ZARZĄDZENIE NR GKG.GPK.0200.86.2023

DYREKTORA POWIATOWEGO OŚRODKA DOKUMENTACJI

GEODEZYJNEJ I KARTOGRAFICZNEJ

z dnia 10 lipca 2023 roku

w sprawie: wprowadzenia Procedury ochrony danych osobowych podczas pracy zdalnej w Powiatowym Ośrodku Dokumentacji Geodezyjnej i Kartograficznej

Na podstawie art. 67^{26} ustawy z dnia 26 czerwca 1974 roku Kodeks pracy oraz § 10 ust. 1 pkt 3 Uchwały nr 3606/2022 Zarządu Powiatu w sprawie Regulaminu Organizacyjnego Powiatowego Ośrodka Dokumentacji Geodezyjnej i Kartograficznej, zarządzam co następuje:

§1. Wprowadza się Procedurę ochrony danych osobowych podczas pracy zdalnej w Powiatowym Ośrodku Dokumentacji Geodezyjnej i Kartograficznej, stanowiącą załącznik do niniejszego Zarządzenia.

§2. Załącznik do niniejszego Zarządzenia stanowi tajemnicę, o której mowa w art. 100 § 2 pkt 4 ustawy z dnia 26 czerwca 1974 r. Kodeks Pracy i nie podlega publikacji na stronach Biuletynu Informacji Publicznej.

§3. Nadzór nad Zarządzeniem powierza się Inspektorowi Ochrony Danych.

§4. Zarządzenie wchodzi w życie z dniem podpisania.

Załącznik do Zarządzenia nr GKG.GPK.0200.86.2023
Dyrektora Powiatowego Ośrodka Dokumentacji
Geodezyjnej i Kartograficznej
z dnia 10 lipca 2023 r.

Procedura ochrony danych osobowych podczas pracy zdalnej w Powiatowym Ośrodku Dokumentacji Geodezyjnej i Kartograficznej

§1. Słownik

1. Ilekroć w instrukcji jest mowa o:
    a) PODGiK - Powiatowy Ośrodek Dokumentacji Geodezyjnej i Kartograficznej;
    b) Dyrektor PODGiK - Dyrektor Powiatowego Ośrodka Dokumentacji Geodezyjnej i Kartograficznej;
    c) Procedura - rozumie się przez to niniejszą Procedurę ochrony danych osobowych podczas pracy zdalnej w Powiatowym Ośrodku Dokumentacji Geodezyjnej i Kartograficznej;
    d) Pracownikach - osoby zatrudnione na podstawie umowy o pracę w PODGiK;
    e) RODO - Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych);
    f) danych osobowych — należy przez to rozumieć informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
    g) Pracy zdalnej — należy rozumieć pracę określoną w art. 67^{18} Kodeksu Pracy.

§2. Sposób wykonywania pracy zdalnej

1. Praca zdalna może być realizowana:
    a) z wykorzystaniem powierzonego przez PODGiK sprzętu komputerowego;

b) z wykorzystaniem prywatnego sprzętu komputerowego pracownika.

