Generali Towarzystwo Ubezpieczeń S.A.
ul. Senatorska 18
00-082 Warszawa
generali.pl

Oświadczenia niezbędne do zawarcia umowy ubezpieczenia cyber dla KIRP
Grupa indywidualna

1.	Przychód firmy za ostatni rok obrachunkowy	_____ PLN
2.	Liczba pracowników merytorycznych[1] świadczących usługi	_____ pracowników merytorycznych
3.	Oświadczam, iż nie mam wiedzy, aby w ciągu 3 ostatnich lat w mojej firmie doszło do zdarzeń naruszających bezpieczeństwo cyfrowe, w tym m.in. wycieku danych, nieautoryzowanego dostępu, blokady usług (np. DDoS), przestoju spowodowanego incydentem cyber, naruszenia bezpieczeństwa sieci.	☐TAK ☐NIE
4.	Oświadczam, że stosuję **uwierzytelnianie wieloskładnikowe** przy dostępie do danych zawartych w **chmurze.**	☐TAK ☐NIE
5.	Oświadczam, że regularnie ale nie rzadziej niż raz na pół roku, wykonuję kopie zapasowe danych przechowywanych cyfrowo (tzw. backup) **w formie zaszyfrowanej** lub bez dostępu do sieci.	☐TAK ☐NIE
6.	Oświadczam, że nie korzystam z systemów operacyjnych pozbawionych wsparcia producenta[2], wgrywam **poprawki bezpieczeństwa** maksymalnie 30 dni od ich wydania i używam tylko i wyłącznie legalnego oprogramowania.	☐TAK ☐NIE
7.	Oświadczam, że korzystam z aktualizowanego na bieżąco **oprogramowania antywirusowego** na komputerach[3].	☐TAK ☐NIE
8.	Oświadczam, że **szyfruję** lub zabezpieczam hasłem dokumenty elektroniczne zawierające dane osobowe oraz inne informacje o charakterze niejawnym przed ich wysyłaniem pocztą elektroniczną.	☐TAK ☐NIE
9.	Oświadczam, że posiadam stronę internetową mojej firmy.	☐TAK ☐NIE Jeżeli tak, prosimy o wskazanie adresu internetowego strony: _____

Kwalifikacja do programu ubezpieczenia wymaga udzielenia odpowiedzi na wszystkie ww. pytania.
W przypadku negatywnej odpowiedzi na pytania 3-8 Wnioskujący nie kwalifikuje się do zawarcia umowy ubezpieczenia w ramach programu.
W wypadku udzielenia odpowiedzi na pytania 3-8 w sposób niezgodny ze stanem rzeczywistym ochrona ubezpieczeniowa wynikająca z programu nie ma zastosowania.

_____

[1] Za **pracowników merytorycznych** uważa się radców prawnych, adwokatów oraz aplikantów tych zawodów
[2] Daty wycofania wsparcia dla najpopularniejszych systemów i języków programowania można sprawdzić tutaj: endoflife.date
[3] Nie dotyczy smartfonów

Generali Towarzystwo Ubezpieczeń S.A. z siedzibą przy ul. Senatorska 18, 00-082 Warszawa, zarejestrowana w Sądzie Rejonowym dla m.st. Warszawy, XII Wydział Gospodarczy Krajowego Rejestru Sądowego pod numer em KRS 10623, kapitał zakładowy 236 509.000 PLN, w pełni opłacony, NIP 526-23-49-108. Spółka należy do Grupy Generali figurującej w Rejestrze Grup Ubezpieczeniowych prowadzonym przez Instytut Nadzoru Ubezpieczeniowego (IVASS) pod nr 26.

Generali Towarzystwo Ubezpieczeń S.A.
ul. Senatorska 18
00-082 Warszawa
generali.pl

