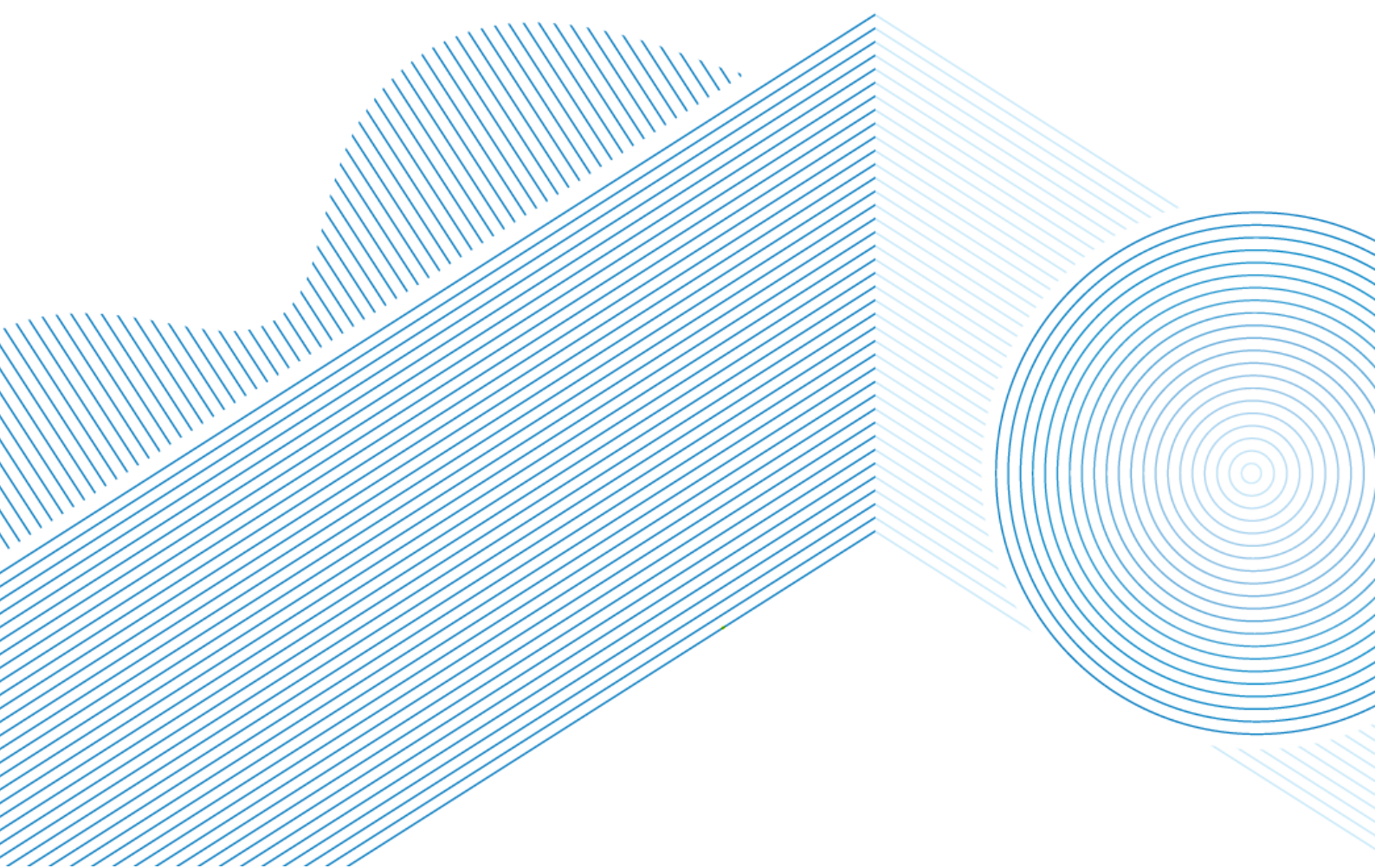


**Klauzula Bezpieczeństwa Informacji  
dla Partnerów Biznesowych  
HOCHTIEF Polska S.A.**



**Budujemy świat jutra.**

## 1. Wstęp

Bezpieczeństwo informacji jest jednym z istotnych elementów odpowiedzialnego i profesjonalnego prowadzenia działalności przez HOCHTIEF Polska S.A.