2. Wykonywanie pracy zdalnej jest możliwe, jeżeli pracownik ma umiejętności i możliwości techniczne oraz lokalowe do wykonywania takiej pracy, w tym zapewnia bezpieczeństwo przetwarzanych danych osobowych.
3. Pracownik wykonujący pracę zdalną zobowiązany jest do przestrzegania zapisów niniejszej Procedury, wewnętrznych regulacji oraz przepisów, których przestrzeganie było wymagane przed podjęciem pracy zdalnej, w tym RODO, zachowania tajemnicy służbowej i wykonywania pracy z zachowaniem należytej staranności, rzetelności oraz postaw etycznych.
4. Pracownik zobowiązany jest do przetwarzania udostępnionych mu danych osobowych jedynie w celach służbowych, określonych w upoważnieniu do przetwarzania danych osobowych.
5. Pracownik wykonuje pracę zdalną w miejscu uzgodnionym i wskazanym w porozumieniu zawartym z PODGiK.
6. Pracownik powinien korzystać ze wsparcia ze strony Wydziału Informatyki w zakresie pomocy technicznej oraz niezbędnych szkoleń dotyczących obsługi sprzętu komputerowego. Pracownik niezwłocznie zgłasza bezpośredniemu przełożonemu wszelkie uzasadnione potrzeby w tym zakresie.
7. Pracownik korzystający ze sprzętu prywatnego zobowiązany jest do używania urządzeń z aktualnym systemem operacyjnym (wspieranym aktualnie przez producenta) oraz aktualnym programem antywirusowym. Wydział Informatyki może wskazać rekomendowanych producentów. Za legalność stosowanego na prywatnym urządzeniu oprogramowania odpowiada właściciel sprzętu.
8. Pracownik zobowiązany jest do zabezpieczenia za pomocą hasła dostępu do systemu operacyjnego na prywatnym sprzęcie wykorzystywanym do pracy zdalnej.
9. Wydział Informatyki informuje Dyrektora PODGiK oraz Inspektora Ochrony Danych lub jego Zastępcę o wystąpieniu wszelkiego rodzaju incydentów, które mogą dotyczyć bezpieczeństwa danych.
10. Bezpośredni przełożony pracownika informuje Wydział Informatyki o konieczności zablokowania dostępu (usunięciu lub blokadzie konta użytkownika). Wydział Informatyki może również podjąć natychmiastową decyzję blokady konta po stwierdzeniu nieuprawnionego dostępu lub kradzieży sprzętu komputerowego.
11. Dane, w szczególności dane osobowe i informacje prawnie chronione, przetwarzane podczas pracy zdalnej podlegają ochronie przed przypadkowym lub niezgodnym z prawem zniszczeniem, utraceniem, zmodyfikowaniem, nieuprawnionym ujawnieniem lub

nieuprawnionym dostępem do danych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

12. Pracownik korzystający ze sprzętu prywatnego, na którym przetwarza dane osobowe, zobowiązany jest do zabezpieczenia go tak, by do tych danych nie miały dostępu osoby nieuprawnione, w tym wspólnie z nim zamieszkujące.
13. Przekazanie pracownikowi służbowego sprzętu do pracy zdalnej następuje zgodnie z wewnętrznymi przepisami obowiązującymi w PODGiK.
14. Wszelkie problemy oraz nieprawidłowości w działaniu udostępnionego sprzętu, narzędzi lub oprogramowania należy niezwłocznie zgłaszać do Wydziału Informatyki.
15. Udostępniony pracownikowi sprzęt służbowy stanowi własność PODGiK. Zabronione jest udostępnianie urządzeń wykorzystywanych do realizowania pracy zdalnej osobom trzecim. Podejmując pracę zdalną pracownik zobowiązuje się odpowiednio zabezpieczyć sprzęt przed kradzieżą, chronić przed uszkodzeniem oraz zniszczeniem.
16. W przypadku kradzieży, zgubienia komputera przenośnego lub naruszenia ochrony zawartych w nim danych osobowych Pracownik zobowiązany jest do niezwłocznego zgłoszenia zdarzenia bezpośredniemu przełożonemu, Wydziałowi Informatyki i Inspektorowi Ochrony Danych.
17. W trakcie wykonywania pracy zdalnej pracownik zobowiązany jest wykorzystywać wyłącznie programy służbowe i systemy informatyczne udostępnione mu przez PODGiK.
18. Jeśli komputer stacjonarny lub przenośny pozostawiony jest w miejscu dostępnym dla osób nieuprawnionych (w domu lub innym miejscu wykonywania pracy zdalnej), konieczne jest zabezpieczenie dostępu hasłem oraz poprzez aktywację wygaszacza ekranu.
19. Zabronione jest zapisywanie hasła w sposób umożliwiający dostęp do niego innym osobom.
20. Monitory stanowisk komputerowych oraz ekrany laptopów, na których przetwarzane są dane osobowe, znajdujące się w pomieszczeniach, w których mogą przebywać osoby nieuprawnione, należy ustawić w taki sposób, aby uniemożliwić tym osobom wgląd w dane.
21. Niedozwolone jest przesyłanie danych osobowych lub dokumentów je zawierających z wykorzystaniem kont pocztowych spoza domeny PODGiK.
22. Dane osobowe przesyłane drogą mailową muszą być zaszyfrowane, na przykład poprzez nałożenie hasła na dokument MS Word i MS Excel lub spakowanie („zzipowanie”) z nałożonym hasłem pliku/plików zawierających dane. Hasło należy przekazywać inną drogą, niż poprzez email, na przykład telefonicznie lub poprzez SMS.
23. Robocze, błędne lub nieaktualne wydruki należy usuwać (niszczyć) natychmiast po ustaniu ich przydatności w sposób uniemożliwiający ich odczyt.

