zasady podejmowania i realizowania pracy zdalnej oraz stacjonarnej w okresie epidemii w Zespole Szkół Nr 1 w Zambrowie im. gen. Stefana Roweckiego „Grota".

2. W regulaminie pod określeniem "pracownik" należy rozumieć zarówno osoby zatrudnione w ramach stosunku pracy, jak i współpracowników, na stale wykonujących zadania w ramach umów cywilnoprawnych wymagające dostępu do zasobów sprzętowych i informacyjnych szkoły.

II. Warunki pracy stacjonarnej w okresie zagrożenia epidemicznego

§ 2. 1. Dyrektor szkoły ustala grafik obecności w pracy, którego pracownik jest zobligowany bezwzględnie przestrzegać, ze względu na konieczność zapewnienia swojego oraz współpracowników bezpieczeństwa pracy.

2. Każda wizyta w pracy poza ustanowionym grafikiem musi zostać zgłoszona pracodawcy z co najmniej 1 dniowym wyprzedzeniem i uprzednio zatwierdzona przez pracodawcę.

3. Osoby przeziębione, kaszlące, gorączkujące, czujące duszności, powinny pozostać w domu i w zależności od samopoczucia podjąć pracę zdalną lub skontaktować się z lekarzem.

4. W celu zapewnienia bezpiecznych oraz komfortowych warunków pracy, pracownik powinien niezwłocznie zgłaszać pracodawcy, że źle się czuje, w szczególności, jeżeli objawy go niepokoją, bo są tożsame z tymi świadczącymi o zachorowaniu na COVID-19. W takim wypadku należy przerwać pracę i jak najszybciej opuścić budynek szkoły.

5. W przypadku zaobserwowania niepojących objawów u innego współpracownika lub gościa, należy niezwłocznie zgłosić ten fakt pracodawcy oraz osobom odpowiedzialnym za bezpieczeństwo w biurze.

6. Ze względu na obowiązek zakrywania nosa i ust weryfikacja tożsamości osób wchodzących do biura jest utrudniona. W związku z tym każdy pracownik jest zobligowany na żądanie pracownika ochrony lub innej wyznaczonej przez pracodawcę osobę do okazania dokumentu potwierdzającego tożsamości lub odsłonięcia twarzy, w zależności od instrukcji osoby weryfikującej tożsamość. W trakcie tego procesu należy zachować bezpieczną odległość (min. 2 metry).

7. Na stanowisku pracy należy zachować jak najwyższe standardy higieny. Możliwe często dezynfekować powierzchnie i przedmioty, których się dotyka, dezynfekować dłonie, unikać dotykania twarzy. Dotyczy to także sytuacji, gdy dotykało się tych samych dokumentów, które dotykały inne osoby.

8. Należy korzystać tylko i wyłącznie z wyznaczonego stanowiska pracy. Powinno ono być oddalone od stanowisk pracy innych osób co najmniej o 2 metry. Jednocześnie ustawienie sprzętu komputerowego i dokumentów powinno uwzględniać zapewnienie ich należytej ochrony przed osobami nieuprawnionymi.

9. Należy unikać zatłoczonych miejsc i podejmować działania minimalizujące ryzyko przebywania w takich miejscach bez zachowania zalecanego dystansu. Szczególnie dotyczy to przejść, wind, korytarzy, pomieszczeń socjalnych, toalet.

10. Należy bezwzględnie przestrzegać ograniczeń w zakresie liczby osób przebywających w pomieszczeniu, w szczególności ograniczać liczbę interesantów, tak by było możliwe zachowanie bezpiecznego dystansu pomiędzy wszystkimi osobami przebywającymi w pomieszczeniu.

