KWESTIONARIUSZ OCENY RYZYKA CYBERNETYCZNEGO
CYBER RISK ASSESSMENT QUESTIONNAIRE
CYBER GUARD

WSTĘP
INTRODUCTION

Ten kwestionariusz ma na celu dostarczenie nam kompleksowego obrazu skuteczności i dojrzałości systemu bezpieczeństwa informacji i danych w Państwa firmie. Odpowiedzi na poniższe pytania są bardzo ważne do oceny ryzyka, której przeprowadzenie jest niezbędne, aby dostarczyć Państwu propozycję ubezpieczenia cybernetycznego. W swojej ocenie opieramy się na Państwa oświadczeniach złożonych w kwestionariuszu, które są podstawą do zawarcia umowy ubezpieczenia. Kwestionariusz powinien być podpisany przez osobę upoważnioną do reprezentowania spółki.

Niniejszy kwestionariusz nie stanowi oferty ani zobowiązania do zawarcia umowy ubezpieczenia. Ponadto wypełnienie tego kwestionariusza nie zobowiązuje ubezpieczyciela do zaoferowania Państwu ochrony ubezpieczeniowej.

Jeżeli jakieś informacje nie mieszczą się w kwestionariuszu, prosimy o przekazanie ich w załączniku do niego.

This questionnaire is designed to provide us with a comprehensive view of the effectiveness and maturity of information and data security within your company. The answers to the questions are very important to us for assessing the risk in order to provide cyber insurance to you based on the information we receive. Therefore we rely on your statements made in the questionnaire which are the basis for the insurance contract. Questionnaire should be signed by an authorized representative.

This questionnaire is neither an offering nor binding of an insurance contract (coverage). Furthermore the completion of this questionnaire does not obligate the insurer to offer coverage to you.

If there are any information you want to provide, please do so in an attachment to this questionnaire.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Waluta użyta w kwestionariuszu Currency used for this questionnaire  | [ ]  | USD | [ ]  | EUR | [ ]  | GBP | [x]  | Inna OtherClick or tap here to enter text. |

1. SPÓŁKA – INFORMACJE O WNIOSKODAWCY
COMPANY – APPLICANT INFORMATION

|  |  |
| --- | --- |
| Nazwa wnioskodawcy Name of applicant | Click or tap here to enter text. |
| Adres Address | Click or tap here to enter text. |
| Państwo Country | Click or tap here to enter text. |
| NIP TIN | Click or tap here to enter text. |
| Email Email | Click or tap here to enter text. |
| Telefon Phone | Click or tap here to enter text. |
| Spółki zależne Subsidiaries | Click or tap here to enter text. |
| Domeny Domains | Click or tap here to enter text. |

* 1. SEKTORY BRANŻOWE
	INDUSTRIAL SECTOR(S)

Prosimy o podanie szczegółowego opisu usług świadczonych przez wnioskodawcę
Please provide detailed description of services provided by the applicant

Click or tap here to enter text.

* 1. OBRÓT/PRZYCHÓD I ZASIĘG REGIONALNY
	TURNOVER/REVENUE AND REGIONAL FOOTPRINT



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **KrajowyDomestic** | **USA** | **Unia EuropejskaEuropean Union**  | **Pozostałe kraje świata Rest of world** |
| **Obrót za ostatni rok podatkowy Your turnover for the last fiscal year** | Click or tap here to enter text. | Click or tap here to enter text. | Click or tap here to enter text. | Click or tap here to enter text. |
| **Zysk przed opodatkowaniem za ostatni rok podatkowy Your gross profit for last fiscal year** | Click or tap here to enter text. | Click or tap here to enter text. | Click or tap here to enter text. | Click or tap here to enter text. |

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Poprzedni rok Last year** | **Szacowany w tym roku Planned this year** | **Szacowany w przyszłym roku Planned next year** |
| **Obrót Your turnover** | Click or tap here to enter text. | Click or tap here to enter text. | Click or tap here to enter text. |
| **Zysk przed opodatkowaniem Your gross profit** | Click or tap here to enter text. | Click or tap here to enter text. | Click or tap here to enter text. |

|  |  |
| --- | --- |
| **Liczba pracownikówThe number of employees**  | Click or tap here to enter text. |
| Przybliżona liczba urządzeń IT The estimated number of individual IT devices deployed | SerweryServers | Click or tap here to enter text. | Komputery stacjonarne Desktops | Click or tap here to enter text. |
| LaptopyLaptops | Click or tap here to enter text. | Urządzenia mobilne Mobile devices | Click or tap here to enter text. |

* 1. RODZAJ I ILOŚĆ DANYCH
	TYPE AND QUANTITY OF DATA

Prosimy o podanie rodzaju i liczby następujących kategorii danych wrażliwych, które według Państwa wiedzy są przechowywane/przetwarzane przez Państwa firmę.

