Załącznik nr 4 do Regulaminu pracy w II Liceum Ogólnokształcącym z Oddziałami Integracyjnymi im. C. K. Norwida w Tychach

# PROCEDURA OCHRONY DANYCH OSOBOWYCH W TRAKCIE SWIADCZENIA PRACY W FORMIE ZDALNEJ

1. Administrator zapewnia stałą pomoc techniczną związaną z wykorzystywaniem sprzętu powierzonego pracownikowi, możliwy jest również serwis obejmujący naprawy gwarancyjne, naprawy bieżące, a także zapewnia dostarczanie niezbędnych do funkcjonowania sprzętu środków eksploatacyjnych.
2. Praca zdalna może odbywać się wyłącznie w godzinach pracy biura, zgodnie z regulaminem pracy, ogólnie przyjętymi godzinami pracy Administratora oraz przedstawionym grafikiem pracy.
3. Powierzony sprzęt i oprogramowanie oraz środki łączności (komputery, programy, urządzenia biurowo-komunikacyjne itp.) mogą zostać użyte przez pracownika wyłącznie do celów służbowych, tak samo jak inne powierzone materiały techniczne (eksploatacyjne).
4. Pracownik zobowiązany jest do ochrony powierzonego sprzętu, oprogramowania, środków łączności przed uszkodzeniem, kradzieżą, zniszczeniem, a także przed nieuprawnionym użyciem oraz zabezpieczania danych informacji stanowiących tajemnicę przedsiębiorstwa oraz danych osobowych, dostępnych pracownikowi za pomocą powierzonego sprzętu, oprogramowania lub środków łączności.
5. Administrator wymaga od pracownika następujących zasad bezpieczeństwa dotyczących
	1. Miejsca świadczenia pracy:
		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, smartfona (lub innego urządzenia do przetwarzania danych), a także zapewnienie pracę z dokumentami w sposób uniemożliwiający wgląd.
		4. Odchodząc od komputera lub kończąc korzystanie ze służbowego smartfona należy upewnić się, że urządzenie zostało zablokowane.
	2. Sieci i Internetu
6. Pracownik wykonuję pracę zdalną z wykorzystaniem urządzeń służbowych, tzn. otrzymanych od Administratora.
7. Pracownik może wykonywać pracę zdalną na innym sprzęcie nie będącym własnością Administratora pod warunkiem implementacji na min polityk bezpieczeństwa oraz wydania zgody na takie użycie (zgodnie z pkt 3).
8. Jeżeli Administrator 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, niemniej dopuszcza się używanie własnych połączeń HotSpot.
9. W przypadku korzystania z domowej sieci WiFi, należy upewnić się, że została ona skonfigurowana w sposób minimalizujący ryzyko włamania, w tym korzystanie z Internetu wymaga uwierzytelnienia, np. poprzez silne hasło.
10. Jeśli to możliwe, należy zmienić login do panelu administracyjnego routera na własny oraz posiadać własne silne hasło do urządzenia.
11. Dostęp do panelu administracyjnego routera jest możliwy wyłącznie z urządzeń znajdujących się w sieci domowej.
12. Jeśli to możliwe dokonano aktualizacji oprogramowania routera.
13. Zastosowano wszystkie wytyczne działu IT dotyczące sieci domowych.
	1. Wykorzystywanego sprzętu
14. Zabronione jest udostępnianie urządzeń wykorzystywanych do realizowania pracy zdalnej innym osobom, np. domownikom.
15. Pracownik jest uprawniony także do zabrania komputera stacjonarnego do miejsca wykonywania pracy zdalnej, na czas wykonywania tej pracy.
16. Urządzenia służbowe jest wydawane pracownikowi za protokołem. Po otrzymaniu zgody na pracę zdalną i uzgodnieniu z Administratorem z jakich urządzeń będzie korzystał pracownik w celu jej zrealizowania, pracownik niezwłocznie zgłasza ten fakt do działu IT
17. Dział IT odnotowuje, które urządzania są wykorzystywane przez pracownika do pracy zdalnej, jeżeli to niezbędne, przeprowadza ich przegląd.
18. W przypadku, gdy przegląd jest niemożliwy, pracownik na żądanie pracownika działu IT udostępnia urządzenie zdalnie (z wykorzystaniem zaproponowanego przez dział IT narzędzia), w celu dokonania jego zdalnego przeglądu.
