Zasady bezpieczeństwa obowiązujące pracowników Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach podczas wykonywania pracy zdalnej.

Realizacja pracy zdalnej wymaga szczególnej troski o kwestie bezpieczeństwa informacji. Pomimo pracy poza siedzibą Uniwersytetu wymagane jest przestrzeganie obowiązujących w tym zakresie procedur funkcjonujących w ramach Systemu Zarządzania Bezpieczeństwem Informacji.
Zwraca się szczególną uwagę na:

I. Procedurę PBI/13(1) Organizację bezpiecznej pracy zdalnej

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:

1) 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.
2) 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.
3) 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.

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:

1) Kierownik jednostki przekazuje w formie pisemnej listę osób oddelegowanych do pracy zdalnej w systemie administratorowi tego systemu.
2) Przedstawienie przez pracownika administratorowi systemu stałego adresu IP przydzielonego przez dostawcę Internetu z którym pracownik ma zawartą umowę, z którego pracownik będzie nawiązywał połączenie do UPH.
3) Wystawieniu przez UPH certyfikatu OpenVPN umożliwiającego podłączenie do sieci wewnętrznej UPH. Ważność certyfikatu nie dłuższa niż 1 rok, z możliwością przedłużenia na kolejny rok.
4) Zainstalowanie i skonfigurowanie na komputerze prywatnym pracownika aplikacji klienckiej OpenVPN, do połączenia z siecią wewnętrzną UPH.
5) 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.
6) W celu minimalizacji ryzyka wycieku danych osobowych, dostęp do systemów UPH może być realizowany wyłącznie za pomocą zdalnego pulpitu dostępnego poprzez połączenie VPN”.
7) Cała praca może być wykonana i zapisana wyłącznie na udostępnionych zdalnie pulpitach komputerów znajdujących się zasobach zarządzanych przez UPH.

8) Po zakończonej pracy należy wylogować się z systemów dziedzinowych, zdalnego komputera i rozłączyć sesję OpenVPN.

II. Procedurę PBI/7(2) - ochrona informacji w miejscu pracy

Zasada czystego biurka

1) Dokumenty papierowe i nośniki komputerowe, kiedy nie są aktualnie używane przechowuje się w niedostępnych miejscach.

Zasady czystego ekranu

2) O ile to możliwe, monitor powinien być ustawiony w taki sposób, by osoby postronne nie miały możliwości wglądu do przetwarzanych aktualnie informacji.
3) Wygaszacze ekranu w stacjach roboczych powinny zostać aktywowane po okresie nieaktywności użytkownika trwającym max.15 minut.
4) W przypadku opuszczania stanowiska pracy, należy zablokować stację roboczą. uniemożliwiając nieautoryzowany dostęp osób trzecich.
5) Z aplikacji zawierających dane osobowe i programów do obsługi poczty elektronicznej należy wylogować się bezpośrednio po zakończeniu w nich pracy.

Zasada poufności rozmów

1) W przypadku rozmów (również telefonicznych) dotyczących realizacji zadań prowadzonych poza obszarem uczelni należy zadbać, aby rozmowy nie były prowadzone w obecności osób nieupoważnionych do otrzymania tych informacji.

Aby zapewnić spełnienie powyższych zasad w warunkach pracy w domu – przed jej rozpoczęciem należy wydzielić sobie odpowiednią przestrzeń, tak aby osoby postronne, nie miały dostępu do dokumentów, nad którymi aktualnie pracujemy.

Zasady bezpiecznego korzystania z Internetu

1. Przed rozpoczęciem korzystania z Internetu należy upewnić się że system operacyjny jest zabezpieczony programem antywirusowym i firewallem oraz że programy te są włączone.
2. Wprowadza się całkowite ograniczenia w dostępie do treści uznanych za pornograficzne, rasistowskie, traktujące o przemocy, przestępstwach, jak również do protokołów umożliwiających wymianę plików w sieciach z naruszeniem przepisów prawa.

Zasady bezpiecznego korzystania z poczty elektronicznej

1. Korzystanie z systemu poczty elektronicznej dla celów prywatnych jest zabronione.
2. Ponadto, zabronione jest:
    a. Odpowiadania na wiadomości żądające podania danych niezbędnych do logowania się.
    b. wysyłanie materiałów służbowych na konta prywatne (np. celem pracy nad dokumentami w domu);
    c. wykorzystywanie systemu poczty elektronicznej do działań mogących zaszkodzić wizerunkowi UPH,
    d. odbieranie przesyłek z nieznanych źródeł;
    e. otwieranie załączników z plikami samorozpakowującymi się bądź wykonalnymi typu exe, com, itp.;
    f. przesyłanie pocztą elektroniczną plików wykonywalnych typu: bat, com, exe, plików multimedialnych oraz plików graficznych;
    g. ukrywanie lub dokonywanie zmian tożsamości nadawcy;
    h. czytanie, usuwanie, kopiowanie lub zmiana zawartości skrzynek pocztowych innego użytkownika;

i. odpowiadanie na niezamówione wiadomości reklamowe lub wysyłane łańcuszki oraz na inne formy wymiany danych określanych spamem; w przypadku otrzymania takiej wiadomości należy przesłać ją administratorowi systemu informatycznego;
j. posługiwanie się adresem służbowym e-mail w celu rejestrowania się na stronach handlowych, informacyjnych, chat'ach lub forach dyskusyjnych, które nie dotyczą zakresu wykonywanej pracy lub obowiązków umownych;
k. wykorzystywanie poczty elektronicznej do reklamy prywatnych towarów lub usług, działalności handlowo-usługowej innej niż wynikającej z potrzeb administratora danych lub do poszukiwania dodatkowego zatrudnienia.