Please estimate type and volume of the following categories of sensitive data your company is maintaining/processing to the best of your knowledge.

|  |  |  |
| --- | --- | --- |
| **Rodzaj danych Type of data**  | **Liczba pojedynczych rekordów Number of unique records**  | **Liczba pojedynczych rekordów obywateli USA Number of unique records of US citizens** |
| Informacje umożliwiające identyfikację osób Personally Identifiable Information (PII)  | Click or tap here to enter text. | Click or tap here to enter text. |
| Informacje o kartach płatniczych Payment Card Information (PCI) | Click or tap here to enter text. | Click or tap here to enter text. |

* 1. ZDARZENIA ZWIĄZANE Z NARUSZENIEM BEZPIECZEŃSTWA INFORMACJI I HISTORIA SZKÓD
	INFORMATION SECURITY EVENTS AND LOSS HISTORY

Prosimy odpowiedzieć na poniższe pytania, biorąc pod uwagę okres ostatnich **trzech lat.**
Please answer the following questions by considering any time during the past **three years**.

|  |  |  |
| --- | --- | --- |
| 1. | Czy miały miejsce jakiekolwiek **incydenty, roszczenia lub pozwy** związane z nieautoryzowanym dostępem lub niewłaściwym wykorzystaniem sieci, w tym defraudacja, oszustwo, kradzież informacji poufnych, naruszenie danych osobowych, kradzież lub utrata laptopów, odmowa usługi, elektroniczny wandalizm lub sabotaż, wirus komputerowy lub inny incydent?Have you had any **incidents, claims or suits** involving unauthorized access or misuse of your network, including embezzlement, fraud, theft of proprietary information, breach of personal information, theft or loss of laptops, denial of service, electronic vandalism or sabotage, computer virus or other incident? | [ ]  Tak Yes[ ]  Nie No |
| 2. | Czy doświadczyli Państwo **nieplanowanej przerwy w działalności gospodarczej**, dłuższej niż cztery godziny, spowodowanej incydentem cybernetycznym?Have you experienced an **unplanned business interruption** of longer than four hours caused by a cyber incident?  | [ ]  Tak Yes[ ]  Nie No |
| 3. | Czy doświadczyli Państwo **próby wymuszenia lub żądania okupu** dotyczących Państwa systemów komputerowych?Have you experienced an **extortion attempt or demand** with respect to your computer systems? /  | [ ]  Tak Yes[ ]  Nie No |
| 4. | Czy otrzymali Państwo jakiekolwiek **roszczenia lub skargi** w związku ze zniesławieniem, naruszeniem prywatności, kradzieżą informacji, naruszeniem bezpieczeństwa informacji, przesłaniem złośliwego oprogramowania, udziałem w ataku typu denial of service albo żądaniem powiadomienia osób fizycznych w związku z faktycznym lub domniemanym ujawnieniem danych osobowych?Have you received any **claims or complaints** with respect to allegations of defamation, invasion or injury of privacy, theft of information, breach of information security, transmission of malware, participation in a denial of service attack, request to notify individuals due to an actual or suspected disclosure of personal information? | [ ]  Tak Yes[ ]  Nie No |
| 5. | Czy jakiekolwiek organy administracji wszczęły wobec Państwa jakiekolwiek **czynności, śledztwo lub wystosowały wezwanie** dotyczące faktycznego lub domniemanego naruszenia prawa lub przepisów dotyczących ochrony danych, informacji lub prywatności?Have you been subject to any **government action, investigation or subpoena** regarding any (alleged) violation of any (privacy) law or regulation? | [ ]  Tak Yes[ ]  Nie No |
| 6. | Czy wiedzą Państwo o jakimkolwiek **nieuprawnionym udostępnieniu, utracie lub ujawnieniu** informacji umożliwiających identyfikację osób, które znajdują się w Państwa posiadaniu, pod Państwa kontrolą lub opieką, lub też pod kontrolą kogokolwiek, kto przechowuje takie informacje w Państwa imieniu?Are you aware of any **release, loss or disclosure of personally identifiable information** in your care, custody or control, or in the control of anyone holding such information on behalf of you? | [ ]  Tak Yes[ ]  Nie No |
| 7. | Czy wiedzą Państwo o jakimkolwiek **zaistniałym lub domniemanym fakcie, okoliczności, sytuacji, błędzie lub zaniechaniu, lub innej sytuacji**, która mogłaby spowodować stratę lub roszczenie w ramach ubezpieczenia cybernetycznego, o które się Państwo ubiegają, lub innego podobnego ubezpieczenia obecnie lub poprzednio obowiązującego lub obecnie proponowanego?Are you aware of any **actual or alleged fact, circumstance, situation, error or omission, or potential issue** which might give rise to a loss or claim against you under the cyber insurance policy for which you are applying for or any similar insurance presently or previously in effect or currently proposed? | [ ]  Tak Yes[ ]  Nie No |

Jeżeli na jedno lub więcej pytań w sekcji 1.4 udzielono odpowiedzi „Tak”, prosimy załączyć opis zawierający szczegóły (przyczyna, koszty, powiadomienie, czas do wykrycia, czas odzyskania i kroki podjęte w celu zmniejszenia narażenia w przyszłości) każdego zdarzenia (incydentu, roszczenia itp.).
If one question or more of this section 1.4 is answered with “Yes”, please attach a description including complete details (cause, costs, notification, time to discover, recovery time and steps taken to mitigate future exposure) of each event (incident, claim etc.).

