Załącznik nr 3
do zarządzenia Rektora
nr 13/2019/2020
z dn. 25 sierpnia 2020 r.

Zasady przetwarzania danych osobowych w komunikacji pracy zdalnej

I. OTOCZENIE PRACY

A. Bezpieczeństwo domowej sieci

1. Upewnij się, że dostęp do panelu konfiguracyjnego urządzenia sieciowego oraz dostęp do rozgłaszanej sieci bezprzewodowej zabezpieczone są silnym hasłem, którym nie jest hasło domyślne, zdefiniowane przez producenta.

2. Zweryfikuj, czy wersja oprogramowania Twojego urządzenia sieciowego jest aktualna, i ewentualnie dokonaj aktualizacji.

3. Wyłącz możliwość konfiguracji swojego sprzętu sieciowego z urządzeń znajdujących się poza siecią LAN lub ogranicz taką możliwość tylko do zdefiniowanych adresów IP. W większości wypadków, w zależności od wykorzystywanego sprzętu, takiej konfiguracji dokonasz z wykorzystaniem funkcjonalności ACL (Access Control List). Jeżeli nie wiesz jak to zrobić, a wątki w tym temacie znalezione w Internecie nie są wystarczające, poproś o pomoc dział IT.

4. Zdefiniuj urządzenia, które mogą uzyskać dostęp do Twojej sieci, np. z wykorzystaniem filtracji adresów MAC.

B. Bezpieczeństwo obszaru przetwarzania

1. Nie prowadź służbowych rozmów telefonicznych, w tym wideokonferencji, w miejscach narażonych na brak poufności wymienianych informacji.

2. Pamiętaj, aby nie udostępniać służbowych urządzeń osobom postronnym, w tym znajomym, dzieciom lub innym członkom rodziny.

3. Nie zapominaj o bezpiecznym przechowywaniu dokumentacji w formie papierowej. W tym celu staraj się korzystać z mebli zamykanych na klucz.

4. Zapewnij bezpieczne niszczenie dokumentów papierowych. Jeżeli nie dysponujesz niszczarką dokumentów, lepszym rozwiązaniem będzie ich utylizacja po powrocie do biura, ale nie zapominaj, żeby na czas pracy zdalnej przechowywać je bezpiecznie.

C. Bezpieczeństwo stanowiska pracy

1. Unikaj spożywania posiłków i napojów w czasie wykonywania swojej pracy przy sprzęcie elektronicznym. Miej na uwadze, że serwis lub wymiana sprzętu, np. na skutek zalania, w obecnej sytuacji mogą być bardzo utrudnione.

2. Upewnij się, że osoby postronne nie mają wglądu w treści wyświetlane na ekranie. Zadbaj o odpowiednie ustawienie ekranu lub zastosuj filtr prywatyzujący.

3. Nie zapominaj o polityce czystego ekranu, w tym o konieczności blokowania konta systemowego przed każdorazowym odejściem od stanowiska pracy. Dodatkowo uruchom wygaszacz ekranu, który taką czynność wykona automatycznie w razie braku Twojej aktywności.

II. SPRZĘT I SYSTEMY INFORMATYCZNE

A. Procedury bezpiecznego logowania

1. Upewnij się, że dostęp do Twojego komputera jest możliwy tylko i wyłącznie z wykorzystaniem indywidualnego identyfikatora oraz hasła. Nie zapominaj o ustawieniu PIN-u lub innej formy uwierzytelniania dla telefonu wykorzystywanego do celów służbowych.

2. Pamiętaj o zakazie udostępniania osobom trzecim haseł oraz o konieczności przechowywania ich w miejscach gwarantujących poufność.

3. Staraj się budować silne hasła, tj. długie i złożone, które nie będą ciągiem znajdujących się obok siebie znaków na klawiaturze ani nie będą oparte na prostych skojarzeniach, np. numer telefonu, data urodzin, imiona lub nazwiska. Nie zapominaj o cyklicznej zmianie swoich haseł.

B. Bezpieczne przechowywanie danych

1. Upewnij się, że nośniki Twoich urządzeń mobilnych, w tym komputera, telefonu lub tabletu, zostały zaszyfrowane.

2. Nie zapominaj o szyfrowaniu zewnętrznych kart pamięci, a także innych nośników danych, takich jak pendrive lub dysk zewnętrzny.

3. Wybierz bezpieczną formę uwierzytelniania do odszyfrowania nośników. Najpopularniejszą formą uwierzytelniania, a zarazem jedną z bezpieczniejszych, jest hasło.

4. Nie umieszczaj danych w publicznych chmurach obliczeniowych, komunikatorach lub innych usługach dostępnych w sieci, które nie są autoryzowane przez WSFiP.

5. Staraj się nie utrwalać danych na lokalnym dysku komputera. Do tego celu wykorzystuj tylko i wyłącznie wskazane przez WSFiP zasoby sieciowe, które podlegają wykonywaniu kopii zapasowych.

6. Stosuj rozwiązania umożliwiającego zdalne zarządzanie urządzeniami mobilnymi, w tym ich zdalne zlokalizowanie lub przywrócenie do stanu fabrycznego, np. MDM(Mobile Device Management).

7. Jeżeli pracujesz na urządzeniu prywatnym, poproś ADO, WSFiP o regulamin wszystkich **zasad konfiguracji sprzętu**.

C. Ochrona przed cyberatakami

1. Upewnij się, że Twoje urządzenia zostały wyposażone w uruchomione i aktualne oprogramowanie antywirusowe.

2. Sprawdź, czy wersja Twojego systemu operacyjnego jest wspierana przez producenta, np. Windows XP lub Windows 7, czy może takie wsparcie już utraciła. np. Windows XP i Windows 7, takiego wsparcia już nie ma.