24. Każdy pracownik, który stwierdzi lub podejrzewa naruszenie ochrony danych osobowych przetwarzanych zobowiązany jest do niezwłocznego poinformowania o tym bezpośredniego przełożonego, Wydziału Informatyki oraz Inspektora Ochrony Danych.
25. Zdalny dostęp do systemów teleinformatycznych PODGiK odbywa się przy wykorzystaniu bezpiecznego kanału dostępowego (VPN) oraz poprzez zdalny pulpit komputera pracownika w siedzibie PODGiK.
26. Dostęp, o którym mowa powyżej, jest przyznawany, konfigurowany i wydawany wraz z instruktażem przez Wydział Informatyki. Pracownik nie ma możliwości zmiany parametrów konfiguracyjnych.
27. Wydział Informatyki przygotowuje dane dostępowe oraz niezbędne parametry uwierzytelniające do usługi VPN. W zależności od obszaru dostępu do konkretnych usług, konto jest przypisywane do określonej grupy uprawnień.
28. Pracownik łącząc się z VPN może korzystać wyłącznie z sieci domowej zabezpieczonej hasłem. Domowa sieć komputerowa powinna być odpowiednio zabezpieczona - dostęp do panelu konfiguracyjnego urządzenia sieciowego oraz dostęp do sieci bezprzewodowej (sieci WiFi) powinien być zabezpieczony silnym hasłem, którym nie jest hasło domyślne, zdefiniowane podczas pierwszej konfiguracji urządzenia. Oprogramowanie urządzenia sieciowego powinno być regularnie aktualizowane.
29. Zabrania się pracownikowi łączyć z darmowymi, publicznymi hot-spotami Wi-Fi (kawiarnie, lotniska, dworzec, centra handlowe itp.)
30. W razie potrzeby, Wydział Informatyki skonfiguruje połączenie zdalne na prywatnym sprzęcie komputerowym. Wydział Informatyki wykonuje czynności na urządzeniu prywatnym Pracownika wyłącznie na jego prośbę i pod jego kontrolą oraz nie ponosi odpowiedzialności za problemy techniczne na prywatnym sprzęcie Pracownika.
31. Możliwość połączenia za pomocą VPN jest blokowane w dni robocze w godzinach 18:00 — 6:00, w weekendy i dni wolne.
32. Zabrania się domyślnego zapamiętywania hasła dostępu do konta użytkownika na urządzeniu oraz do programów wykorzystywanych w pracy zdalnej.
33. Zabrania się przechowywania haseł w formie jawnej, ich ujawniania w sposób celowy lub przypadkowy. Hasła i parametry dostępu powinny być znane wyłącznie Pracownikowi.
34. Za ujawnianie danych dostępowych odpowiedzialność ponosi Pracownik.
35. Zabrania się pozostawiania sprzętu komputerowego, na których przetwarza się dane osobowe, bez nadzoru w miejscach publicznych oraz w samochodach i środkach transportu publicznego.

Ich transport powinien odbywać się w sposób uniemożliwiający ich kradzież, zagubienie tub utratę.

