Zadania i obowiązki Zespołu Projektowego:

1. Kierownik projektu:

a) przygotowanie projektu zgodnie z wytycznymi Narodowego Centrum Nauki, z uwzględnieniem zaleceń Zespołu ds. Wsparcia Zarządzania Danymi Badawczymi.

b) zaplanowanie prac projektowych w taki sposób, aby zapewnić bezpieczeństwo danych (tj. poufność, integralność i dostępność) oraz zgodność z obowiązującymi regulacjami zewnętrznymi i wewnętrznymi, w szczególności z Polityką Bezpieczeństwa Danych Osobowych UEW wprowadzonej Zarządzeniem nr 39a/2018 Rektora Uniwersytetu Ekonomicznego we Wrocławiu z dnia 25 maja 2018 r. oraz z Polityką Bezpieczeństwa Informacji w Uniwersytecie Ekonomicznym we Wrocławiu wprowadzoną Zarządzeniem nr 54/2021 Rektora Uniwersytetu Ekonomicznego we Wrocławiu z dnia 7 maja 2021 r. ;

c) nadzór nad przestrzeganiem zasad ochrony danych w trakcie trwania projektu;

d) nadzór nad wypełnieniem założeń PZD;

e) po zakończeniu projektu kontakt z Centrum Informatyki w celu usunięcia konta Teams/Sharepoint/OneDrive oraz przekazanie danych badawczych do dalszej archiwizacji;

f) po zakończeniu projektu kontakt na adres dane.badawcze@ue.wroc.pl w celu przekazania informacji o udostępnieniu danych badawczych w innych repozytoriach lub wskazanych w projekcie innych miejscach;

g) zgłaszanie incydentów związanych z bezpieczeństwem danych Menedżerowi Bezpieczeństwa Teleinformatycznego oraz związanych z naruszeniem ochrony danych osobowych Inspektorowi Ochrony Danych.

2. Członkowie Zespołu projektowego:

a) prowadzenie prac badawczych w sposób zapewniający zgodność z obowiązującymi regulacjami zewnętrznymi i wewnętrznymi, w szczególności z Polityką Bezpieczeństwa Danych Osobowych UEW oraz Polityką Bezpieczeństwa Informacji;

b) realizacja założeń PZD;

c) zgłaszanie incydentów związanych z bezpieczeństwem danych Menedżerowi Bezpieczeństwa Teleinformatycznego oraz związanych z naruszeniem ochrony danych osobowych Inspektorowi Ochrony Danych.

Zadania członków Zespołu ds. Wsparcia Zarządzania Danymi Badawczymi działającego na UEW

1.Członkowie Zespołu z Biblioteki:

a) konsultacje Planów Zarządzania Danymi z kierownikiem Projektu oraz pozostałym członkami Zespołu;

b) prowadzenie szkoleń dla pracowników oraz doktorantów UEW dotyczących: danych badawczych i tworzenia Planu Zarządzania Danymi, Open Access, licencji Creative Commons, repozytoriów danych badawczych;

c) prowadzenie strony internetowej dotyczącej danych badawczych;

d) wprowadzenie informacji o miejscu udostępnienia danych badawczych do Bazy Wiedzy WIR;

e) archiwizacja ostatecznych wersji Planów Zarządzania Danymi,

2. Członkowie Zespołu z Centrum Obsługi Badań Naukowych:

a) konsultacje w sprawie przygotowywania PZD;

b) wsparcie pracowników oraz doktorantów UEW w szkoleniach dotyczących: danych badawczych i pisania Planu Zarządzania Danymi, Open Access, Creative Commons, repozytoriów danych badawczych.

3. Menedżer Bezpieczeństwa Teleinformatycznego:

a) konsultacje w sprawie przygotowywania PZD;

b) prowadzenie szkoleń dla pracowników i doktorantów UEW z zakresu bezpieczeństwa danych;

c) wsparcie w trakcie trwania projektu w zakresie bezpieczeństwa danych;

d) obsługa incydentów bezpieczeństwa danych przetwarzanych w projekcie;

e) w przypadku podejrzenia przetwarzania danych w sposób niezgodny z regulacjami zewnętrznymi lub wewnętrznymi przeprowadzenie audytu i przygotowanie raportu, który wraz z wnioskami pokontrolnymi przedstawiany jest Przewodniczącemu Zespołu ds. Wsparcia Zarządzania Danymi Badawczymi.

