Polityka bezpieczeństwa programu GGApp

1. Polityka haseł

• Hasło do konta użytkownika powinno mieć co najmniej 8 znaków i zawierać minimum jeden znak z 3 wymienionych grup znakowych:
◦ wielkie litery,
◦ małe litery,
◦ znaki specjalne ~!@#$%^&*,
◦ cyfry;
• Przed zatwierdzeniem hasła jest ono weryfikowane w celu wykluczenia użycia ciągu znaków, który nie spełnia pierwszego podpunktu polityki haseł,
• Format haseł po stronie serwera jest niejawny (zaszyfrowany),
• Hasła powinny być zmieniane przynajmniej raz w miesiącu.

2. Poufność informacji

• Użytkownicy komunikują się z serwerem poprzez połączenie szyfrowane protokołem SSL,
• Każdy użytkownik posiada dostęp wyłącznie do takich danych, do jakich w danym momencie dostęp mieć powinien,
• Serwer przechowuje logi połączeń.

3. Zabezpieczenie stacji roboczej

• Użytkownicy nie powinni odchodzić od stacji bez zablokowania komputera,
• Użytkownicy powinni chronić swoje hasła w jak największym stopniu.

4. Odpowiedzialność pracowników za dane poufne

• Każdy pracownik odpowiada za utrzymanie danych poufnych w tajemnicy,
• Każdy pracownik zobowiązany jest do ochrony swoich danych dostępowych do systemów informatycznych, w szczególności są to hasła dostępów, klucze softwarowe oraz sprzętowe,
• Pracownicy w zależności od zajmowanego stanowiska muszą ukończyć szkolenia z zakresu ochrony Danych Osobowych, świadomości istnienia problemów bezpieczeństwa, szczegółowych aspektów bezpieczeństwa.

5. Korzystanie z firmowej infrastruktury IT w celach prywatnych

• Zabrania się korzystania firmowej infrastruktury IT w celach prywatnych,
• Sieć lokalna musi być odpowiednio chroniona przed nieuprawnionym dostępne, przykładowo goście nie mogą uzyskać dostępu do sieci lokalnej,
• Systemy IT przechowujące dane poufne (np. dane osobowe) muszą być odpowiednio zabezpieczone.

6. Publiczne udostępnianie infrastruktury IT

Infrastruktura udostępniona publicznie musi być szczególnie

zabezpieczona.
• Dostęp do upublicznionej infrastruktury nie może dać możliwości połączenia z wewnętrzną siecią
• Systemy IT przechowujące dane poufne (np. dane osobowe) muszą być odpowiednio zabezpieczone
• Wykonywanie wewnętrznej lub zewnętrznej weryfikacji bezpieczeństwa poprzez np. testy penetracyjne
• Zwiększanie bezpieczeństwa poprzez hardening systemu

7. Kopie zapasowe

• Każde istotne dane (w tym dane poufne) powinny być archiwizowane.
• Zarchiwizowane dane powinny być trzymane w niedostępnym dla osób nieupoważnionych miejscu.
• Wszelakie podejrzenia naruszenia bezpieczeństwa danych w Firmie należy zgłaszać do Zarządu Spółki GiganticGranite