* 1. REGULACJE I STANDARDY
	FRAMEWORKS AND STANDARDS

Prosimy zaznaczyć, które regulacje dotyczą działalności wnioskodawcy i **czy są przestrzegane**:
Please specify which frameworks you are required to be and are compliant with:

|  |  |
| --- | --- |
| [ ]  | Ogólne rozporządzenie o ochronie danych (GDPR) Unii Europejskiej (UE)General Data Protection Regulation (GDPR) of the European Union (EU)  |
| [ ]  | NIS/KSC/KSC2 |
| [x]  | Ustawa o przenoszeniu i odpowiedzialności za ubezpieczenia zdrowotne w USA (HIPAA) oraz ustawa o technologii informacji zdrowotnej dla zdrowia ekonomicznego i klinicznego (HITECH) w USA US Health Insurance Portability and Accountability Act (HIPAA) and US Health Information Technology for Economic and Clinical Health (HITECH) Act |
| [x]  | Inne, jakie Other, which: Click or tap here to enter text. |

Prosimy zaznaczyć wszystkie normy, dla których przeszli Państwo pomyślnie audyt lub posiadają ważny certyfikat.
Please check all standards for which you have successfully been audited or hold a valid ertificate.

|  |  |
| --- | --- |
| [x]  | Payment Card Industry Data Security Standard (PCI DSS) |
| [x]  | Merchant level 1 | [x]  | Merchant level 2 | [x]  | Merchant level 3 | [x]  | Merchant level 4 |

|  |  |
| --- | --- |
| [ ]  | Systemy zarządzania bezpieczeństwem informacji ISO 27001:2013 Information security management systems |
| [ ]  | Inne Other Click or tap here to enter text. |

1. BEZPIECZEŃSTWO INFORMACJI
INFORMATION SECURITY

Poniższe pytania pomogą nam ocenić poziom zaawansowania bezpieczeństwa informacji w Państwa firmie. Prosimy odpowiedzieć na wszystkie pytania i przedstawić dowody, jeśli są dostępne (np. raporty, prezentacje, dokumenty itp.). Pytania są ułożone zgodnie z klauzulami normy ISO/IEC 27002. Stąd pytania koncentrujące się na jednym celu bezpieczeństwa mogą pojawić się w różnych sekcjach niniejszego kwestionariusza. Aby lepiej zrozumieć, dlaczego zadajemy pytania, każda sekcja zaczyna się od celu (celów) kategorii kontroli bezpieczeństwa ISO.

The following questions help us to evaluate the maturity of your information security. Please answer all questions and provide evidence where available (e.g. reports, presentations, documents etc.). The questions are structured according to the clauses of the ISO/IEC 27002 standard. Hence questions focusing on one security objective can appear in different sections of this questionnaire. In order to create a better understanding about why we ask the questions, each section starts with the objective(s) of the ISO security control categories.

* 1. POLITYKA BEZPIECZEŃSTWA INFORMACJI
	INFORMATION SECURITY POLICIES

**Cel:** Zapewnienie zarządzania, kierowania i wsparcia dla systemu bezpieczeństwa informacji zgodnie z wymaganiami biznesowymi i odpowiednimi przepisami prawa.
**Objective:** To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

|  |  |  |
| --- | --- | --- |
| 1. | Czy opracowali Państwo i wdrożyli politykę bezpieczeństwa informacji, która obejmuje całą spółkę i jest stale dostępna dla wszystkich pracowników i podwykonawców?Have you developed and implemented a formal information security policy which is corporate-wide and permanently available for all employees and relevant external parties? | [ ]  Tak Yes[ ]  Nie No |

## ORGANIZACJA BEZPIECZEŃSTWA INFORMACJI ORGANIZATION OF INFORMATION SECURITY

**Cel:** Ustanowienie struktury zarządzania w celu inicjowania i kontrolowania wdrażania i funkcjonowania bezpieczeństwa informacji w organizacji.
**Objective:** To establish a management framework to initiate and control the implementation and operation of information security within the organization.

|  |  |  |
| --- | --- | --- |
| 1. | Czy wyznaczono osobę odpowiedzialną za bezpieczeństwo informacji (np. dyrektor ds. bezpieczeństwa informacji)?Have you assigned a responsible person for information security (e.g. Chief Information Security Officer “CISO”)? | [ ]  Tak Yes[ ]  Nie No |
| 2. | Czy mają Państwo aktualną listę osób odpowiedzialnych i kontaktów zewnętrznych, które muszą być poinformowane w przypadku wystąpienia incydentu związanego z bezpieczeństwem informacji?Do you have an up to date list of authorities and external contacts, which must be informed in case of an information security incident? | [ ]  Tak Yes[ ]  Nie No |