4. Inspektor Ochrony Danych:

a) konsultacje w sprawie przygotowywania PZD;

b) prowadzenie szkoleń dla pracowników i doktorantów UEW z zakresu ochrony danych osobowych;

c) wsparcie w trakcie trwania projektu w zakresie bezpieczeństwa danych osobowych;

d) obsługa incydentów bezpieczeństwa danych osobowych przetwarzanych w projekcie;

e) w przypadku podejrzenia przetwarzania danych w sposób niezgodny z regulacjami zewnętrznymi lub wewnętrznymi przeprowadzenie audytu i przygotowanie raportu, który wraz z wnioskami pokontrolnymi przedstawiany jest Przewodniczącemu Zespołu ds. Wsparcia Zarządzania Danymi Badawczymi.

5. Radcy prawni

a) weryfikacja umów z agencjami realizującymi badania/pozyskującymi dane;

b) opracowanie procedur na Uczelni dotyczących danych badawczych oraz publikacji;

c) konsultacje w sprawie przygotowywania PZD.

Informacje z PZD nie będą przekazywane osobom niebędącym członkami Zespołu ds. Wsparcia Zarządzania Danymi Badawczymi.

Instrukcje techniczne:

Procedura tworzenia konta lub przestrzeni dyskowej dla projektu:

Tworzeniem zespołów w MS Office 365 dla projektu zajmuje się Centrum Informatyki. Kierownik projektu zgłasza potrzebę utworzenia zespołu na stronie https://helpit.ue.wroc.pl/.

W przypadku prac nad projektem międzyuczelnianym Kierownik projektu może przekazać dostęp do wybranych folderów umieszczonych w chmurze za pomocą wygenerowanego linku. O udostępnieniu danych oraz o sposobie udostępnienia jak również o uprawnieniach (tylko do odczytu, pełen dostęp z możliwością edycji) decyduje Kierownik projektu.

W każdym przypadku, gdy wymagane jest udostępnienie danych osobom spoza Uczelni należy skonsultować się z Menedżerem Bezpieczeństwa Teleinformatycznego oraz gdy w projekcie przetwarzane są dane osobowe, z Inspektorem Ochrony Danych. W przypadku, gdy Kierownik lub wykonawca projektu stwierdzi lub ma podstawy, aby podejrzewać, iż doszło do naruszenia bezpieczeństwa danych (w tym danych wrażliwych), zobowiązany jest poinformować o tym fakcie wyżej wymienione osoby.

Dodatkową możliwą opcją jest na wniosek Kierownika projektu Centrum Informatyki udostępnienie na czas trwania projektu przestrzeni dyskowej jako zasób sieciowy służący do przechowywania kopii danych. Maksymalna przestrzeń dyskowa dla zespołu to 50 GB. Dostęp jest możliwy po poprawnym zalogowaniu. Centrum Informatyki codziennie wykonuje kopie danych znajdujących się w udostępnionej przestrzeni i przechowuje przez dwa tygodnie. Wszystkie odstępstwa od tej zasady wymagają każdorazowo uzgodnienia z Centrum Informatyki. Dostęp do zasobu sieciowego możliwy jest z sieci wewnętrznej Uczelni oraz przez VPN.

Kierownik projektu zgłasza na stronie https://helpit.ue.wroc.pl/ potrzebę utworzenia zasobu sieciowego przeznaczonego dla Zespołu.

Dane składowane na zasobach Centrum Informatyki będą przechowywane przez okres niezbędny w projekcie. W przypadku dłuższego przechowywania danych (np. 10 lat), Kierownik projektu musi skontaktować się po zakończeniu projektu z CI w celu przekazania dostępu do konta projektu oraz zobowiązania do robienia kopii zapasowych.

W przypadku, gdy dane badawcze będą udostępnione w całości w wybranym repozytorium, wówczas Kierownik projektu zgłasza do CI prośbę o usunięcie konta.