SŁOWNIK POJĘĆ

1. **Uwierzytelnianie wieloskładnikowe (and. Multi-Factor Authentication, MFA) –** proces zabezpieczenia dostępu do konta lub systemu, który wymaga więcej niż jednego sposobu potwierdzenia tożsamości użytkownika, np. hasło oraz kod SMS/token z aplikacji/klucz bezpieczeństwa. Za uwierzytelnianie wieloskładnikowe należy uznać proces autoryzacji, w którym użytkownik podaje co najmniej dwa czynniki ze wskazanych obszarów:
   a. Coś, co wiem – np. login i hasło
   b. Coś, co mam – np. token z aplikacji, hasło SMS, klucz bezpieczeństwa
   c. Ktoś, kim jestem – biometria rozumiana jako odciski papilarne, skan twarzy, skan siatkówki oka, etc.
2. **Chmura obliczeniowa** – usługa, która umożliwia przechowywanie danych na zdalnych serwerach, do których można uzyskać dostęp przez internet; dzięki temu użytkownicy mogą przechowywać, zarządzać i przetwarzać dane bez potrzeby posiadania własnego sprzętu; do najpopularniejszych dysków chmurowych można zaliczyć:
   a. Google Drive (Dysk Google)
   b. iCloud
   c. OneDrive
   d. Dropbox
3. **Szyfrowanie backupu (kopii zapasowej)** – to proces zabezpieczenia kopii zapasowych danych poprzez ich zaszyfrowanie, czyli przekształcenie w formę nieczytelną dla osób nieuprawnionych, dzięki czemu nawet w wypadku przechwycenia takiej kopii dane pozostają bezpieczne; do szyfrowania kopii zapasowych wykorzystywane są m.in. następujące rozwiązania:
   a. **BitLocker** – narzędzie wbudowane w system Windows
   b. **Veeam Backup & Replication**
   c. **Acronis True Image**
   d. **Backup Exec**
4. **Poprawki bezpieczeństwa oprogramowania –** aktualizacje oprogramowania, które naprawiają wykryte luki i błędy mogące stanowić zagrożenie dla bezpieczeństwa systemu. Regularne stosowanie poprawek jest kluczowe dla ochrony przed atakami cybernetycznymi
5. **Oprogramowanie antywirusowe** – to programy zaprojektowane do wykrywania, blokowania i usuwania złośliwego oprogramowania z komputerów i innych urządzeń. Chronią systemy przed wirusami komputerowymi, trojanami, robakami i innymi znanymi zagrożeniami. Operują na podstawie tzw. sygnatur, czyli bazy danych zawierających fragmenty złośliwego kodu komputerowego, które twórca oprogramowania dodał w ramach aktualizacji bazy. Nie chronią przed atakami typu 0-day oraz innymi atakami złożonymi.
6. **Szyfrowanie poczty elektronicznej** - jest to proces zabezpieczania wiadomości e-mail, aby tylko uprawnieni odbiorcy mogli je odczytać. Popularne protokoły szyfrowania poczty elektronicznej to:
   - **SSL/TLS (Secure Sockets Layer/Transport Layer Security**) - używane do szyfrowania połączeń między klientem poczty a serwerem,
   - **PGP (Pretty Good Privacy)** - używane do szyfrowania treści wiadomości e-mail,
   - **S/MIME (Secure/Multipurpose Internet Mail Extensions)** - używane do szyfrowania i podpisywania wiadomości e-mail,
   - **SMTP** (Simple Mail Transfer Protocol) – SMTP sam w sobie nie zapewnia szyfrowania, co oznacza, że dane przesyłane przez ten protokół mogą być podatne na przechwycenie; aby zwiększyć bezpieczeństwo stosuje się rozszerzenia takie jak STARTTLS, które umożliwiają szyfrowanie połączeń SMTP za pomocą protokołu SSL/TLS
   - **POP3 (Post Office Protocol version 3) –** POP3 nie zapewnia domyślnie szyfrowania, jednak podobnie jak w przypadku SMTP można używać POP3S (z dopiskiem „Secure"), który korzysta z SSL/TLS do szyfrowania połączeń
   - **IMAP (Internet Message Access Protocol)** – domyślnie nie oferuje szyfrowania, ale istnieje jego bezpieczniejsza wersja IMAPS (IMAP Secure), który używa SSL/TLS do szyfrowania połączeń

Generali Towarzystwo Ubezpieczeń S.A. z siedzibą przy ul. Senatorska 18, 00-082 Warszawa, zarejestrowana w Sądzie Rejonowym dla m.st. Warszawy, XII Wydział Gospodarczy Krajowego Rejestru Sądowego pod numer em KRS 10623, kapitał zakładowy 236 509.000 PLN, w pełni opłacony, NIP 526-23-49-108. Spółka należy do Grupy Generali figurującej w Rejestrze Grup Ubezpieczeniowych prowadzonym przez Instytut Nadzoru Ubezpieczeniowego (IVASS) pod nr 26.