3. Zweryfikuj, czy systemy, z których korzystasz, w tym system operacyjny oraz system antywirusowy, są aktualizowane.

4. Upewnij się, że na Twoim komputerze została uruchomiona **zapora sieciowa**.

5. Nigdy **nie korzystaj z uprawnień administracyjnych** do realizowania swoich codziennych obowiązków. Takie konta powinny być uruchamiane tylko doraźnie, w razie potrzeby.

6. Nie pobieraj ani nie instaluj oprogramowania bez zgody działu IT WSFiP.

III. STAN OSOBOWY

A. Procedury bezpieczeństwa

1. Zweryfikuj, czy masz dostęp do polityk i procedur obowiązujących w WSFiP oraz przypomnij je sobie.

2. Upewnij się, że wiesz, z kim możesz skontaktować się na wypadek nieprzewidzianej awarii lub incydentu.

3. Nie naprawiaj sprzętu, na którym znajdują się dane służbowe, z wykorzystaniem wsparcia podmiotów zewnętrznych bez uzyskania wcześniejszej zgody organizacji.

4. Nie drukuj dokumentów służbowych w punktach ksero lub z pomocą innych podmiotów/osób trzecich.

5. Nie zapominaj o zagrożeniach w sieci, w tym phishingu, na które Twoja sieć domowa może być bardziej podatna niż sieć firmowa.

6. Dokładnie **weryfikuj nadawców** wiadomości mailowych, a w razie wątpliwości nie otwieraj załączników oraz hiperłączy znajdujących się w tekście. Pamiętaj, że zawsze możesz zadzwonić i potwierdzić intencje osoby.

7. Szyfruj załączniki wiadomości mailowych, a hasło wysyłaj zawsze inną formą kontaktu, np. SMS.

8. Nie wysyłaj wiadomości służbowych na swoje prywatne konta mailowe.

9. Nie ufaj stronom internetowym, na których nie zaimplementowano protokołu szyfrującego (poinformuje Cię o tym brak kłódki obok paska adresu), ani nie podawaj na nich danych. Niezależnie od tego dokładnie weryfikuj, czy wprowadzony adres strony jest poprawny i nie ma w nim żadnej literówki.

10. Nigdy i nikomu **nie udostępniaj swojego hasła**, nawet jeśli poprosi Cię o to dział IT.

IV. PRYWATNE URZĄDZENIA

Zasady wykorzystania prywatnego sprzętu komputerowego.

W przypadku gdy musisz wykorzystywać sprzęt prywatny do użytku służbowego, zapewnij co najmniej, że:

1. Wykorzystywane przez Ciebie systemy, w szczególności systemy operacyjne, dysponują wsparciem producenta. **Warto wiedzieć**, że popularny Windows XP takiego wsparcia już nie zapewnia, podobnie jak Windows 7, którego asysta skończyła się w styczniu 2020 r.,

2. Wykorzystywane przez Ciebie **systemy podlegają** automatycznej, cyklicznej **aktualizacji**, a jej przebieg nie jest zakłócony żadnymi błędami. W szczególności zwróć uwagę na system operacyjny oraz oprogramowanie antywirusowe,

3. Twój system operacyjny dysponuje uruchomioną **zaporą ogniową**, a na komputerze skonfigurowano oprogramowanie antywirusowe,

4. Dostęp do Twojego komputera realizowany jest z wykorzystaniem **hasła dostępowego** znanego tylko i wyłącznie Tobie. Pamiętaj, że jego długość, złożoność i częstotliwość zmiany powinny zapewniać minimalizację ryzyka nieuprawnionego dostępu do danych, np. budowane hasła mogą składać się z co najmniej 8 znaków, w tym małych i dużych liter, cyfr lub znaków specjalnych, a ich zmiana powinna następować w cyklach 30-dniowych,

5. Konto systemowe, na którym wykonujesz obowiązki służbowe, jest kontem o **ograniczonych uprawnieniach**, a jedyną osobą posiadającą uprawnienia administracyjne na Twoim komputerze jesteś Ty,

6. Jeżeli nie masz dostępu do zasobów WSFiP – będziesz systematycznie wykonywać **kopię zapasową**, np. na zewnętrznych, zaszyfrowanych nośnikach danych,

7. Dysk Twojego komputera **jest zaszyfrowany**, a odszyfrowanie odbywa się za pomocą np. dodatkowego hasła lub hasła połączonego z tokenem,

8. Twój smartfon ma ustawioną **kontrolę dostępu** (np. PIN, znak graficzny, czytnik linii papilarnych), aktualne oprogramowanie oraz skonfigurowane szyfrowanie pamięci wbudowanej i zewnętrznej (jeśli występuje),

9. Twój komputer i telefon mają ustawiony **wygaszacz ekranu**, który blokuje urządzenie na wypadek kilkuminutowej nieaktywności użytkownika, np. po 5 minutach nieaktywności w przypadku komputera i po 1 minucie nieaktywności w przypadku telefonu,

10. Będziesz stosować wszystkie wymienione wyżej **dobre praktyki bezpiecznej pracy zdalnej**. Niezależnie od tego dowiedź się w WSFiP, jakie jeszcze wymagania powinieneś spełnić.