## BEZPIECZEŃSTWO INFORMACJI DLA ZASOBÓW LUDZKICH HUMAN RESOURCE SECURITY

**Cel:** Zapewnienie, że pracownicy i wykonawcy rozumieją swoje obowiązki i są odpowiedni do ról, które im przypisano. Zapewnienie, że pracownicy i wykonawcy są świadomi i wypełniają swoje obowiązki w zakresie bezpieczeństwa informacji. Ochrona interesów organizacji w ramach procesu zmiany lub zakończenia zatrudnienia.
**Objective:** To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered. To ensure that employees and contractors are aware of and fulfil their information security responsibilities. To protect the organization’s interests as part of the process of changing or terminating employment**.**

|  |  |  |
| --- | --- | --- |
| 1. | Czy prowadzą Państwo co najmniej raz w roku szkolenia mające na celu zwiększenie świadomości bezpieczeństwa użytkowników (pracowników i kontrahentów) oraz przygotowanie użytkowników do większej czujności i odporności na phishing?Do you provide at least annual education to increase your users (employees and contractors) security awareness and to prepare users to be more resilient and vigilant against phishing? | [ ]  Tak Yes[ ]  Nie No |

## ZARZĄDZANIE AKTYWAMI ASSET MANAGEMENT

**Cel:** Identyfikacja zasobów organizacyjnych i określenie odpowiednich obowiązków w zakresie ochrony. Zapewnienie, że informacja ma poziom ochrony odpowiedni do jej znaczenia dla organizacji. Zapobieganie nieautoryzowanemu ujawnieniu, modyfikacji, usunięciu lub zniszczeniu informacji przechowywanych na nośnikach.
**Objective:** To identify organizational assets and define appropriate protection responsibilities. To ensure that information receives an appropriate level of protection in accordance with its importance to the organization. To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.

|  |  |  |
| --- | --- | --- |
| 1. | Czy prowadzony jest aktualny spis oprogramowania (w tym systemów operacyjnych) i zasobów sprzętowych w sieci?Do you keep an up-to-date inventory of software (incl. operating systems) and hardware assets in your network?  | [ ]  Tak Yes[ ]  Nie No |
| 2. | Czy klasyfikują Państwo informacje pod względem poufności, integralności, dostępności?Do you classify information (i.e. with regards to confidentiality, integrity, availability)?  | [ ]  Tak Yes[ ]  Nie No |
|  | Jeśli tak, to w jaki sposób?If yes, how? | Click or tap here to enter text. |
| 3. | Czy wprowadzono rozwiązania techniczne umożliwiające nadzorowanie stosowania tej klasyfikacji?Have you technically enforced the information classification scheme? | [ ]  Tak Yes[ ]  Nie No |
| 4. | Czy udzielają Państwo pracownikom instrukcji, jak postępować z informacjami niejawnymi?Do you provide guidance how to handle classified information? | [ ]  Tak Yes[ ]  Nie No |
| 5. | Czy blokują Państwo osobom nieuprawnionym dostęp do informacji poufnych przechowywanych na nośnikach wymiennych, takich jak zewnętrzne urządzenia pamięci masowej (np. pamięci USB lub dyski twarde), albo czy szyfrują je Państwo?Do you either restrict access to or encrypt confidential information stored on removable media like external storage devices (e.g. USB sticks or hard disks)? | [ ]  Tak Yes[ ]  Nie No |
| 6. | Czy trwale pozbywają się Państwo nośników zawierających informacje wrażliwe, jeśli nie są one już używane?Do you securely dispose media containing sensitive information if it is not used any longer? | [ ]  Tak Yes[ ]  Nie No |
| 7. | Czy korzystają Państwo z jakiegokolwiek oprogramowania bądź sprzętu, dla którego producent wycofał wsparcie (np. systemy operacyjne Windows, stary firmware na routerach)? Do you use any unsupported software or hardware (e.g. Windows operating systems, old router firmware)? | [ ]  Tak Yes[ ]  Nie No |
|  | Jeśli tak, to czy są połączone z siecią publiczną?If yes, are they connected to any public networks? | [ ]  Tak Yes[ ]  Nie No |

## KONTROLA DOSTĘPU ACCESS CONTROL

**Cel:** Ograniczenie dostępu do informacji i urządzeń przetwarzających informacje. Zapewnienie autoryzowanego dostępu użytkowników i zapobieganie nieautoryzowanemu dostępowi do systemów i usług. Nałożenie na użytkowników odpowiedzialności za zabezpieczenie informacji uwierzytelniających. Zapobieganie nieuprawnionemu dostępowi do systemów i aplikacji.
**Objective:** To limit access to information and information processing facilities. To ensure authorized user access and to prevent unauthorized access to systems and services. To make users accountable for safeguarding their authentication information. To prevent unauthorized access to systems and applications.