11. W przypadku konieczności pracy z dokumentami papierowymi, należy stosować wobec zawartych w nich informacji najwyższe standardy ochrony, w szczególności zapewnić, aby nie były udostępniane (pozostawione bez opieki, pozostawione w sposób, który może być dowolnie modyfikowany i dostosowywany umożliwiający zapoznanie się z treścią) osobom postronnym. Te same standardy dotyczą wszelkich kopii dokumentów. Po zakończeniu pracy z dokumentem lub jego kopią, która już nie jest potrzebna i nie wymaga dalszego przechowywania, należy dokument niezwłocznie zniszczyć z wykorzystaniem niszczarki.

12. Wszystkie wydruki, skanowane lub kopiowane dokumenty powinny być niezwłocznie usuwane z urządzeń, w celu uniemożliwienia zapoznania się z nimi osobom postronnym.

13. Jeżeli praca odbywa się w trybie hybrydowym, tzn. częściowo w biurze, częściowo w domu, należy korzystać tylko z zatwierdzonych przez pracodawcę metod udostępniania plików oraz dokumentów, określonych w niniejszym Regulaminie.

14. W przypadku chwilowego opuszczania stanowiska pracy, należy blokować komputer i zabezpieczać dokumenty papierowe.

15. W przypadku opuszczania chwilowego pomieszczenia pracy, należy zamknąć pomieszczenie i zabrać klucz ze sobą.

16. Po otwarciu pomieszczeń i szafek, należy klucze usuwać z zamków, tzn., aby nie pozostawały w zamkach, umożliwiając ich kradzież, skopiowanie lub zamknięcie pomieszczenia przez osobę nieuprawnioną.

17. Jeżeli pomieszczenie jest współdzielone z innymi pracownikami, należy postępować zgodnie z przyjętą w organizacji polityką kluczy.

18. Po zakończeniu pracy należy wyłączyć urządzenia elektroniczne, a także schować wszystkie elektroniczne i papierowe nośniki informacji do szafek zamykanych na klucz. Zbędne nośniki należy zniszczyć. Zasada obowiązuje wszystkich bez wyjątków, ze względu na możliwość wprowadzenia odkażania powierzchni biurowych pod nieobecność pracowników.

III. Warunki pracy zdalnej

§ 3. 1. O możliwości podjęcia pracy zdalnej przez pracownika decyduje pracodawca.

2. Pracownik może zgłosić pracodawcy chęć podjęcia pracy zdalnej.

3. Warunki i zasady pracy zdalnej, w tym zakres i harmonogram wykonywanej pracy określa pracodawca, jednakże pracownik może także zaproponować własny harmonogram i zakres pracy, który będzie mógł realizować po uzyskaniu zgody pracodawcy.

4. W przypadku podjęcia pracy zdalnej pracownika obowiązują zasady pracy zdalnej określone w niniejszym Regulaminie.

5. Pracownik podejmując pracę zdalną zapewnia odpowiednie, zgodnie z niniejszym Regulaminem, warunki świadczenia tej pracy.

6. Jeżeli pracownik nie ma możliwości świadczenia pracy zdalnej z zapewnieniem właściwych zabezpieczeń, w szczególności ze względu na siłę wyższą (np. brak prądu lub Internetu), niezwłocznie zgłasza to pracodawcy i postępuje zgodnie z jego instrukcjami.

7. Złamanie zasad określonych w Regulaminie lub niedostosowanie się do postanowień niniejszego Regulaminu może stanowić naruszenie obowiązków pracowniczych. W przypadku osób realizujących zadania w oparciu o umowy cywilnoprawne postępowanie niezgodnie z niniejszym Regulaminem może oznaczać wykonanie zadania niezgodnie z przedmiotem umowy i z wymaganą przez pracodawcę starannością i zawodowym profesjonalizmem i skutkować rozwiązaniem umowy, a także przewidzianymi w umowie karami umownymi.

IV. Warunki jakie musi spełniać miejsce świadczenia pracy zdalnej

§ 4. 1. Pracownik musi zapewnić właściwe warunki umożliwiające mu skuteczną pracę zdalną z zachowaniem właściwego poziomu bezpieczeństwa informacji.