W przypadku gdy Kierownik projektu przestaje być pracownikiem UEW, a jest w trakcie prowadzenia projektu, musi skontaktować się z Centrum Informatyki oraz Centrum Obsługi Badań Naukowych w celu uzgodnienia dalszych działań.

Działania mające na celu zapewnienie bezpieczeństwa danych:

a) **Szyfrowanie nośników** w ramach zachowania bezpieczeństwa Kierownik projektu powinien dopilnować, aby każdy dysk oraz komputer członków zespołu był zaszyfrowany programem VeraCrypt (oprogramowanie darmowe) lub BitLocker (oprogramowanie zawarte w Windows Pro). W razie konieczności członek zespołu badawczego może zwrócić się do Centrum Informatyki z prośbą o pomoc w zaszyfrowaniu komputera/dysku. W przypadku komputerów będących własnością Uczelni operacja szyfrowania musi zostać wykonana przez Centrum Informatyki.

Instrukcja szyfrowania dysków programem BitLocker:

https://support.microsoft.com/pl-pl/help/4028713/windows-10-turn-on-device-encryption

Instrukcje dla programy VeraCrypt: w języku angielskim:

https://www.veracrypt.fr/en/Beginner%27s%20Tutorial.html.

W Internecie dostępne są instrukcje w języku polskim, np.:

https://www.komputerswiat.pl/poradniki/programy/veracrypt-szyfrowanie-dyskow-nie-dozlamania/xnvkg2y

b) **Przenoszenie danych** Do pracy z danymi należy korzystać z rozwiązań chmurowych. Z powodu ryzyka utraty danych w razie zgubienia lub kradzieży nie jest rekomendowane przechowywanie i przenoszenie danych na nośnikach zewnętrznych. Wyjątek stanowi użycie zaszyfrowanych dysków zewnętrznych do przechowywania kopii zapasowych.

c) **Kopie zapasowe** Kierownik projektu (lub wskazany przez niego członek zespołu) zobowiązany jest do tworzenia kopii zapasowych.

Zasada dotycząca kopii zapasowych: 3-2-1:

- 3 kopie (chmura, dysk lokalny, dysk zewnętrzny lub udostępniony zasób sieciowy),
- 2 różne nośniki (a nawet 3 różne) i
- 1 nośnik jest poza Uczelnią (w chmurze).

Kopie zapasowe danych powinny być wykonywane regularnie (pełna kopia przynajmniej 1 raz w tygodniu) na zasób sieciowy udostępniony przez Centrum Informatyki. Jeżeli uwarunkowania techniczne nie pozwalają na użycie przestrzeni dyskowej Centrum Informatyki, to kopie zaleźy wykonywać na zewnętrzny, zaszyfrowany nośnik (dysk twardy).

Dysk do kopii zapasowych powinien być podłączany tylko na czas wykonywania kopii i wykorzystywany wyłącznie do tworzenia kopii bezpieczeństwa.

Dysk należy przechowywać w miejscu bezpiecznym na UEW (miejsce zamknięte).

d) **Ochrona przed wirusami** Na każdym komputerze przetwarzającym dane badawcze musi być zainstalowane oprogramowanie antywirusowe. Wymagana jest bieżąca aktualizacja oprogramowania oraz sygnatur antywirusowych.

e) **Aktualizacje systemu operacyjnego** Na każdym komputerze przetwarzającym dane badawcze wymagana jest bieżąca aktualizacja systemu operacyjnego.

f) **Zapora internetowa** Każdy system operacyjny obsługujący komputer przetwarzający dane badawcze musi mieć włączoną zaporę internetową (firewall) chroniącą przed atakami sieciowymi.

g) **Przyłączenie do domeny Active Directory** Każdy komputer z systemem Windows, na którym są przetwarzane dane badawcze powinien być przyłączony do domeny Active Directory „pracownik.ue.wroc.pl”. W ten sposób automatycznie zostaną zapewnione aktualność systemu operacyjnego i oprogramowania antywirusowego oraz włączenie wszystkich funkcji systemu zwiększających bezpieczeństwo danych. W przypadku, gdy komputer jest poza domeną, odpowiedzialność za wypełnienie wymagań spoczywa na użytkowniku komputera.