36. Z poczty służbowej pracownik korzysta wyłącznie w trakcie aktywnego połączenia VPN, po podłączeniu poprzez pulpit zdalny, do komputera w sieci PODGiK. Zabrania się korzystania z poczty prywatnej w trakcie aktywnego połączenia zdalnego poprzez VPN.
37. W przypadku korzystania z poczty elektronicznej otwieranie linków, załączników z niewiadomego źródła, podawanie danych lub haseł w odpowiedzi na przesłane drogą elektroniczną wiadomości może doprowadzić do zawirusowania komputera, kradzieży, utraty, ujawnienia danych.
38. Pracownik zobowiązany jest do zachowania poufności informacji podczas służbowych rozmów telefonicznych lub wideokonferencji.
39. Zabrania się drukowania dokumentów w ogólnodostępnych punktach.
40. W przypadku chwilowego odejścia od stanowiska pracy należy stosować „zasadę czystego ekranu", to jest zablokować dostęp do komputera (np. skrótem klawiszowym: Windows + L), aby powrót do pracy był możliwy wyłącznie po ponownym uwierzytelnieniu za pomocą hasła.
41. Po zakończeniu pracy zdalnej należy wylogować się z systemów teleinformatycznych, rozłączyć nawiązany kanał VPN, a następnie prawidłowo zamknąć urządzenie wykorzystywane do pracy zdalnej.

§3. Korzystanie z dokumentów papierowych podczas wykonywania pracy zdalnej

1. Zabrania się wynoszenia wszelkiej dokumentacji poza teren Powiatowego Ośrodka Dokumentacji Geodezyjnej i Kartograficznej.
2. Podczas pracy zdalnej, Pracownik może korzystać tylko z dokumentów w formie elektronicznej.
3. W szczególnie uzasadnionych przypadkach Pracownikowi można zezwolić na korzystanie z kopii dokumentów.
4. W przypadku, o którym mowa w ust.3, należy prowadzić ewidencję dokumentów, dla których sporządzono kopie, zawierającą liczbę wykonanych kopii, imię, nazwisko Pracownika, datę wydania kopii, datę zwrotu, a w przypadku zniszczenia datę i sposób zniszczenia kopii.
5. Ewidencję, o którym mowa w ust. 4 prowadzi bezpośredni przełożony pracownika występującego o zgodę.
6. Podczas przenoszenia dokumentów pracownik zobowiązany jest do odpowiedniego ich zabezpieczenia i przenoszenia w taki sposób, aby były niewidoczne dla osób trzecich.
7. Pracownik ma obowiązek zapewnienia bezpieczeństwa dokumentów przed wglądem osób nieupoważnionych oraz przed zniszczeniem, uszkodzeniem, zabraniem przez

osoby nieupoważnione. Po zakończonej pracy dokumenty należy przechowywać w bezpiecznym miejscu jak np. zamykane szafki.

8. Podczas pracy zdalnej pracownik zobowiązany jest przechowywać udostępnione kopie dokumentów papierowych tylko przez okres niezbędny do wykonania określonego zadania podczas pracy zdalnej.

§4. Postanowienia końcowe

1. Przed przystąpieniem do wykonywania pracy zdalnej Pracownik zapoznaje się z treścią niniejszego Regulaminu. Pracownik potwierdza niniejsze pisemnym oświadczeniem i zobowiązaniem do jego przestrzegania. Wzór oświadczenia stanowi Załącznik nr 1 .
2. Zasady postępowania podczas wykonywania pracy zdalnej, minimalizujące ryzyko wystąpienia incydentu zagrażającego bezpieczeństwu teleinformatycznemu PODGiK oraz ryzyko wystąpienia naruszenia praw i wolności osoby fizycznej, z wyszczególnieniem konkretnego zdarzenia oraz sposobu postępowania zostały szczegółowo opisane w Załączniku nr 2 do niniejszej Procedury.
3. W sprawach nieuregulowanych niniejszym Regulaminem zastosowanie znajdą wewnętrzne procedury obowiązujące u Pracodawcy oraz przepisy prawa powszechnie obowiązującego.

