Załącznik Nr 3

do Regulaminu wykonywania pracy zdalnej

przez pracowników Urzędu Miasta Świnoujście

**ZASADY KORZYSTANIA Z URZĄDZEŃ TECHNICZNYCH**

**W ZWIĄZKU Z PRACĄ ZDALNĄ**

**Przedmiot regulacji i jej adresaci**

**§ 1.**1. Niniejsza cześć określa zasady instalacji, inwentaryzacji, konserwacji, aktualizacji oprogramowania i serwisu narzędzi pracy powierzanych pracownikom w związku z wykonywaniem przez nich pracy zdalnej, z uwzględnieniem ochrony znajdujących się na powierzonych narzędziach pracy danych osobowych.

2. Niniejsza, cześć znajdzie zastosowanie do osób zatrudnionych w oparciu o umowę o pracę, jak i do stosunków pracy nawiązanych na innej podstawie niż umowa o pracę.

**Inwentaryzacja**

**§ 2.**1. Powierzone w związku z pracą zdalną pracownikowi narzędzia pracy podlegają inwentaryzacji w ramach ewidencji powierzonych narzędzi pracy, według wzoru określonego w załączniku Nr 1 do niniejszych zasad. Prowadzenie ewidencji nie zwalnia z obowiązku prowadzenia inwentaryzacji wymaganych przepisami ogólnymi.

2. Powierzenie narzędzi pracy następuje poprzez protokół przekazania określony w załączniku Nr 2, w którym strony, w tym pracownik, mogą wpisać uwagi dotyczące powierzonych narzędzi.

3. Protokół, o którym mowa w ust. 2 jest podpisywany w 2 egzemplarzach przez pracownika Biuro Technologii Informacyjnych.

4. W przypadku trwałego zakończenia używania narzędzia pracy lub na żądanie pracodawcy, powierzone narzędzia pracy podlegają zwrotowi na podstawie protokołu przekazania określonego w załączniku Nr 2, zawierającego datę i podpisy pracownika oraz pracownika Biura Technologii Informacyjnych.

5. Biuro Technologii Informacyjnych prowadzi ewidencję powierzonych narzędzi pracy na podstawie protokołów przekazania.

**Bezpieczeństwo pracy zdalnej – Internet**

**§ 3.**1. Pracownik wykonuje pracę zdalną z wykorzystaniem urządzeń służbowych, tzn. otrzymanych od pracodawcy.

2. Jeżeli pracodawca udostępnia pracownikowi modem internetowy lub telefon służbowy z dostępem do Internetu, który może pełnić funkcję HotSpot, pracownik korzysta z tych urządzeń do połączeń z Internetem. Korzystanie z domowej sieci internetowej odbywa się za zgodą i wiedzą pracodawcy.

3. Zabrania się łączenia z publicznych, dostępnych HotSpot`ów oraz z innych nieznanych sieci, co do których reputacji nie jesteśmy pewni (np. przypadkowa dostępna bez hasła sieć wi-fi).