19. Przegląd urządzeń prywatnych jest obowiązkowy.
20. Minimalne wymagania w zakresie bezpieczeństwa zostały określone w następujący sposób:
	* + 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;
			10. Administrator może dodatkowo wymagać, aby urządzenie wykorzystywane do pracy zdalnej zawierało inne zabezpieczenia, jak np. zaszyfrowany dysk;
			11. Nie wykonuje się kopii danych służbowych z komputerów prywatnych;
			12. Administrator może wymagać instalacji oprogramowania służącego monitorowaniu wykonywania pracy przez pracownika i wykorzystywania zgodnie z wymaganiami przepisów prawa pracy.
	1. Danych:
21. Do pracy zdalnej pracownik powinien wykorzystywać tylko i wyłącznie służbowe programy i systemy udostępnione mu przez Administratora.
22. Jeżeli jest niezbędne przesłanie informacji o charakterze poufnym, w szczególności danych osobowych, powinny zostać one zabezpieczone hasłem.
23. Jeżeli informacje poufne będą przekazywane z wykorzystaniem poczty e-mail, powinny zostać udostępnione w załączniku zabezpieczonym hasłem.
24. Zabezpieczeniu powinny podlegać wszelkiego rodzaju dane osobowe, niezależnie od ich charakteru, nawet jeżeli są to jedynie imiona, nazwiska, czy adresy e-mail.
25. Hasło powinno zostać przekazane odbiorcy inną drogą komunikacji.
26. Hasło powinno być odpowiednio skomplikowane i niesłownikowe.
27. Dozwolone jest ustalenie stałego hasła na komunikację z jednym odbiorcą.
28. Każda wiadomość powinna być wysyłana z należytą starannością, polegającą w szczególności na sprawdzeniu, czy jest kierowana do odpowiedniego odbiorcy.
29. 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.
30. Pracownik może także przekazywać pliki z informacjami chronionymi z wykorzystaniem udostępnionych przez Administratora serwerów sieciowych lub plików.
31. Jakakolwiek komunikacja w sieci internet i transmisja danych musi być zabezpieczona i szyfrowana (w tym VPN, przesyłanie plików i wiadomości)
32. Wykorzystywanie innych narzędzi do przesyłania i udostępniania plików (weTransfer, Googe Dirve, DropBoX) jest zabronione
33. Zabrania się przesyłania danych innymi kanałami komunikacji niż przyjęte przez Administratora
34. Zabrania się przenoszenia danych na niezabezpieczonych nośnikach
	1. Dokumentów papierowych
35. Zgodnie z obowiązującym u Administratora zasadami wszystkie dokumenty zawierające informacje poufne, w tym dane osobowe, powinny być przechowywane w szafach zamykanych na klucz w siedzibie Administratora.
36. Obowiązuje ogólny zakaz zabierania dokumentów lub ich kopii poza siedzibę Administratora o ile nie jest on niezbędny na potrzeby pracy zdalnej
37. W przypadku konieczności zabierania dokumentów poza siedzibę Administratora pracownik zgłasza do przełożonego prośbę o możliwość ich skopiowania oraz zabrania do domu na czas wykonywania pracy zdalnej.
38. Po otrzymaniu zgody, pracownik może sporządzić kopie niezbędnych dokumentów.
39. Zabronione jest zabieranie poza siedzibę Administratora oryginałów dokumentów.
40. Po skopiowaniu dokumentów pracownik przygotowuje ich zestawienie, zawierające informacje jakie dokumenty, w jakiej liczbie zostały skopiowane.
41. Informacja jest przekazywana Administratorowi.
42. Podczas przewożenia dokumentów do miejsca realizowania pracy zdalnej, należy zachować szczególną ostrożność, aby ich nie zgubić.
43. Praca z dokumentami nie może być wykonywana w miejscu publicznym (świetlica w szkole, kawiarnia, restauracja, galeria handlowa, itp.).
44. Po zakończeniu pracy, wszystkie dokumenty należy zwrócić Administratorowi, który weryfikuje ich kompletność.
45. Zabronione jest niszczenie dokumentów poza siedzibą Administratora, w tym notatek wytworzonych podczas pracy zdalnej.
46. Wszystkie kopie dokumentów oraz dokumenty robocze muszą być niszczone w siedzibie Administratora
47. W przypadku, jeżeli wymienione zasady nie są do zrealizowania/spełnienia przez pracownik ze wzglądów mieszkaniowych lub innych pracownik zobowiązany jest poinformować o tym Administratora a ten podejmuje decyzję co do formy pracy, jej zakresu lub innych warunków do spełnienia.
48. Podczas pracy zdalnej zachowują ważność wszystkie zapisy Polityk Bezpieczeństwa oraz innych procedur pracy.
49. W przypadku występowania konfliktów pomiędzy niniejsza polityką a pozostałymi procedurami na potrzeby pracy zdalnej za istotniejsze uznaje się zapisy niniejszej procedury.