1. Informacje wrażliwe, a szczególnie dane osobowe przed wysłaniem za pomocą e-mail należy zaszyfrować.
2. Załączniki do wiadomości e-mail należy przeskanować przed ich otwarciem.
3. Kończąc pracę w programie pocztowym należy zawsze samodzielnie wylogować się z serwisu, klikając w przycisk „wyloguj".
4. Należy zachować szczególną ostrożność przypadku otrzymania wiadomości:
   a. gdy nie znamy nadawcy wiadomości;
   b. tytuł wiadomości i nazwa załącznika nie mają sensu;
   c. gdy tytuł lub treść widomości napisana jest niepoprawnie pod względem gramatycznym lub stylistycznym;

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).

III. Procedurę PBI/4(2) Postępowanie z nośnikami informacji

1. Nośniki danych zawierające dane osobowe, informacje niejawne, lub inne dane wrażliwe muszą być szczególnie zabezpieczone przed nieautoryzowanym dostępem, ich nieautoryzowaną modyfikacją lub utratą. W związku z powyższym są one poddane obowiązkowi wykonania kopii tych danych.
2. Nie jest dozwolone wynoszenie takich nośników danych poza miejsce wykonywania pracy bez ich zabezpieczenia (dostęp do nośnika po uwierzytelnieniu oraz zaszyfrowanie danych na nośniku).
3. **Zabronione jest korzystanie z prywatnych nośników informacji (np. dysk zewnętrzny, pen drive).**
4. **Bez potrzeby nie należy tworzyć plików komputerowych zawierających dane osobowe.**

IV. Procedurę PBI/5(3) Zarządzanie dostępem użytkowników do usług sieciowych.

Należy zweryfikować, czy komputer jest zabezpieczony poprzez używanie silnych haseł dostępu, co pozwoli na ograniczenie dostępu do urządzenia, a jednocześnie na ograniczenia ryzyka utraty danych w przypadku kradzieży lub zgubienia urządzenia.

V. Procedurę PBI/6(2) Bezpieczeństwo sprzętu i okablowania

Bezpieczeństwo sprzętu poza siedzibą

1) Przekazywanie sprzętu komputerowego pracownikowi jest regulowane Zarządzeniem Rektora UPH **Nr 2/2015 z dnia 2 lutego 2015 r.** w sprawie ustalenia instrukcji przeprowadzania inwentaryzacji aktywów i pasywów w Uniwersytecie Przyrodniczo-Humanistycznym w Siedlcach oraz Zarządzeniem Kanclerza UPH Nr 40/2014 z dnia 23

maja 2014 r. w sprawie określenia podstawowych zasad dotyczących zarządzania majątkiem UPH

2) Korzystanie ze środków przetwarzania informacji poza siedzibą organizacji jest autoryzowane przez kierownictwo, niezależnie od tego, kto jest ich właścicielem.

3) W odniesieniu do ochrony sprzętu znajdującego się poza siedzibą, wprowadza się następujące wytyczne:
   a) nie pozostawiać w miejscach publicznych bez nadzoru urządzeń lub nośników wynoszonych poza siedzibę; przewozić komputery przenośne jako bagaż podręczny i, w miarę możliwości, maskować je w czasie podróży;
   b) przestrzegać instrukcji producenta dotyczących ochrony sprzętu, np. ochrony przed wystawieniem na silne pola elektromagnetyczne;
   c) stosować odpowiednie zabezpieczenia określone w procesie szacowania ryzyka, niezbędne podczas pracy w domu, np. zamykane szafki, polityka czystego biurka, zabezpieczenia dostępu do komputerów oraz bezpieczne połączenie z biurem
   d) zapewnić odpowiednie ubezpieczenie sprzętu używanego poza siedzibą.
4) Zaleca się, aby przy wyborze właściwych zabezpieczeń uwzględnić fakt, że ryzyka, np. uszkodzeń, kradzieży lub podsłuchu, mogą znacząco różnić się w zależności od miejsca.

Należy pamiętać, że urządzenia i oprogramowanie przekazane przez pracodawcę do pracy zdalnej służą do wykonywania obowiązków służbowych. Zabrania się więc wykorzystywania ich w celach prywatnych, bądź przez osoby trzecie.

VI. Procedurę PBI/8(1) Konfiguracja stacji roboczej

1. Należy dążyć do minimalizowania zmian w oprogramowaniu i instalowania nowych aplikacji do zmian niezbędnych.
2. Niewskazane jest samodzielne instalowanie jakichkolwiek aplikacji przez pracowników.
3. Zabronione jest instalowanie aplikacji pochodzących z niepewnych źródeł.
4. Oprogramowanie każdej stacji roboczej jest na bieżąco aktualizowane o poprawki bezpieczeństwa oraz o nową bazę wirusów.
5. Na komputerach podłączonych do sieci Internet włączone są funkcje codziennego automatycznego pobierania i instalacji poprawek.

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.

VII. Procedurę PBI/3 (4) Postępowanie przy stwierdzeniu incydentów naruszających bezpieczeństwo informacji

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 (4) należy zgłosić odpowiednim jednostkom w niej opisanym.