Załącznik nr 1 do Procedury ochrony danych osobowych podczas pracy zdalnej
do Zarządzenia nr GKG.GPK.0200.86.2023
Dyrektora Powiatowego Ośrodka Dokumentacji
Geodezyjnej i Kartograficznej
z dnia 10 lipca 2023 r.

OŚWIADCZENIE

Ja niżej podpisana/yKliknij lub naciśnij tutaj, aby wprowadzić tekst.

oświadczam, że podczas wykonywania pracy zdalnej będę przestrzegać obowiązujących przepisów o ochronie danych osobowych (w szczególności rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE), w tym także wewnętrznych aktów prawnych i procedur dotyczących ochrony danych osobowych obowiązujących w PODGiK, a także dbać o bezpieczne przetwarzanie przeze mnie powierzonych mi danych z zapewnieniem, że osoby nieupoważnione nie uzyskają dostępu do tych danych.

Jednocześnie oświadczam, że znane są mi zasady ochrony danych osobowych oraz że zapoznałem/am się z Procedurą ochrony danych osobowych podczas pracy zdalnej.

Data, miejscowość, podpis pracownika Kliknij lub naciśnij tutaj, aby wprowadzić tekst.

Wyk.l egz.
1 — Wydział Organizacyjny i Kadr

Załącznik nr 1 do Procedury ochrony danych osobowych podczas pracy zdalnej
do Zarządzenia nr GKG.GPK.0200.86.2023
Dyrektora Powiatowego Ośrodka Dokumentacji
Geodezyjnej i Kartograficznej
z dnia 10 lipca 2023 r.

Zasady postępowania podczas wykonywania pracy zdalnej, minimalizujące ryzyko wystąpienia incydentu zagrażającego bezpieczeństwu teleinformatycznemu Powiatowego Ośrodka Dokumentacji Geodezyjnej i Kartograficznej oraz ryzyko wystąpienia naruszenia praw i wolności osoby fizycznej.

1. Informacje dla pracownika wykonującego pracę zdalną:

DOTYCZY PRACY NA SPRZĘCIE ELEKTRONICZNYM

ZDARZENIE: Zgubienie/kradzież sprzętu, na którym wykonywana jest praca zdalna.
SPOSOBY POSTĘPOWANIA: Niezwłoczne poinformowanie pracownika Wydziału Informatyki oraz Inspektora Ochrony Danych o zdarzeniu.Niezwłoczna zmiana hasła do sieci Wi-Fi, z którą sprzęt łączy się automatycznie.

ZDARZENIE: Awaria sprzętu, na którym wykonywana jest praca zdalna.
SPOSOBY POSTĘPOWANIA: Niezwłoczne poinformowanie pracownika Wydziału Informatyki o zdarzeniu, zwłaszcza przed oddaniem sprzętu do naprawy.

ZDARZENIE: Przekazanie komputera prywatnego, na którym wykonywana jest praca zdalna innej osobie (np. domownikowi) w miejscu wskazanym pracodawcy jako miejsce wykonywania pracy zdalnej.
SPOSOBY POSTĘPOWANIA: Upewnienie się, że nastąpiło wylogowanie z systemu operacyjnego. Upewnienie się, że nastąpiło rozłączenie połączenia zdalnego oraz połączenia VPN.

ZDARZENIE: Przekazanie komputera prywatnego, na którym wykonywana jest praca zdalna innej osobie, która użytkować go będzie poza miejscem wskazanym pracodawcy jako miejsce wykonywania pracy zdalnej.
SPOSOBY POSTĘPOWANIA: Przed wydaniem komputera prywatnego poinformowanie o tym fakcie pracownika Wydziału Informatyki, w celu zablokowania możliwości wykonywania połączenia VPN.

ZDARZENIE: Ujawnianie sposobu działania aplikacji i systemu, jego zabezpieczeń oraz informacji o sprzęcie i pozostałej infrastrukturze osobom nieuprawnionym.