|  |  |  |
| --- | --- | --- |
| 1. | Czy ograniczają Państwo uprawnienia pracowników i użytkowników zewnętrznych na zasadzie business need to know (w szczególności uprawnienia administracyjne i dostęp do danych wrażliwych, np. danych osobowych)?Do you restrict employees' and external users' privileges on a business-need to know basis (particularly administrative permissions and access to sensitive data e.g. personal data)? | [ ]  Tak Yes[ ]  Nie No |
| 2. | Czy wprowadzono uwierzytelnianie wieloczynnikowe dla dostępu zdalnego?Have you enforced multi-factor authentication for remote access? | [ ]  Tak Yes[ ]  Nie No [ ]  Nie dotyczy Not applicable |
| 3. | Czy wdrożono proces nadawania i odbierania praw dostępu?Do you have a formal access provisioning process in place for assigning and revoking access rights? | [ ]  Tak Yes[ ]  Nie No |
| 4. | Czy zakazują Państwo użytkownikom uprawnień lokalnego administratora na stacjach roboczych?Do you prohibit local admin rights on workstations for users? | [ ]  Tak Yes[ ]  Nie No |
| 5. | Czy co najmniej raz w roku dokonują Państwo przeglądu praw dostępu użytkowników?Do you review user access rights at least annually? | [ ]  Tak Yes[ ]  Nie No |
| 6. | Czy po zakończeniu pracy użytkowników (w tym pracowników, pracowników tymczasowych, wykonawców lub sprzedawców) odbierane są wszystkie dostępy do systemu, konta i związane z nimi uprawnienia?Do you revoke all system access, accounts and associated rights after termination of users (incl. employees, temporary employees, contractors or vendors)?  | [ ]  Tak Yes[ ]  Nie No |
| 7. | Czy wdrożono politykę haseł wymuszającą stosowanie długich i złożonych haseł w całej organizacji? Długie i złożone hasła są definiowane jako: ośmioznakowe lub dłuższe; nieskładające się z wyrazów zawartych w słownikach; wolne od następujących po sobie identycznych, całkowicie numerycznych lub całkowicie alfabetycznych znaków.Have you implemented a password policy enforcing the use of long and complex passwords across your organisation? Long and complex passwords are defined as: eight characters or more; not consisting of words included in dictionaries; free of consecutive identical, all-numeric or all-alphabetic characters. | [ ]  Tak Yes[ ]  Nie No |
| 8. | Czy zmieniono wszystkie domyślne hasła na wszystkich podłączonych urządzeniach (np. router, Internet of Things)?Have you changed all default passwords on all your connected devices (e.g. router, Internet of Things)?  | [ ]  Tak Yes[ ]  Nie No |

## SZYFROWANIE CRYPTOGRAPHY

**Cel:** Zapewnienie właściwego i skutecznego wykorzystania techniki kryptograficznej do ochrony poufności, autentyczności i/lub integralności informacji.
**Objective:** To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.

|  |  |  |
| --- | --- | --- |
| 1. | Czy wszystkie poufne informacje przechowywane na urządzeniach mobilnych (np. smartfonach i laptopach) są zaszyfrowane?Is all confidential information stored on mobile devices (e.g. smart phones and laptops) encrypted? | [ ]  Tak Yes[ ]  Nie No |
| 2. | Czy szyfrują Państwo dane wrażliwe i informacje poufne przy ich przesyłaniu?Do you encrypt sensitive data and confidential information in transit? | [ ]  Tak Yes[ ]  Nie No |
| 3. | Czy opracowano i wdrożono politykę dotyczącą wykorzystania, ochrony i czasu życia kluczy kryptograficznych?Have you developed and implemented a policy on the use, protection and lifetime of cryptographic keys? | [ ]  Tak Yes[ ]  Nie No |

## BEZPIECZEŃSTWO FIZYCZNE I OCHRONA PHYSICAL AND ENVIRONMENTAL SECURITY

**Cel:** Zapobieganie nieautoryzowanemu fizycznemu dostępowi, uszkodzeniu i ingerencji
w informacje organizacji i urządzenia do przetwarzania informacji. Zapobieganie utracie, uszkodzeniu, kradzieży lub ujawnieniu aktywów oraz przerwaniu działalności organizacji.

**Objective:** To prevent unauthorized physical access, damage and interference to the organization’s information and information processing facilities. To prevent loss, damage, theft
or compromise of assets and interruption to the organization’s operations.

|  |  |  |
| --- | --- | --- |
| 1. | Czy prowadzą Państwo listę personelu (pracowników, dostawców i gości) upoważnionych do dostępu do Państwa obiektów i wrażliwych stref bezpieczeństwa?Do you maintain a list of personnel (employees, vendors and visitors) with authorized access to your premises and sensitive security areas? | [ ]  Tak Yes[ ]  Nie No |

## BEZPIECZEŃSTWO OPERACJI OPERATIONS SECURITY

**Cel:** Zapewnienie prawidłowego i bezpiecznego działania obiektów przetwarzania informacji. Zapewnienie ochrony informacji i obiektów przetwarzania informacji przed złośliwym oprogramowaniem. Zapewnienie ochrony przed utratą danych. Rejestrowanie zdarzeń
i generowanie dowodów. Zapewnienie integralności systemów operacyjnych. Zapobieganie wykorzystywaniu podatności technicznych. Minimalizowanie wpływu działań audytowych na systemy operacyjne.