4. W przypadku korzystania z domowej sieci, należy skonfigurować domowy router na maksymalnie bezpieczne ustawienia:

1. **bezwzględnie należy zmienić domyślne hasło i jeśli to możliwe również login do logowania do panelu ustawień routera, ustalając hasło, należy zadbać o jego siłę;**
2. **silne** hasło dostępu, powinno składać się co najmniej z 12 znaków, w tym z dużych i małych liter oraz cyfr i znaków specjalnych;
3. **w routerze powinna być wyłączona możliwość zarządzania zdalnego routerem – aby d**ostęp do panelu administracyjnego routera był możliwy wyłącznie z urządzeń znajdujących się w sieci domowej, można również rozważyć zmianę domyślnego adresu routera na inny;
4. **DNS routera jest ustawiony zgodnie z wymaganiami naszego dostawcy internetu lub na DNS Google: 8.8.8.8 i 8.8.4.4;**
5. dla sieci przewodowej, stacja robocza/komputer, powinna być podłączona bezpośrednio do routera (a nie np. przez telefon VoIP);
6. dla sieci bezprzewodowej (wi-fi) nie należy korzystać ze standardu WEP **(Wired Equivalent Privacy), należy korzystać z najwyższego z dostępnych standardów na używanym urządzeniu/routerze np. WAP3/WAP2 (Wi-Fi Protected Access ver.3 lub 2) lub WAP   
   (Wi-Fi Protected Access), zaś połączenie powinno wymagać uwierzytelnienia np. poprzez silne hasło dostępu oraz nieoczywisty login, nieoczywisty login nie jest nazwą własną (np. imieniem) nie jest nazwą punktu dostępowego/routera;**
7. **jeśli to możliwe, należy wyłączyć w routerze „rozgłaszanie SSID”, aby nie był on widoczny dla osób postronnych, w przypadku pierwszego połączenia może koniecznym okazać się włączenie „rozgłaszania SSID” do nawiązania połączenia i wyłączenie go gdy połączenie jest nawiązane i zapisane w komputerze;**
8. **jeśli to możliwe, należy włączyć filtrowanie MAC, aby utrudnić urządzeniom innym niż urządzenia użytkownika połączenie z siecią wi-fi;**
9. **należy rozważyć włączenie izolacji klientów – aby podłączone do routera urządzenia nie mogły się między sobą komunikować.**

5. Porad i wsparcia w zakresie konfiguracji sieci domowej, w tym jej zabezpieczenia na potrzeby pracy zdalnej udziela Biuro Technologii Informacyjnych.

6. W każdej sytuacji zastosowanie mają także inne ograniczenia ujęte w polityce bezpieczeństwa obowiązujące w Urzędzie.

**Urządzenia służące do pracy zdalnej**

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

2. Praca zdalna jest realizowana z wykorzystaniem służbowego sprzętu, jak komputer stacjonarny, laptop.

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 protokolarnie.

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 Biura Technologii Informacyjnych.

8. Biuro Technologii Informacyjnych 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 pracownika Biura Technologii Informacyjnych udostępnia urządzenie zdalnie w celu dokonania jego zdalnego przeglądu.

10. Przegląd urządzeń prywatnych, na których wykorzystanie pracodawca wyraził zgodę, jest obowiązkowy.

11. Minimalne wymagania w zakresie bezpieczeństwa:

1. na urządzeniu jest legalne i aktualne oprogramowanie;
2. zostały włączone automatyczne aktualizacje, chyba że Biuro Technologii Informacyjnych wyraża zgodę na wyjątek w tym zakresie;
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. został zainstalowany program umożliwiający zabezpieczenie danych hasłem (np. 7-zip);
7. zostało ustawione automatyczne blokowanie urządzenia po braku aktywności przez czas 5 minut;
8. jeżeli urządzenie daje taką możliwość, praca jest wykonywana na koncie z ograniczonymi uprawnieniami;
9. zabrania się wykonywania screen-shotów (zrzutów ekranu), nagrywania ekranu i/lub nagrywania aktywności klawiatury i myszy, chyba że Biuro Technologii Informacyjnych wyraża zgodę na wyjątek w tym zakresie;
10. łącząc się klientem VPN z siecią Urzędu zabrania się zapamiętywania hasła użytkownika w kliencie VPN;
11. zabrania się, podczas połączenia VPN skanowania sieci, podatności etc;
12. zabrania się, podczas połączenia VPN korzystania z innych serwisów internetowych wymagających uwierzytelnienia użytkownika, w szczególności prywatnej bankowości internetowej.

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.

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 pracownikowi Biura Technologii Informacyjnych 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. logowanie się na konto innego użytkownika;
10. zabranie dokumentów bez pisemnej lub elektronicznej zgody pracodawcy.

**Instalacja oprogramowania**

**§ 5.**1. Wszelkie oprogramowanie niezbędne do wykonywania obowiązków zawodowych podlega na danym narzędziu pracy instalacji dokonywanej przed powierzeniem pracownikowi danego narzędzia pracy.

2. Instalacji lub zmiany oprogramowania, o którym mowa w ust. 1, dokonuje pracownik Biura Technologii Informacyjnych lub na pozytywnie rozpatrzony wniosek pracownika.

