Załącznik Nr 16 do Zasad funkcjonowania Systemu Zarządzania Bezpieczeństwem Informacji Procedura PBI/13(3) Organizacja bezpiecznej pracy zdalnej

Opracowana dnia 14.04.2023 r. przez dr inż. Tomasz Stefaniuka Specjalistę ds. bezpieczeństwa informacji i systemów teleinformatycznych

Zatwierdzona dnia 15.05.2023 r. przez prof. dr hab. Mirosława Minkinę, Rektora UPH

Obowiązuje od: 15 maja 2023 r.

1. CEL PROCEDURY

Celem niniejszej procedury jest zapewnienie bezpieczeństwa informacji (a w szczególności danych osobowych) oraz systemów teleinformatycznych podczas świadczenia pracy zdalnej.

2. ODPOWIEDZIALNOŚĆ

Odpowiedzialność za realizację procedury ponoszą Kierownicy jednostek organizacyjnych oraz osoby zatrudnione na stanowiskach jednoosobowych podległych bezpośrednio Rektorowi.

3. ZAKRES STOSOWANIA

Procedura obejmuje pracowników Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach.

4. OPIS SPOSOBU POSTĘPOWANIA

Realizacja pracy poza siedzibą Uniwersytetu w formie zdalnej niesie ze sobą nowe wymagania w zakresie bezpieczeństwa informacji, będące konsekwencją przetwarzania zasobów informacyjnych w innych lokalizacjach, bądź na innych zasobach sprzętowych niż będących własnością UPH.

W takich warunkach szczególnie istotne jest przestrzeganie zapisów procedur systemu zarządzania bezpieczeństwem informacji, a w szczególności:

1. Wydzielenie odpowiedniej przestrzeni pracy tak, aby osoby postronne, nie miały dostępu do dokumentów i informacji, nad którymi aktualnie prowadzone są prace (zasada czystego biurka, czystego ekranu, poufności rozmów – *Procedura PBI/7-ochrona informacji w miejscu pracy*).
2. Szczególna troska o uczelniane środki przetwarzania informacji używane w domu:

a) uwzględnienie faktu, iż ryzyka, np. naruszeń danych, lub podsłuchu, są znacząco wyższe niż w siedzibie UPH (*Procedura PBI/6 - Bezpieczeństwo sprzętu i okablowania*),
b) ponieważ urządzenia i oprogramowanie przekazane przez pracodawcę do pracy zdalnej służą do wykonywania obowiązków służbowych, zabrania się wykorzystywania ich w celach prywatnych, bądź przez osoby trzecie,
c) w przypadku, gdy zdalna praca się wydłuża (trwa ponad miesiąc) pracownicy wykorzystujący sprzęt komputerowy UPH poza siedzibą Uniwersytetu zobowiązani są podłączyć ten sprzęt do sieci uczelnianej w celu aktualizacji oprogramowania (zwłaszcza bazy wirusów) oraz możliwości zaudytowania pod kątem legalności zainstalowanego oprogramowania.

3. W przypadku konieczności pracy zdalnej z wykorzystaniem komputera prywatnego wprowadza się zakaz zapisywania na nim, bądź na prywatnych nośnikach informacji jakichkolwiek plików z danymi wrażliwymi (dane osobowe, informacje niejawne, lub inne istotne z punktu Uczelni dane). Dodatkowo:
   a) Cała praca może być zapisana wyłącznie na udostępnionych zdalnie pulpitach komputerów znajdujących się zasobach zarządzanych przez UPH lub na zarejestrowanych zgodnie z procedurą *PBI/4 Postępowanie z nośnikami informacji* szyfrowanych nośnikach danych.
   b) Tak jak w przypadku komputerów służbowych, należy zweryfikować, czy komputer jest zabezpieczony poprzez używanie silnych haseł, co pozwoli na ograniczenie dostępu do urządzenia, a jednocześnie na ograniczenia ryzyka utraty danych w przypadku kradzieży lub zgubienia urządzenia.
   c) Przed rozpoczęciem korzystania z komputera prywatnego w celach służbowych należy upewnić się że system operacyjny jest zabezpieczony programem antywirusowym i firewallem oraz że programy te są włączone.

4. Realizacja pracy zdalnej z prywatnego komputera poprzez dostęp do krytycznych systemów informatycznych (min.: USOS. Simple.ERP, HMS. Prolib) jest dozwolona tylko w szczególnych przypadkach, po spełnieniu poniższych wymagań i tylko według opisanego poniżej schematu:
   a) Kierownik jednostki przekazuje w formie pisemnej listę osób oddelegowanych do pracy zdalnej w systemie administratorowi tego systemu.

b) Przedstawienie przez pracownika administratorowi systemu adresu IP przydzielonego przez dostawcę Internetu z którym pracownik ma zawartą umowę, z którego pracownik będzie nawiązywał połączenie do UPH.
c) Wystawieniu przez UPH certyfikatu OpenVPN umożliwiającego podłączenie do sieci wewnętrznej UPH. Ważność certyfikatu nie dłuższa niż 1 rok, z możliwością przedłużenia na kolejny rok.
d) Zainstalowanie i skonfigurowanie na komputerze prywatnym pracownika aplikacji klienckiej OpenVPN, do połączenia z siecią wewnętrzną UPH.
e) Po uzyskaniu połączenia OpenVPN z komputera prywatnego, inicjowanie połączenia przy użyciu „Zdalnego pulpitu" na komputer znajdujący się w zasobach UPH. Może to być komputer fizyczny pracownika lub maszyna wirtualna utworzona na potrzeby uzyskania dostępu zdalnego.
f) W celu minimalizacji ryzyka wycieku danych osobowych, dostęp do systemów UPH może być realizowany wyłącznie za pomocą zdalnego pulpitu dostępnego poprzez połączenie VPN".
g) Cała praca może być wykonana i zapisana wyłącznie na udostępnionych zdalnie pulpitach komputerów znajdujących się zasobach zarządzanych przez UPH.
h) Po zakończonej pracy należy wylogować się z systemów dziedzinowych, zdalnego komputera i rozłączyć sesję OpenVPN.

