System Zarządzania Bezpieczeństwem Informacji (SZBI)
SZBI-P-05 Procedura pracy zdalnej

10.11.2019

1. Czego dotyczy procedura pracy zdalnej?

Procedura została stworzona w celu usystematyzowania metod pracy poza zasięgiem Administratora Danych Osobowych (ADO). Przez zasięg ADO należy rozumieć:

- Pracę na komputerach i oprogramowaniu służbowym poza siedzibą ADO.
- Pracę na komputerach i oprogramowaniu prywatnym w celach służbowych poza siedzibą ADO.
- Pracę na smartphone'ach służbowych poza siedzibą ADO.
- Pracę na smartphone'ach prywatnych w celach służbowych poza siedzibą ADO.
- Przenoszenie danych przetwarzanych przez oraz w imieniu ADO z użyciem urządzeń prywatnych i służbowych.
- Przenoszenie danych przetwarzanych przez oraz w imieniu ADO z użyciem usługi chmury.

2. Procedura nie obejmuje:

Usług wsparcia, które są realizowane zdalnie przy pomocy narzędzi zdalnego pulpitu (np. TeamViewer, RemoteDesktop). Te zagadnienia usystematyzowano w PBDO-P-05-ProceduraUslugWsparciaZdalnego.docx.

3. Kto powinien stosować niniejszą procedurę?

Procedurę powinny stosować wszystkie osoby, które w wyniku realizacji powierzonych przez ADO obowiązków pracują w sposób oraz z użyciem narzędzi opisanych w punkcie pierwszym oraz posiadających zgodę wydaną przez ADO uprawniającą do wykonywania obowiązków w sposób zdalny.

4. Co zawiera niniejsza procedura?

Niniejsza procedura zawiera:

- Spis zasad, którymi należy kierować się w przypadku przetwarzania danych w sposób opisany w punkcie pierwszym.
- Zestawienie narzędzi wraz z opisem ich działania, które są wymagane dla celów przetwarzania danych osobowych ADO w sposób bezpieczny.

5. Spis zasad dla bezpiecznego przetwarzania danych przy pracy zdalnej:

W celu przetwarzania danych ADO opisanych w punkcie pierwszym w sposób bezpieczny muszą zostać spełnione następujące warunki wstępne przez osobę przetwarzającą:

- **W przypadku uszkodzenia sprzętu prywatnego, na którym przetwarzano dane osobowe ADO, należy niezwłocznie powiadomić o tym ADO i IOD przed rozpoczęciem naprawy urządzenia (oddaniem do serwisu lub wymianą).**
- Oprogramowanie wykorzystywane dla celów przetwarzania danych osobowych musi posiadać wsparcie producenta. Należy przez to rozumieć, że oprogramowanie jest rozwijane i aktualizowane przez producenta.
- Zabrania się wykorzystywania oprogramowania nieposiadającego wsparcia producenta lub nierozwijanego przez producenta od co najmniej dwóch lat ze szczególnym uwzględnieniem systemów operacyjnych firmy Microsoft Windows XP, 7, Vista, 8.
- Zabrania się wykorzystywania dla celów edycji dokumentów pakietu biurowego Microsoft Office w wersji 2010 i starszych. Dopuszczone do użytkowania są wersje 2013, 2016, 2019 i 365.

- Zabrania się przetwarzania danych w usłudze chmury, w tym: przenoszenia, kopiowania danych na dyski chmurowe ze szczególnym uwzględnieniem Google Drive, Microsoft OneDrive, Dropbox, Apple iCloud, itp.
- Zabrania się oddawania do użytku sprzętu służbowego osobom nieuprawnionym w tym członkom rodzin.
- W przypadku współdzielenia sprzętu i oprogramowania pomiędzy różnych użytkowników, np. jeden komputer współdzielony pomiędzy członkami rodziny, nakazuje się wykorzystywanie narzędzi i procedur w niniejszym dokumencie.
- Wszystkie dane osobowe zarządzane przez ADO, a przetwarzane na smartphone'ach i komputerach służbowych i prywatnych powinny być zaszyfrowane. Dopuszcza się nieszyfrowanie danych na stacjonarnych komputerach służbowych, o ile nośnik danych (dysk twardy) w przypadku awarii pozostaje w siedzibie ADO (nie zostanie oddany do serwisu).
- Zaszyfrowane archiwa należy otwierać wyłącznie na komputerach, które znasz (np. swój komputer w pracy lub w domu), nie korzystaj z komputerów publicznie dostępnych (np. w centach handlowych).
- Nie należy logować się do nieznanych sieci WiFi, zwłaszcza tych dostępnych publicznie (np. w hotelu, centrum handlowym, pociągu, na rynku miejskim).