SPOSOBY POSTĘPOWANIA: W przypadku wystąpienia takiej sytuacji należy przerwać rozmowę lub inną czynność prowadzącą do ujawnienia informacji oraz powiadomić Inspektora Ochrony Danych oraz pracownika Wydziału Informatyki o tym, jaka informacja została ujawniona.

ZDARZENIE: Dopuszczenie, aby osoby nieuprawnione np. domownicy, goście itp. mogli mieć wgląd do plików, aplikacji poprzez użytkowanie komputera w momencie gdy jest aktywne połączenie zdalne
SPOSOBY POSTĘPOWANIA: W przypadku wystąpienia takiej sytuacji należy niezwłocznie podjąć czynność prowadzącą do zabezpieczenia informacji.
Należy wezwać osobę nieuprawnioną do opuszczenia stanowiska pracy i ustalić jakie czynności zostały przez osobę nieuprawnioną wykonane. Należy również powiadomić Inspektora Ochrony Danych o tym, jaka informacja została ujawniona.

ZDARZENIE: Stwarzanie warunków umożliwiających aby osoby nieuprawnione np. domownicy, goście itp. mogli mieć wgląd do plików, aplikacji np. poprzez wgląd do monitora
SPOSOBY POSTĘPOWANIA: Należy przerwać działanie włączonych programów, można wyłączyć monitor lub zablokować dostęp do komputera (np. skrótem klawiszowym: Windows + L).Jeżeli to możliwe, należy ustalić jakie dane były widoczne przez osobę nieuprawnioną i powiadomić Inspektora Ochrony Danych o tym, jaka informacja została ujawniona.

ZDARZENIE: Korzystanie z poczty prywatnej na sprzęcie prywatnym w czasie pracy zdalnej
SPOSOBY POSTĘPOWANIA: Zabrania się korzystania z poczty prywatnej w trakcie połączenia zdalnego poprzez VPN. W momencie gdy pracownik chce skorzystać z poczty prywatnej wykonuje to, na swoim prywatnym komputerze, po rozłączeniu połączenia VPN .

ZDARZENIE: Otrzymanie wiadomości e-mail, dla której zachodzi podejrzenie, że zawiera zainfekowany załącznik lub niebezpieczny link
SPOSOBY POSTĘPOWANIA: W przypadku otrzymania wiadomości e-mail z nieznanego źródła nie należy odpowiadać na wiadomość, otwierać załączników i klikać w linki znajdujące się w treści wiadomości. Podczas obsługi poczty elektronicznej i otrzymywania wiadomości e-mail użytkownik powinien odpowiedzieć sobie na poniższe pytania: Czy znany jest nadawca wiadomości? Czy otrzymano już inne wiadomości od tego nadawcy? Czy spodziewano się otrzymania przedmiotowej wiadomości? Czy tytuł wiadomości i nazwa załącznika mają sens? Czy wiadomość zawiera niegramatyczne zwroty, błędy ortograficzne lub istnieje podejrzenie, że została automatycznie przetłumaczona na język polski? Negatywna odpowiedź na przynajmniej jedno z pytań powinna wzbudzić czujność użytkownika i spowodować, że wiadomość zostanie skasowania bez podejmowania próby odpowiedzi. Proszę zwracać szczególną uwagę na nadawcę wiadomości. Jeżeli nie posiadamy

usług w firmie, która wysyła nam fakturę/załącznik - proszę ją zignorować, zweryfikować poprzez telefon do tej firmy lub powiadomić niezwłocznie pracownika Wydziału Informatyki. W przypadku gdy pracownikowi zależy na otwarciu załącznika/odpowiedzi na maila, przed podjęciem jakiejkolwiek czynności należy skonsultować to z pracownikiem Wydziału Informatyki