**Objective:** To ensure correct and secure operations of information processing facilities. To ensure that information and information processing facilities are protected against malware. To protect against loss of data. To record events and generate evidence. To ensure the integrity of operational systems. To prevent exploitation of technical vulnerabilities. To minimize the impact of audit activities on operational systems.

|  |  |  |
| --- | --- | --- |
| 1. | Czy wdrożono procedury zarządzania zmianami w systemach krytycznych?Have you implemented change management procedures for critical systems? | [ ]  Tak Yes[ ]  Nie No |
| 2. | Czy środowisko IT dla rozwoju i testów jest oddzielone od środowiska IT dla produkcji?Is the IT-environment for development and testing separated from production IT-environment?  | [ ]  Tak Yes[ ]  Nie No [ ]  Nie dotyczy Not applicable |
| 3. | Czy używają Państwo ochrony przed złośliwym oprogramowaniem dla wszystkich serwerów internetowych, bramek poczty elektronicznej, stacji roboczych i laptopów?Do you use malware protection for all web-proxies, email-gateways, workstations and laptops? | [ ]  Tak Yes[ ]  Nie No |
| 4. | Czy wykonywane są codziennie kopie zapasowe krytycznych danych biznesowych?Do you perform daily backups of business critical data? | [ ]  Tak Yes[ ]  Nie No |
| 5. | Czy przechowują Państwo kopie zapasowe fizycznie oddzielone od sieci (np. poza pomieszczeniami biurowymi)?Do you store backups physically separated from your network (e.g. outside the office premises)? | [ ]  Tak Yes[ ]  Nie No |
| 6. | Czy przechowują Państwo kopie zapasowe poza środowiskiem źródłowym?Do you store backups separate from the source environment? | [ ]  Tak Yes[ ]  Nie No |
| 7. | Czy regularnie upewniają się Państwo, że kopie zapasowe danych są kompletne i mogą być przywrócone tak szybko, jak to możliwe przy minimalnym wpływie na działalność?Do you regularly ensure that data backups are complete and can be restored as quickly as possible with minimal impact to business? | [ ]  Tak Yes[ ]  Nie No |
| 8. | Czy tworzą Państwo i regularnie przeglądają dzienniki zdarzeń rejestrujące działania użytkowników, wyjątki, usterki i zdarzenia związane z bezpieczeństwem informacji (przynajmniej z Państwa firewalli i kontrolera domeny)?Do you produce and regularly review event logs recording user activities, exceptions, faults and information security events (at least from your firewalls and domain controller)? | [ ]  Tak Yes[ ]  Nie No |
| 9. | Czy wdrożono scentralizowany proces instalacji oprogramowania?Have you implemented a centralized software installation process? | [ ]  Tak Yes[ ]  Nie No |
| 10. | Czy regularnie – co najmniej w ciągu miesiąca od wydania – wprowadzają Państwo aktualizacje do krytycznych systemów i aplikacji IT (“security patching”)?Do you timely – at least within one month of release – apply updates to critical IT-systems and applications (“security patching”)? | [ ]  Tak Yes[ ]  Nie No |
| 11. | Czy technicznie lub organizacyjnie uniemożliwiają Państwo użytkownikom samodzielne instalowanie oprogramowania na swoich stacjach roboczych?Do you technically or organisationally ensure that users must not install software on their workstations by themselves? | [ ]  Tak Yes[ ]  Nie No |

## BEZPIECZEŃSTWO KOMUNIKACJI COMMUNICATIONS SECURITY

**Cel:** Zapewnienie ochrony informacji w sieciach i wspierających je urządzeniach do przetwarzania informacji. Utrzymanie bezpieczeństwa informacji przekazywanych wewnątrz organizacji
i z każdym podmiotem zewnętrznym.

**Objective:** To ensure the protection of information in networks and its supporting information processing facilities. To maintain the security of information transferred within an organization and with any external entity.

|  |  |  |
| --- | --- | --- |
| 1. | Czy wszystkie punkty dostępu do Internetu są zabezpieczone przez odpowiednio skonfigurowane zapory sieciowe?Are all internet access points secured by appropriately configured firewalls? | [ ]  Tak Yes[ ]  Nie No |
| 2. | Czy wprowadzili Państwo kontrolę dostępu do korporacyjnych sieci bezprzewodowych?Have you implemented controlled access to corporate wireless networks? | [ ]  Tak Yes[ ]  Nie No |
| 3. | Czy monitorują Państwo swoją sieć i identyfikują Państwo zdarzenia związane z bezpieczeństwem?Do you monitor your network and identify security events? | [ ]  Tak Yes[ ]  Nie No |
| 4. | Czy wszystkie systemy dostępne z Internetu (np. serwery WWW i poczty elektronicznej) są odseparowane od zaufanej sieci (np. w strefie zdemilitaryzowanej (DMZ) lub u innego dostawcy)?Are all internet-accessible systems (e.g. web-, email-servers) segregated from your trusted network (e.g. within a demilitarized zone (DMZ) or at a 3rd party provider)?  | [ ]  Tak Yes[ ]  Nie No[ ]  Nie dotyczy Not applicable |
| 5. | Czy wszystkie segmenty sieci o wysokim ryzyku (np. systemy punktów sprzedaży (PoS), przetwarzanie wrażliwych danych, sieci biurowe i produkcyjne technologii operacyjnej (OT) itp.) są odseparowane od reszty sieci?Are all high risk network segments (e.g. point of sales (PoS) systems, sensitive data processing, office and operational technology (OT) production networks etc.) segregated? | [ ]  Tak Yes[ ]  Nie No[ ]  Nie dotyczy Not applicable |