6. Zestawienie narzędzi dla bezpiecznego przetwarzania danych przy pracy zdalnej.

6.1. Cryptomator - narzędzie dla bezpiecznego przetwarzania danych na urządzeniach współdzielonych i dla celów przenoszenia danych.

Cryptomator to całkowicie bezpłatne oprogramowanie służące do szyfrowania danych. Dane szyfrowane algorytmem AES o długości klucza 256 bitów. Szczegóły instalacji i użytkowania, znajdują się w instrukcji SZBI-I-02-Instrukcja użytkowania Cryptomator – bezpieczne przenoszenie danych.

Zalecamy używanie oprogramowania Cryptomator, ponieważ:

- jest łatwy w użyciu, nie wymaga fachowej wiedzy,
- jest stabilnie rozwijany w Unii Europejskiej, przez niemiecką firmę Skymatic od kilku lat,
- jest bezpłatny,
- oferuje solidne szyfrowanie AES 256 bit,
- struktura folderów oraz plików jest szyfrowana w sposób uniemożliwiający jej identyfikację bez Cryptomatora,
- nie wymaga zakładania konta w żadnej witrynie internetowej w przypadku użytkowania.

Cryptomator'a należy używać, gdy:

- prywatny komputer, na którym przetwarzane są dane ADO jest współdzielony pomiędzy różnych użytkowników (np. w rodzinie). Cryptomator umożliwia utworzenie bezpiecznego sejfu danych, które przechowywane są w postaci zaszyfrowanej,
- stosowane są prywatne lub służbowe urządzenia do przenoszenia danych (np. pendrive, płyta CD/DVD, dysk zewnętrzny),
- służbowy komputer, na którym przetwarzane są dane ADO jest współdzielony pomiędzy różnych użytkowników, którzy z uwagi na brak upoważnień nie mogą przetwarzać tego samego zakresu danych osobowych.

6.2. 7zip - narzędzie dla bezpiecznego przetwarzania dla celów przesyłania danych osobowych pocztą elektroniczną.

7zip to całkowicie bezpłatny, również dla celów komercyjnych program służący do archiwizowania plików. 7zip jest również wyposażony w funkcje szyfrowania archiwizowanych plików. Więcej informacji na temat użycia można znaleźć w System Zarządzania Bezpieczeństwem Informacji (SZBI) SZBI-P-03 Procedura szyfrowania załączników poczty elektronicznej.

Zalecamy używanie 7zip, ponieważ:

- jest łatwy w użyciu, nie wymaga fachowej wiedzy,
- bo jest stabilnie rozwijany przez wiele lat, a kod źródłowy jest otwarty,
- jest bezpłatny,
- oferuje solidne szyfrowanie AES 256 bit,
- nie wymaga zakładania konta w żadnej witrynie internetowej w przypadku użytkowania.

7zip należy używać, gdy:

- zachodzi potrzeba przesłania danych osobowych w pliku, np.: Excel (xls, xlsx), Word (doc, docx), PDF lub innym pocztą elektroniczną. Należy bezwzględnie unikać przesyłania danych osobowych pocztą elektroniczną.
- zachodzi potrzeba skopiowania danych osobowych na nośnik przenośny (pendrive), który później zostanie przekazany osobie upoważnionej do przetwarzania tych danych. Należy bezwzględnie unikać kopiowania danych osobowych na nośnik przenośny.

6.3. Szyfrowanie smartfonów.

Funkcja szyfrowania wbudowana jest w system operacyjny smartfona, co oznacza, że w celu zaszyfrowania smartfona nie jest wymagane żadne dodatkowe oprogramowanie.

Szyfrowanie smartfona jest wymaganym elementem bezpieczeństwa w przypadku przetwarzania na tym urządzeniu danych osobowych. Należy przez to rozumieć zapisanie w smartfonie zdjęć, kontaktów, maili oraz innych danych zarządzanych przez ADO.