ZDARZENIE: Kliknięcie w zainfekowany link/plik otrzymany w wiadomości e-mail
SPOSOBY POSTĘPOWANIA: Zabrania się korzystania z poczty prywatnej w trakcie połączenia zdalnego poprzez VPN. Jeżeli pracownik nie zastosował się do zaleceń i kliknął w zainfekowany plik/link podczas połączenia VPN, należy niezwłocznie rozłączyć połączenie.W momencie kliknięcia w zainfekowany link/plik otrzymany w wiadomości e-mail na poczcie służbowej lub prywatnej, zaleca się niezwłoczne wyłączenie komputera, poprzez przytrzymanie przez kilka sekund włącznika. Pracownik niezwłocznie informuje o zdarzeniu pracownika Wydziału Informatyki

ZDARZENIE: Kliknięcie w zainfekowany link/plik otrzymany w wiadomości e-mail w momencie gdy pracownik nie był połączony poprzez VPN do sieci PODGiK.
SPOSOBY POSTĘPOWANIA: Po kliknięciu w zainfekowany link/plik zabrania się wykonywania połączenia poprzez VPN z siecią PODGiK. Należy niezwłocznie poinformować pracownika Wydziału Informatyki o zaistniałym zdarzeniu. Należy przeskanować komputer programem antywirusowym.

ZDARZENIE: Przerwa w wykonywaniu pracy przy komputerze
SPOSOBY POSTĘPOWANIA: W przypadku chwilowego odejścia od komputera, wykorzystywanego do pracy zdalnej, pracownik powinien zablokować komputer służbowy oraz komputer prywatny. Należy zwrócić uwagę na to, czy blokada nie ograniczyła się jedynie do komputera lokalnego w sieci PODGiK lub do komputera prywatnego. Należy pamiętać, że blokowanie komputera prywatnego, do którego logować się mogą inni domownicy, bez zablokowania systemu na komputerze służbowym (w połączeniu zdalnym) stwarza ryzyko dostępu do danych przez osoby nieuprawnione.

DOTYCZY PRACY NA DOKUMENTACH

ZDARZENIE: Potrzeba pracy na dokumentach w wersji papierowej poza siedzibą PODGiK
SPOSOBY POSTĘPOWANIA: Pracownik informuje o tym fakcie swojego bezpośredniego przełożonego. Po otrzymaniu zgody, Pracownik wnoszący o zgodę lub inna wyznaczona osoba wykonuje kopie dokumentów, które są niezbędne do wykonywania pracy poza siedzibą PODGiK. Pracownik przed wyniesieniem dokumentów poza teren PODGiK przekazuje je bezpośredniemu przełożonemu w celu ich zaewidencjonowania. Pracownik ustala z bezpośrednim przełożonym sposób i miejsce zniszczenia

dokumentów po ustaniu ich przydatności, uwzględniając fakt, że dokumenty należy zniszczyć w sposób uniemożliwiający odczytanie informacji na nich zawartych.

ZDARZENIE: Dopuszczenie i stwarzanie warunków, aby osoby nieuprawnione np. domownicy, goście itp. mogli mieć wgląd do dokumentów papierowych zawierających dane osobowe
SPOSOBY POSTĘPOWANIA: W przypadku wystąpienia takiej sytuacji należy niezwłocznie zabezpieczyć dokumenty. Zaleca się wykonywanie pracy na dokumentach elektronicznych. W przypadku wykorzystywania do pracy dokumentacji papierowej, pracownik przechowuje ją w miejscu uniemożliwiającym odczyt dokumentów przez osoby nieuprawnione. Informację o incydencie, w przypadku ujawnienia danych niezwłocznie przekazuje się Inspektorowi Ochrony Danych.

ZDARZENIE: Tworzenie brudnopisów, wydruków podczas wykonywania pracy zdalnej
SPOSOBY POSTĘPOWANIA: Zaleca się pracę na dokumentach elektronicznych. Każdy dokument papierowy zawierający dane służbowe, powstały podczas wykonywania pracy zdalnej powinien zostać zniszczony w stopniu uniemożliwiającym odczytanie danych na nim zawartych. W momencie gdy pracownik utraci dokument, należy podjąć niezwłocznie czynności umożliwiające jego odzyskanie i zabezpieczenie. Informację o incydencie wraz z informacją jakie dane zawierał dokument niezwłocznie przekazuje się IOD.