3. Pracownik nie może na powierzonych narzędziach pracy instalować żadnego własnego oprogramowania.

**Aktualizacja oprogramowania**

**§ 6.**1. Pracownik ma obowiązek na bieżąco aktualizować oprogramowanie zainstalowane na powierzonych narzędziach pracy, postępując według wskazówek przesłanych przez dostawcę oprogramowania.

2. O wszelkich wątpliwościach dotyczących bieżących aktualizacji oprogramowania, w tym o podejrzeniu wystąpienia zagrożeń w związku z taką aktualizacją, pracownik ma obowiązek niezwłocznie powiadomić kierownika Biura Technologii Informacyjnych.

**Przeglądy stanu technicznego**

**§ 7.**1. Pracownicy Biura Technologii Informacyjnych mają prawo dokonywać przeglądów stanu technicznego powierzonych pracownikowi narzędzi pracy w miejscu i czasie ustalonym przez strony.

2. W razie braku porozumienia co do miejsca i czasu dokonywania przeglądów decyzję o miejscu i czasie ich dokonania podejmuje pracodawca.

**Niezbędne naprawy**

**§ 8.**1. Niezależnie od prawa do dokonywania przeglądów, o których mowa w § 7, pracownik ma prawo zgłaszania do Biura Technologii Informacyjnych wszelkich zdarzeń uniemożliwiających prawidłowe korzystanie z powierzonego narzędzia pracy, a w szczególności:

* 1. braku możliwości uruchomienia danego sprzętu;
  2. braku lub awarii jakichkolwiek urządzeń towarzyszących powierzonemu sprzętowi;
  3. znaczącemu zmniejszeniu prędkości działania urządzenia, przez dłuższy czas.

2. Zgłoszenia, o których mowa w ust. 1, pracownik dokonuje pisemnie poprzez wiadomość e-mail wysłaną ze służbowego adresu e-mail na adres **e-mail bti@um.swinoujscie.pl**. Jeżeli dokonanie zgłoszenia w ten sposób nie jest możliwe, pracownik może takiego zgłoszenia dokonać osobiście.

3. Kierownik Biura Technologii Informacyjnych odpowiada za rozwiązanie problemu przedstawionego przez pracownika bez zbędnej zwłoki.

4. W związku z dokonanym zgłoszeniem, o którym mowa w ust. 1, pracownikowi można przyznać zastępcze narzędzie pracy na zasadach określonych w § 1.

**Wezwanie pracownika na teren zakładu pracy**

**§ 9.**1. Pracownik może zostać wezwany na teren zakładu pracy w celu dokonania na powierzonym mu sprzęcie niezbędnych dodatkowych czynności w zakresie dodatkowej instalacji, aktualizacji, konserwacji, czy też napraw.

2. Fakt przekazania powierzonego narzędzia pracy przez pracownika, w związku z wezwaniem, o którym mowa w ust. 1, należy odnotować w protokole przekazania określonym w załączniku Nr 2.

Załącznik Nr 1

**Ewidencja powierzonych narzędzi pracy w związku z pracą zdalną w Urzędzie Miasta Świnoujście**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Imię i nazwisko pracownika, któremu powierzono narzędzie** | **Powierzone narzędzia (rodzaj, nazwa, model)** | **Data powierzenia** | **Data zwrotu** | **Numer protokołu przekazania stanowiącego podstawę powierzenia/zwrotu** | **Uwagi** |
|  |  |  |  |  |  |
|  |  |  |  |  |
| (...) |  |  |  |  |  |
| (...) |  |  |  |  |  |
| Osoba odpowiedzialna za prowadzenie protokołu | |  | | | |

Załącznik Nr 2

**Protokół przekazania narzędzi powierzonych w Urzędzie Miasta Świnoujście**

**Numer:** ……………………………

Na podstawie ………………………….. przekazuję:

Pani/Panu……………………………….……………………………………………………......

pracownikowi wydziału/biura …………………………………………………………………...

niżej wymieniony sprzęt:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Nazwa** | **Nr seryjny** | **Akcesoria\*** | **Data powierzenia**  **(podpis)** | **Data zwrotu**  **(podpis)** | **Uwagi** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

miejscowość, data …….………………………….………………………

imię, nazwisko …….………………………….………………………

adres zamieszkania pracownika …….………………………….………………………

podpis pracownika …….………………………….………………………