2. Niedozwolone jest podejmowanie pracy zdalnej w miejscach publicznych, jak kawiarnie, restauracje, galerie handlowe, gdzie osoby postronne mogłyby usłyszeć fragmenty służbowych rozmów lub zapoznać się z fragmentami wykonywanej pracy.

3. Pracując w domu należy zapewnić, aby domownicy nie mieli wglądu w wykonywaną pracę, w szczególności poprzez właściwe ustawienie ekranu komputera oraz smartfona, a także zapewnienie pracę z dokumentami w sposób uniemożliwiający wgląd.

4. Praca zdalna powinna odbywać się zgodnie z harmonogramem ustalonym z pracodawcą, co oznacza, że pracownik jest dostępny i realizuje swoje działania w ustalonych godzinach.

5. Odchodząc od komputera lub kończąc korzystanie z urządzeń IT należy upewnić się, że urządzenie zostało zablokowane.

V. Bezpieczeństwo pracy zdalnej i stacjonarnej

§ 5. Internet

1. Pracownik wykonuję pracę zdalną z wykorzystaniem urządzeń służbowych, tzn. otrzymanych od pracodawcy lub własnych.

2. Jeżeli pracodawca udostępnia pracownikowi modem Internetowy lub telefon służbowy z dostępem do Internetu, który może pełnić funkcję HotSpot, pracownik powinien korzystać w pierwszej kolejności z tych urządzeń.

3. W przypadku korzystania z domowej sieci WiFi, należy upewnić się, że została ona skonfigurowana w sposób minimalizujący ryzyko włamania, w szczególności:

1) korzystanie z Internetu powinno wymagać uwierzytelnienia, np. poprzez hasło;
2) hasło dostępu powinno składać się z co najmniej 8 znaków, w tym z dużych i małych liter oraz cyfr i znaków specjalnych;
3) jeśli to możliwe, należy zmienić login do panelu administracyjnego routera na własny;
4) dostęp do panelu administracyjnego routera jest możliwy wyłącznie z urządzeń znajdujących się w sieci domowej.

4. Porad i wsparcia w zakresie konfiguracji sieci domowej, w tym jej zabezpieczenia na potrzeby pracy zdalnej udziela informatyk zatrudniony w szkole (nauczyciel, wicedyrektor, dyrektor).

§ 6. Urządzenia służące do pracy zdalnej

1. Zabronione jest udostępnianie urządzeń wykorzystywanych do realizowania pracy zdalnej innym osobom, np. domownikom.

2. Praca zdalna powinna być realizowana z wykorzystaniem służbowego sprzętu, jak komputera stacjonarny, laptop, smartfon, tablet, itp.

3. Zgoda na pracę zdalną obejmuje zgodę na korzystanie ze służbowego sprzętu poza siedzibą pracodawcy.

4. Pracownik jest uprawniony także do zabrania komputera stacjonarnego do miejsca wykonywania pracy zdalnej, na czas wykonywania tej pracy.

5. Jeżeli z jakiś względów pracownik nie może wykonywać pracy zdalnej z wykorzystaniem służbowego sprzętu, zgłasza to pracodawcy, który może wydać zgodę na pracę z wykorzystaniem prywatnych urządzeń.

6. Urządzenie służbowe jest wydawane pracownikowi za protokołem.

7. Po otrzymaniu zgody na pracę zdalną i uzgodnieniu z pracodawcą z jakich urządzeń będzie korzystał pracownik w celu jej zrealizowania, pracownik niezwłocznie zgłasza ten fakt do działu IT.

8. Dział IT odnotowuje, które urządzania są wykorzystywane przez pracownika do pracy zdalnej, jeżeli to niezbędne, przeprowadza ich przegląd.

9. W przypadku, gdy przegląd jest niemożliwy, pracownik na żądanie inspektora ds. działu IT udostępnia urządzenie zdalnie w celu dokonania jego zdalnego przeglądu.

