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

**Oświadczenia niezbędne do zawarcia umowy ubezpieczenia cyber dla KIRP**
**Grupa kolektywna**

| | | |
|---|---|---|
| 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<br>☐NIE |
| 4. | Oświadczam, że stosuję **uwierzytelnianie wieloskładnikowe** przy zdalnym dostępie do danych zawartych w **chmurze** oraz na serwerach firmy. | ☐TAK<br>☐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<br>☐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<br>☐NIE |
| 7. | Oświadczam, że korzystam z aktualizowanego na bieżąco **oprogramowania antywirusowego** na komputerach[3]. | ☐TAK<br>☐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<br>☐NIE |
| 9. | Oświadczam, że dostęp do danych osobowych i informacji niejawnych jest **objęty polityką minimalizacji uprawnień**. | ☐TAK<br>☐NIE |
| 10. | Oświadczam, że w firmie stosowana jest **polityka haseł** wymagająca wykorzystywania haseł o określonym poziomie skomplikowania (minimum 8 znaków, duże i małe litery, cyfry, znaki specjalne) | ☐TAK<br>☐NIE |
| 11. | Oświadczam, że posiadam stronę internetową mojej firmy. | ☐TAK<br>☐NIE<br><br>Jeżeli tak, prosimy o wskazanie adresu internetowego strony:<br>_____ |

***Kwalifikacja do programu ubezpieczenia wymaga udzielenia odpowiedzi na wszystkie ww. pytania.***
*W przypadku negatywnej odpowiedzi na pytania 3-10 Wnioskujący nie kwalifikuje się do zawarcia umowy ubezpieczenia w ramach programu.*
*W wypadku udzielenia odpowiedzi na pytania 3-10 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.
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

7. **Polityka minimalizacji uprawnień** (ang. Least priviledge policy) – to zasada bezpieczeństwa informatycznego, która polega na przyznawaniu użytkownikom, programom i procesom tylko tych uprawnień, które są niezbędne do wykonania ich zadań. Oznacza to, że każdy użytkownik lub proces ma dostęp tylko do tych zasobów i funkcji, które są absolutnie konieczne do wykonania ich pracy, a nie więcej. Korzyści płynące z polityki minimalizacji uprawnień to:
    - **Zwiększone bezpieczeństwo** – ograniczenie uprawnień minimalizuje ryzyko nieautoryzowanego dostępu do wrażliwych danych i systemów
    - **Ograniczenie skutków naruszeń** – w przypadku, gdy konto użytkownika lub proces zostanie skompromitowany (potocznie: „zhackowany"), atakujący będzie miał dostęp tylko do ograniczonego zakresu zasobów
    - **Łatwiejsze zarządzanie** - mniej uprawnień do zarządzania oznacza prostsze monitorowanie i dostępu
8. **Polityka haseł** – to zbiór zasad i wytycznych dotyczących tworzenia, używania i zarządzania hasłami w organizacji. Celem polityki jest zapewnienie, że hasła są wystarczająco silne, aby chronić konta użytkowników i systemy przed nieautoryzowanym dostępem. Zazwyczaj jest rozwiązaniem technicznym, wdrażanym wobec domeny firmowej (służbowych kont pracowników), coraz rzadziej spotyka się polityki haseł w formie papierowej. Polityka haseł reguluje kwestie takie jak:
    - **Złożoność haseł** – wymaganie kombinacji dużych i małych liter, cyfr oraz znaków specjalnych
    - **Długość haseł** – wymaganie minimalnej liczby znaków, która nie powinna być mniejsza niż 8
    - **Częstotliwość zmiany haseł** – reguły dotyczące okresu obowiązywania i wymuszania zmiany hasła na nowe
    - **Historia hasła** – reguły zakazujące wykorzystania tego samego hasła w kolejnych okresach
    - **Zwielokrotnienie hasła** – wytyczne zakazujące wykorzystania tego samego hasła w wielu usługach/serwisach/systemach
    - **Inne czynniki** – takie jak edukacja użytkowników nt. haseł, wykorzystanie uwierzytelniania wieloskładnikowego