DOTYCZY POZOSTAŁYCH CZYNNOŚCI WYKONYWANYCH PODCZAS PRACY ZDALNEJ
ZDARZENIE: Rozmowa telefoniczna w sprawach służbowych
SPOSOBY POSTĘPOWANIA: Pracownik wykonuje służbowe rozmowy telefoniczne w sposób gwarantujący poufność. W momencie wystąpienia sytuacji, która nie gwarantuje poufności informacji pracownik przerywa rozmowę. W przypadku wystąpienia incydentu, polegającego na ujawnieniu danych osobowych osobie nieuprawnionej, pracownik informuje o tym Inspektora Ochrony Danych.

2. Informacja dla bezpośredniego przełożonego pracownika wykonującego pracę zdalną, Wydziału Organizacyjnego i Kadr oraz Wydziału Informatyki

DOTYCZY USTANOWIENIA DOSTĘPU
ZDARZENIE: Pracownik z ważnych powodów wnioskuje o skierowanie go na pracę zdalną
SPOSOBY POSTĘP ZDARZENIE: Pracownik konsultuje z bezpośrednim przełożonym potrzebę wykonywania pracy zdalnej. Pracownik składa wniosek o umożliwienie pracy zdalnej do Pracodawcy. Po otrzymaniu zgody, pracownik udaje się do Wydziału Organizacyjnego i Kadr. Wydział Organizacyjny i Kadr przekazuje informację do Wydziału Informatyki o możliwości ustanowienia dostępu dla

pracownika. Pracownik kieruje się do Wydziału Informatyki w celu otrzymania informacji, które umożliwią mu wykonywanie pracy zdalnej.

ZDARZENIE: Pracownik dostał polecenie pracy zdalnej
SPOSOBY POSTĘPOWANIA: Pracownik otrzymuje polecenie pracy zdalnej. Pracownik udaje się do Wydziału Organizacyjnego i Kadr. Wydział Organizacyjny i Kadr przekazuje informację do Wydziału Informatyki o możliwości ustanowienia dostępu dla pracownika. Pracownik kieruje się do Wydziału Informatyki w celu otrzymania informacji, które umożliwią mu wykonywania pracy zdalnej.

ZDARZENIE: Wykonywanie pracy zdalnej przez pracownika
SPOSOBY POSTĘPOWANIA: Bezpośredni przełożony pracownika, nadzoruje konieczność odbywania pracy zdalnej przez pracownika. Zgłasza do pracodawcy każdą wątpliwość w tym zakresie. Bezpośredni przełożony powinien mieć aktualne informacje o tym, kto ma ustanowiony dostęp VPN, tj. kto aktualnie ma techniczną możliwość wykonywania pracy zdalnej. Bezpośredni przełożony pracownika wykonującego pracę zdalną powinien zostać poinformowany w momencie gdy polecenie pracy zdalnej lub zgoda na pracę zdalną zostanie odwołana.

DOTYCZY ZABLOKOWANIA DOSTĘPU
ZDARZENIE: Pracownik kończy pracę zdalną
SPOSOBY POSTĘPOWANIA: W momencie gdy pracownik zostaje odwołany z pracy zdalnej, Wydział Organizacyjny i Kadr informuje o tym niezwłocznie pracownika Wydziału Informatyki. Pracownik Wydziału Informatyki blokuje dostęp pracownikowi do zasobów PODGiK i przekazuje informację o zablokowaniu do bezpośredniego przełożonego pracownika. Bezpośredni przełożony pracownika powinien oczekiwać informacji zwrotnej od pracownika Wydziału Informatyki, w momencie gdy nie otrzyma informacji o zablokowaniu, powinien skontaktować się z pracownikiem Wydziału Informatyki.