## RELACJE Z DOSTAWCAMI SUPPLIER RELATIONSHIPS

**Cel:** Zapewnienie ochrony aktywów organizacji, które są dostępne dla dostawców. Utrzymanie uzgodnionego poziomu bezpieczeństwa informacji i świadczenia usług zgodnie z umowami
z dostawcami.

**Objective:** To ensure protection of the organization’s assets that is accessible by suppliers. To maintain an agreed level of information security and service delivery in line with supplier agreements.

|  |  |  |
| --- | --- | --- |
| 1. | Czy zidentyfikowano i udokumentowano wszystkich ważnych dostawców (w tym usługodawców zewnętrznych)?Have you identified and documented all your important suppliers (including third party service providers)? | [ ]  Tak Yes[ ]  Nie No |
| 2. | Czy umowy z zewnętrznymi dostawcami usług wymagają poziomów bezpieczeństwa współmiernych do własnych standardów bezpieczeństwa informacji?Do agreements with third party service providers require levels of security commensurate with your own information security standard? | [ ]  Tak Yes[ ]  Nie No |
| 3. | Czy monitorują Państwo działania zewnętrznych dostawców usług pod kątem zdarzeń bezpieczeństwa w celu utrzymania uzgodnionego poziomu bezpieczeństwa informacji?Do you monitor third party service provider activities for security events to maintain an agreed level of information security? | [ ]  Tak Yes[ ]  Nie No |
| 4. | Prosimy o uzupełnienie poniższej tabeli.Please complete the table below. |  |
| Nazwa dostawcy Supplier name | Jakie usługi lub systemy dostarcza? What services or systems does the supplier provide? | Do jakich usług lub systemów ma dostęp?To what services or systems does he have access to? |
| Click or tap here to enter text. | Click or tap here to enter text. | Click or tap here to enter text. |

## ZARZĄDZANIE INCYDENTAMI ZWIĄZANYMI Z BEZPIECZEŃSTWEM INFORMACJI INFORMATION SECURITY INCIDENT MANAGEMENT

**Cel:** Zapewnienie spójnego i skutecznego podejścia do zarządzania incydentami związanymi
z bezpieczeństwem informacji, w tym informowania o zdarzeniach i słabościach w zakresie bezpieczeństwa.

**Objective:** To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

|  |  |  |
| --- | --- | --- |
| 1. | Czy mają Państwo wdrożony plan reagowania na incydenty związane z bezpieczeństwem informacji?Do you have an information security incident response plan in place? | [ ]  Tak Yes[ ]  Nie No |
| 2. | Czy co roku testują Państwo swój plan reagowania na incydenty bezpieczeństwa?Do you annually test your security incident response plan? | [ ]  Tak Yes[ ]  Nie No |
| 3. | Czy wszyscy pracownicy i dostawcy zewnętrzni znają linię raportowania zdarzeń związanych z bezpieczeństwem informacji?Do all your employees and third party providers know the reporting line for information security events? | [ ]  Tak Yes[ ]  Nie No |
| 4. | Czy pracownicy i wykonawcy są zobowiązani do zgłaszania wszelkich zidentyfikowanych słabości bezpieczeństwa informacji (jeszcze nie incydentów lub zdarzeń) w systemach lub usługach?Are employees and contractors required to report any identified information security weakness (not yet an incident or event) in systems or services? | [ ]  Tak Yes[ ]  Nie No |
| 5. | Czy ustanowiono procedurę eskalacji dla incydentów bezpieczeństwa informacji?Have you established an escalation procedure for information security incidents?  | [ ]  Tak Yes[ ]  Nie No |

## BEZPIECZEŃSTWO INFORMACJI W ZARZĄDZANIU CIĄGŁOŚCIĄ DZIAŁANIA INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT

**Cel:** Ciągłość bezpieczeństwa informacji powinna być osadzona w systemach zarządzania ciągłością działania organizacji. Zapewnienie dostępności urządzeń do przetwarzania informacji.