10. Przegląd urządzeń prywatnych jest obowiązkowy.

11. Minimalne wymagania w zakresie bezpieczeństwa:

1) na urządzeniu jest legalne i aktualne oprogramowanie;
2) zostały włączone automatyczne aktualizacje;
3) została włączona zapora systemowa;
4) został zainstalowany i działa w tle program antywirusowy;
5) zalogowanie do systemu operacyjnego wymaga uwierzytelnienia, np. poprzez indywidualny login i hasło użytkownika, kod PIN, token;
6) wyłączono autouzupełnianie i zapamiętywanie hasła w przeglądarce internetowej;
7) został zainstalowany program umożliwiający zaszyfrowanie i odszyfrowanie danych (np. 7- zip);
8) zostało ustawione automatyczne blokowanie urządzenia po dłuższym braku aktywności;
9) jeżeli urządzenie daje taką możliwość, praca jest wykonywana na koncie z ograniczonymi uprawnieniami.

12. Pracodawca może dodatkowo wymagać, aby urządzenie wykorzystywane do pracy zdalnej zawierało inne zabezpieczenia, jak:

1) zaszyfrowany dysk;
2) wyłączone porty pamięci zewnętrznych;

3) oprogramowanie służące monitorowaniu wykonywania pracy przez pracownika, wykorzystywane zgodnie z wymaganiami przepisów prawa pracy.

§ 7. Zabezpieczanie przekazywanych informacji

1. Do pracy zdalnej pracownik powinien wykorzystywać tylko i wyłącznie służbowe programy i systemy udostępnione mu przez pracodawcę.

2. Jeżeli jest niezbędne przesłanie informacji o charakterze poufnym, w szczególności danych osobowych, powinny zostać one zabezpieczone hasłem.

3. Jeżeli informacje poufne będą przekazywane z wykorzystaniem poczty e-mail, powinny zostać udostępnione w załączniku zabezpieczonym hasłem.

4. Zabezpieczeniu powinny podlegać wszelkiego rodzaju dane osobowe, niezależnie od ich charakteru, nawet jeżeli są to jedynie imiona, nazwiska czy adresy e-mail.

5. Hasło powinno zostać przekazane odbiorcy inną drogą komunikacji.

6. Hasło powinno być odpowiednio skomplikowane i niesłownikowe.

7. Dozwolone jest ustalenie stałego hasła na komunikację z jednym odbiorcą.

8. Rekomendowane metody zabezpieczania hasłem:

1) nadanie hasła do pliku, w którym są dane osobowe;
2) zabezpieczenie pliku lub plików poprzez kompresję z zabezpieczeniem archiwum wynikowego hasłem.

9. Każda wiadomość powinna być wysyłana z należytą starannością, polegającą w szczególności na sprawdzeniu, czy jest kierowana do odpowiedniego odbiorcy.

10. W przypadku wysyłania informacji do kilku odbiorców, którzy nie znają się wzajemnie i/lub ich adresy e-mail są adresami prywatnymi, należy skorzystać z opcji Ukrytej kopii (UDW/BCC), tzn. adresy wpisać w to pole.

11. Szczegółowe zasady korzystania z poczty e-mail określa odrębny regulamin.

12. Masowe wysyłki wiadomości e-mail należy realizować poprzez specjalne oprogramowanie udostępnione w tym celu przez pracodawcę.

13. Pracownik może także przekazywać pliki z informacjami chronionymi z wykorzystaniem udostępnionych przez pracodawcę serwerów sieciowych lub plików FTP.

14. Wykorzystywanie innych narzędzi do przesyłania i udostępniania plików (We Transfer, Googe Drive, DropBoX) może odbywać się tylko za zgodą pracodawcy, po wcześniejszym zabezpieczeniu hasłem plików.

§ 8. Zasady korzystania z dokumentów w formie papierowej

1. Zgodnie z obowiązującym u pracodawcy zasadami wszystkie dokumenty zawierające informacje poufne, w tym dane osobowe, powinny być przechowywane w szafach zamykanych na klucz w siedzibie pracodawcy.