5. Wszelka korespondencja prowadzona jest tylko za pomocą poczty służbowej. Przesyłanie danych zawierających dane osobowe możliwe jest tylko w formie niejawnej (zaszyfrowanej) – *Procedura PBI/7- ochrona informacji w miejscu pracy.*
6. Jeżeli w realizowanej pracy niezbędne jest korzystanie z pamięci w chmurze, dozwolone jest jedynie wykorzystywanie dysku Google na koncie UPH, z zachowaniem wszelkich zasad i procedur dotyczących logowania i udostępniania danych (np. szyfrowania danych osobowych przed umieszczeniem w chmurze).
7. Należy podjąć szczególne środki, aby urządzenia wykorzystywane podczas pracy zdalnej, szczególnie te wykorzystywane do przenoszenia danych, jak dyski zewnętrzne nie zostały zgubione, czy też skradzione. Jeśli dojdzie do takiego przypadku, fakt ten, zgodnie z procedurą *PBI/3 Postępowanie przy stwierdzeniu incydentów naruszających bezpieczeństwo informacji* należy niezwłocznie zgłosić odpowiednim jednostkom w niej opisanym.

8. W przypadku konieczności korzystania z dokumentacji papierowej zawierającej dane osobowe bądź inne wrażliwe dane poza siedzibą Uczelni konieczne jest zastosowanie się do poniższych wymogów:
    a) Wynoszenie dokumentacji papierowej z siedziby Uczelni powinno być ograniczone do niezbędnego minimum. Przełożony może zezwolić pracownikom na korzystanie z dokumentacji papierowej zawierającej dane osobowe w trakcie pracy zdalnej tylko w wyjątkowych sytuacjach.
    b) Wydawane dokumenty zawierające dane osobowe na potrzeby pracy zdalnej podlegają ewidencji przez przełożonego.
    c) Wynoszenie dokumentów lub ich kopii powinno mieć miejsce w zabezpieczonej aktówce i w taki sposób, aby były niewidocznie dla osób trzecich.
    d) Po wykorzystaniu oryginałów dokumentów powinny one zostać niezwłocznie zwrócone. Zwrot dokumentów podlega odnotowaniu w prowadzonej ewidencji.
    e) Po wykorzystaniu kopii dokumentacji powinny one zostać w całości zniszczone przez Pracownika. W przypadku nieposiadania niszczarki w miejscu pracy Pracownika powinien on wykonane kopie zniszczyć niezwłocznie w siedzibie zakładu pracy.
    f) Należy rozważyć wykonanie kopii dokumentacji, na której Pracownik będzie pracował. Kopie dokumentów z danymi osobowymi podlegają takiej samej ochronie jak oryginały.
    g) Drukowanie dokumentów na potrzeby pracy należy ograniczyć do niezbędnego minimum. W przypadku dokumentów zawierających dane osobowe należy w miarę możliwości dokonać anonimizacji danych.
9. W przypadku prowadzenia lub korzystania z wideokonferencji, należy stosować się do poniższych zasad:[7]
    a) Przed rozpoczęciem wideokonferencji należy zapoznać się z ogólnymi warunkami użytkowania lub polityką prywatności wykorzystywanego programu oraz sprawdzić, czy rozmowy będą nagrywane i przechowywane. Konieczna jest również weryfikacja, do jakich celów będą wykorzystywane podane dane osobowe. Sprawdzić należy także, o jakie uprawnienia do

[7] Opracowano na podstawie: *https://uodo.gov.pl/pl/138/1525*

danych zostaniemy poproszeni - lista kontaktów, lokalizacja itp. Wprowadzając hasło do aplikacji konferencyjnej należy użyć innego hasła, niż używane w innych usługach. Należy się upewnić, że osoby postronne nie mają dostępu do naszego ekranu. Przed udostępnieniem ekranu podczas rozmowy należy zamknąć wszystkie okna, które nie są niezbędne w trakcie wideokonferencji tak, aby inni uczestnicy konferencji ich nie zobaczyli.

b) W trakcie korzystania z wideokonferencji należy ograniczyć ilość podawanych danych osobowych. Nie należy udostępniać linków do konferencji w mediach społecznościowych, ani dokumentów służbowych za pomocą czatu, który może być publiczny. Jeżeli to możliwe, należy korzystać z opcji zamazywania tła (tak żeby rozmówcy nie widzieli Twojego otoczenia). Podczas administrowania konferencją zalecane jest korzystanie z opcji "poczekalnia", tak aby można było kontrolować osoby uczestniczące w telekonferencji; unikając przypadkowych lub niechcianych osób. W trakcie logowania się do telekonferencji, należy wyłączyć mikrofon i kamerę (włączając je, jak będzie to potrzebne).
c) Po skorzystaniu z wideokonferencji należy wyłączyć mikrofon i kamerę, upewnić się, że spotkanie on-line zostało zakończone, a aplikacją zamknięta i że program do telekonferencji nie działa w tle.