**Objective:** Information security continuity should be embedded in the organization’s business continuity management systems. To ensure availability of information processing facilities.

|  |  |  |
| --- | --- | --- |
| 1. | Czy przeprowadzono analizę wpływu na biznes (BIA)?Have you conducted a Business Impact Analysis (BIA)? | [ ]  Tak Yes[ ]  Nie No |
| 2. | Czy mają Państwo wdrożony plan zarządzania ciągłością działania (BCM), który dotyczy w szczególności incydentów cybernetycznych?Do you have a Business Continuity Management (BCM) plan in place that specifically addresses cyber incidents? | [ ]  Tak Yes[ ]  Nie No |
| 3. | Czy mają Państwo wdrożony plan odzyskiwania danych po awarii IT (DR)?Do you have an IT Disaster Recovery Plan (DRP) in place? | [ ]  Tak Yes[ ]  Nie No |
| 4. | Czy przynajmniej raz w roku testują Państwo swoje plany zarządzania ciągłością działania (np. Business Continuity Management, Disaster Recovery)?Do you test your information security continuity plans (e.g. Business Continuity Management, Disaster Recovery) at least annually? | [ ]  Tak Yes[ ]  Nie No |
| 5. | Czy urządzenia do przetwarzania informacji (tj. każdy system, usługa lub infrastruktura, lub fizyczna lokalizacja, w której się znajdują) są wdrożone z zachowaniem zasad redundancji?Are your information processing facilities (i.e. any system, service or infrastructure, or physical location housing it) implemented with redundancy? | [ ]  Tak Yes[ ]  Nie No |

## ZGODNOŚĆ COMPLIANCE

**Cel:** Unikanie naruszeń zobowiązań prawnych, ustawowych, wykonawczych lub umownych związanych z bezpieczeństwem informacji oraz wszelkich wymogów bezpieczeństwa. Zapewnienie, że bezpieczeństwo informacji jest wdrażane i obsługiwane zgodnie z polityką
i procedurami organizacyjnymi.

**Objective:** To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements. To ensure that information security is implemented and operated in accordance with the organizational policies and procedures.

|  |  |  |
| --- | --- | --- |
| 1. | Czy posiadają Państwo wytyczne wydane w sprawie przechowywania, magazynowania, obsługi i usuwania zapisów i informacji?Do you have guideline issued on the retention, storage, handling and disposal of records and information? | [ ]  Tak Yes[ ]  Nie No |
| 2. | Czy wyznaczono osobę odpowiedzialną za wdrożenie i kontrolę przestrzegania zasad postępowania z informacjami i danymi (np. inspektor ochrony danych IOD)?Have you assigned a responsible person for providing guidance and ensuring awareness of privacy principles (e.g. Data Privacy Officer DPO)? | [ ]  Tak Yes[ ]  Nie No |
| 3. | Czy regularnie skanują Państwo krytyczne systemy (w tym przeprowadzają testy penetracyjne lub oceny podatności) – samodzielnie lub przy wsparciu strony trzeciej – w szczególności za każdym razem, gdy wprowadzane są nowe systemy i po zmianach?Do you regularly scan critical systems (incl. penetration tests or vulnerability assessments) – either by yourself or supported by third party – particularly each time new systems are introduced and following changes?  | [ ]  Tak Yes[ ]  Nie No |
|  | Jeśli tak, to jak często?If yes, how often? | Click or tap here to enter text. |

1. DODATKOWE UWAGI I PODPISY
ADDITIONAL COMMENTS AND SIGNATURE(S)

Czy chcieliby Państwo podzielić się dalszymi informacjami lub szczegółami dotyczącymi bezpieczeństwa informacji?
Would you like to share further information or details regarding your information security?

Click or tap here to enter text.

Poprzez złożenie podpisu pod tym dokumentem, potwierdzam, że jestem odpowiednio upoważnionym przedstawicielem spółki posiadającym wystarczające umiejętności techniczne, aby udzielić w imieniu spółki – zgodnie z moją najlepszą wiedzą – dokładnych i wyczerpujących odpowiedzi na pytania zawarte w tym kwestionariuszu. Wypełniony kwestionariusz i załączniki stanowią podstawę do objęcia ochroną ubezpieczeniową i w związku z tym staną się częścią umowy ubezpieczenia, o ile zostanie zawarta.
Herewith, by undersigning this document (must be signed by officer, owner or manager), I confirm that I am a duly authorized representative of the company with sufficient technical skills to provide – to my best knowledge – accurate and comprehensive answers regarding the questions within this questionnaire on behalf of the company. The completed questionnaire and optional attachments are basis for the coverage and will therefore become part of the insurance contract.

|  |  |  |  |
| --- | --- | --- | --- |
| Data Date | Click or tap to enter a date. | Data Date | Click or tap to enter a date. |
| Podpis Signature |  | Podpis Signature |  |
| Imię i nazwisko Name and surname | Click or tap here to enter text. | Imię i nazwisko Name and surname | Click or tap here to enter text. |
| Stanowisko Position, task | Click or tap here to enter text. | Stanowisko Position, task | Click or tap here to enter text. |
| Email Email | Click or tap here to enter text. | Email Email | Click or tap here to enter text. |