2. Obowiązuje ogólny zakaz zabierania dokumentów lub ich kopii poza siedzibę pracodawcy.

3. Jeżeli do pracy zdalnej niezbędny jest dostęp do dokumentów papierowych, pracownik zgłasza do pracodawcy prośbę o możliwość ich skopiowania oraz zabrania do domu na czas wykonywania pracy zdalnej.

4. Po otrzymaniu zgody na piśmie lub w formie służbowej wiadomości e-mail, pracownik może sporządzić kopie niezbędnych dokumentów.

5. Zabronione jest zabieranie poza siedzibę pracodawcy oryginałów dokumentów.

6. Po skopiowaniu dokumentów pracownik przygotowuje ich zestawienie, zawierające informacje jakie dokumenty, w jakiej liczbie zostały skopiowane.

7. Informacja jest przekazywana pracodawcy.

8. W czasie przewożenia dokumentów do miejsca realizowania pracy zdalnej, należy zachować szczególną ostrożność, aby ich nie zgubić.

9. Praca z dokumentami nie może być wykonywana w miejscu publicznym (świetlica w szkole, kawiarnia, restauracja, galeria handlowa, itp.).

10. Po zakończeniu pracy, wszystkie dokumenty należy zwrócić pracodawcy, który weryfikuje ich kompletność.

VI. Szczególne sytuacje

§ 9. W przypadku zgubienia lub kradzieży sprzętu, dokumentów lub innych nośników informacji, należy niezwłocznie, w dniu zdarzenia zgłosić zdarzenie do pracodawcy a także inspektora ochrony danych.

§ 10. Należy niezwłocznie zgłaszać pracodawcy wszelkie podejrzenia naruszeń dla ochrony danych, jak pozostawione bez nadzoru wydruki, niezniszczone dokumenty, pozostawienie kluczy w drzwiach, pozostawienie niezabezpieczonego stanowiska pracy, utrata danych, udostępnienie danych osobie nieuprawnionej, itd. Należy zgłaszać każdą sytuację, która w opinii pracownika odbiega od przyjętej normy i obowiązujących standardów bezpieczeństwa. Do pracodawcy należy ocena ryzyka zdarzenia.

§ 11. Zmiana trybu i sposobu pracy nie zwalania z obowiązku zapewnienia ochrony danych osobowych i nie może wpływać na zmniejszenie lub ograniczenie wcześniej obowiązujących zabezpieczeń.

§ 12. Wszelkiego rodzaju problemy związane z możliwością zapewnienia ochrony danych, należy niezwłocznie zgłaszać, zgodnie z obowiązującą procedurą postępowania przy naruszeniach.

VII. Działania niedozwolone

§ 13. Niedozwolone jest:

1) udostępnianie innym osobom danych służących do uwierzytelnienia do systemów i/lub usług;

2) przekazywanie informacji chronionych, w szczególności danych osobowych bez zabezpieczenia hasłem, w szczególności w treści wiadomości e-mail;

3) przekazywanie hasła do zabezpieczonych informacji tą samą drogą komunikacji, którą przekazywany jest zabezpieczony hasłem plik lub pliki;

4) korzystanie z urządzeń, które nie zostały zatwierdzone przez pracodawcę;

5) odmówienie inspektorowi d.s. IT przeglądu urządzenia;

6) niszczenie dokumentów w domu;

7) udostępnianie służbowego sprzętu lub sprzętu wykorzystywanego do realizowania zadań służbowych innym osobom;

8) dzielenie się informacjami poufnymi z innymi osobami, w szczególności domownikami;

9) samodzielne zniszczenie dokumentów w domu;

10) logowanie się na konto innego użytkownika;

11) zabranie dokumentów bez pisemnej lub elektronicznej zgody pracodawcy;

12) zabranie oryginałów dokumentów;

13) niezwrócenie dokumentów;

14) niepotwierdzenie z pracodawcą zakresu zwróconych danych.

DYREKTOR
ZESPOŁU SZKÓŁ Nr 1
im. gen. Stefana Roweckiego „Grota"
w Ząbkowie
.....
mgr inż. Sławomir Baran