Copniac Sp. z o.o. Staromiejska 6/10d Katowice
Strona: www.copniac.pl E-mail: biuro@copniac.pl
Tel: 32-790-95-52, 502-922-072, 32-797-68-75
NIP: 634-285-82-84 REGON: 363908132

INSTRUKCJA BEZPIECZNEGO KORZYSTANIA Z APLIKACJI DO UDZIELANIA POŻYCZEK

WER. 1.0

1. Do systemu powinny mieć dostęp tylko osoby uprawnione do dostępu do danych osobowych,

2. Każdy użytkownik ma przypisany swój indywidualny login oraz hasło, których nie powinien nikomu udostępniać.

3. Każdy użytkownik powinien mieć nadane najmniejsze możliwe uprawnienia.

4. Do aplikacji można się logować tylko z osobistych lub firmowych komputerów (nigdy z publicznie dostępnych) z aktualnym oprogramowaniem, z aktualnym i włączonym oprogramowaniem antywirusowym oraz zaporą ogniową, oraz aktualną wersją przeglądarki. Należy unikać dodatków do przeglądarki, stosować jedynie te zaufane. Komputer ten powinien być pod stałą opieką informatyka, tak aby był regularnie aktualizowany i sprawdzany w kierunku bezpieczeństwa.

5. Nie należy zapamiętywać haseł do aplikacji w przeglądarce, ani nigdzie ich zapisywać.

6. Nie zaleca się korzystania z trybu fast startup w Windows 10, ponieważ może powodować, że zapisane tymczasowe pliki z danymi osobowymi pozostaną tam na dłużej niż do kolejnego uruchomienia systemu.

7. System powinien być zabezpieczony przed dostępem osób trzecich. Po odejściu od komputera lub zakończeniu pracy należy wylogować się z aplikacji. Zaleca się uśpienie komputera lub zastosowanie wygaszacza ekranu z hasłem w przypadku odejścia od komputera, nawet na chwilę.

8. Zaleca się korzystanie z połączenia z Internetem ze stałym adresem IP, co umożliwi skonfigurowanie aplikacji w ten sposób, aby dostęp był możliwy tylko z konkretnego adresu IP, czyli w tym wypadku tylko z biura.

9. Aplikacja powinna być tak skonfigurowana aby pracownicy mieli dostęp tylko do danych niezbędnych do ich pracy oraz w godzinach ich pracy, a także z komputerów z biura (patrz punkt 8).

10. W przypadku komputerów przenośnych - zaleca się zastosowanie szyfrowania partycji systemowej lub całego dysku twardego, co w przypadku zagubienia lub kradzieży komputera uniemożliwi odczyt jakichkolwiek danych osobowych zapisanych na tym komputerze.

11. Wszelkie pliki generowane przez program takie jak pliki pdf, docx, xls powinny

być usunięte trwale po ich wydrukowaniu, przejrzeniu. Należy także regularnie usuwać pliki tymczasowe w komputerze, aby upewnić się, że nie ma tam zapisanych wcześniej plików mogących zawierać dane osobowe. Nie należy przesyłać takich plików mailem, ani zapisywać na nośnikach przenośnych np. Pendrive, czy płyty CD/DVD. Jeżeli istnieje potrzeba udostępnienia tych danych osobie 3 np. do biura rachunkowego - należy utworzyć specjalnego użytkownika z minimalnymi uprawnieniami, przykładowo w przypadku biura rachunkowego będą to uprawnienia do raportów. W takiej sytuacji pracownik biura rachunkowego będzie mógł się zalogować w systemie i pobrać raport bezpośrednio z systemu, co jest dużo bezpieczniejszym rozwiązaniem. W takim wypadku, jak każdy użytkownik, biuro rachunkowe powinno zapoznać się i zaakceptować niniejszą instrukcję.

12. Przed zalogowaniem się do aplikacji należy się upewnić, że logujemy się do tej właśnie aplikacji sprawdzając adres oraz to, czy połączenie jest szyfrowane (przedrostek HTTPS). W przypadku braku szyfrowania nie należy się logować. Może to oznaczać awarię lub próbę wyłudzenia danych do logowania. Nie należy podawać danych do logowania na żadnych innych stronach, zapisywać gdziekolwiek lub przekazywać e-mailem.

13. Zaleca się stosowanie dwuskładnikowego logowania do aplikacji - w takiej sytuacji każdorazowe logowanie będzie wymagało podania kodu przesłanego poprzez sms, co sprawi, że nawet przejęcie danych do logowania nie pozwoli na zalogowanie się do aplikacji osobie trzeciej.

14. W przypadku zgłoszeń związanych z działaniem aplikacji np. problemów z jej działaniem, pytań o sposób jej funkcjonowania, jeśli konieczne jest podanie w zgłoszeniu danych klienta lub pożyczki, z którą związane jest zgłoszenie, należy przekazywać identyfikator klienta/pożyczki. Nigdy nie należy przesyłać danych osobowych przez wiadomości email lub sms.

15. Pracownicy Copniac lub osoby przez Copniac wyznaczone mogą uzyskać dostęp do aplikacji oraz danych osobowych w niej zgromadzonych tylko na żądanie administratora danych osobowych lub osobę przez niego wyznaczoną (przykładowo zgłoszenie problemów technicznych) i każdy taki dostęp jest rejestrowany.

16. W aplikacji należy przechowywać dane osobowe tylko w minimalnym, niezbędnym zakresie. Nie należy zapisywać danych osobowych w polach typu uwagi, opis, w wiadomościach itp.

17. Zaleca się, aby komputery, na których korzysta się z aplikacji, były wyposażone w

a. filtry zabezpieczające stacje robocze przed skutkami przepięcia,

b. zasilacze awaryjne

Co pozwoli na bezpieczne zamkniecie aplikacji w sposób umożliwiający poprawne zapisanie przetwarzanych danych w przypadku problemów z zasilaniem.