W ramach współpracy biznesowej zarówno HOCHTIEF Polska S.A., jak i jej Partnerzy Biznesowi mogą uzyskiwać dostęp do informacji, danych, dokumentów, systemów, zasobów technicznych lub organizacyjnych drugiej strony. Informacje te mogą mieć znaczenie biznesowe, techniczne, prawne, finansowe, organizacyjne, kontraktowe lub wizerunkowe.

Dlatego oczekujemy, że każda organizacja współpracująca z HOCHTIEF Polska S.A. będzie traktować bezpieczeństwo powierzonych jej informacji z należytą starannością, odpowiedzialnością i profesjonalizmem.

HOCHTIEF Polska S.A. stosuje zasady zarządzania bezpieczeństwem informacji zgodne z wymaganiami normy ISO/IEC 27001, w szczególności w zakresie ochrony informacji, zarządzania dostępem, nadzoru nad relacjami z dostawcami, reagowania na incydenty oraz ciągłego doskonalenia bezpieczeństwa informacji.

Wymagania wobec dostawców i partnerów biznesowych są częścią naszego systemowego podejścia do bezpieczeństwa informacji. Obejmują w szczególności zasady współpracy z dostawcami, wymagania bezpieczeństwa w umowach, ochronę łańcucha dostaw ICT, monitorowanie usług świadczonych przez dostawców oraz korzystanie z usług chmurowych.

Dokument należy czytać jako podstawowy zestaw zasad bezpieczeństwa informacji obowiązujących w toku współpracy z HOCHTIEF Polska S.A. W praktyce oznacza to, że Partner Biznesowy powinien chronić otrzymane informacje, udostępniać je wyłącznie osobom uprawnionym, korzystać z nich tylko w celu realizacji współpracy oraz niezwłocznie zgłaszać każdy incydent lub podejrzenie naruszenia bezpieczeństwa informacji.

---

## 2. Cel dokumentu

Celem niniejszej Klauzuli jest:

- wskazanie podstawowych zasad ochrony informacji przekazywanych Partnerom Biznesowym,
- określenie minimalnych oczekiwań HOCHTIEF Polska S.A. w zakresie bezpieczeństwa informacji,
- zapewnienie, że informacje HOCHTIEF Polska S.A. oraz informacje Partnerów Biznesowych są chronione w sposób adekwatny do ich znaczenia i poziomu ryzyka,
- wskazanie zasad klasyfikacji informacji i dokumentacji przekazywanej Partnerom Biznesowym,
- uregulowanie zasad zgłaszania incydentów bezpieczeństwa informacji,

- określenie prawa HOCHTIEF Polska S.A. do weryfikacji poziomu bezpieczeństwa u Partnerów Biznesowych, w szczególności w przypadku dostępu do systemów, sieci, danych, dokumentacji lub zasobów HOCHTIEF Polska S.A.

---

### 3. Zakres stosowania

Niniejsza Klauzula ma zastosowanie do wszystkich Partnerów Biznesowych, którzy w ramach współpracy z HOCHTIEF Polska S.A.:

- otrzymują, przetwarzają, przechowują lub przekazują informacje HOCHTIEF Polska S.A.,
- uzyskują dostęp do systemów informatycznych, sieci, aplikacji, środowisk chmurowych, zasobów technicznych lub dokumentacji HOCHTIEF Polska S.A.,
- realizują usługi, które mogą mieć wpływ na poufność, integralność lub dostępność informacji HOCHTIEF Polska S.A.,
- działają w imieniu HOCHTIEF Polska S.A. lub na jej rzecz,
- korzystają z własnych pracowników, współpracowników, przedstawicieli lub podwykonawców przy realizacji współpracy z HOCHTIEF Polska S.A.

Klauzula ma zastosowanie niezależnie od formy informacji, w szczególności do informacji w postaci elektronicznej, papierowej, ustnej, wizualnej oraz utrwalonej na nośnikach danych.

---

### 4. Definicje

Na potrzeby niniejszej Klauzuli przyjmuje się następujące znaczenie podstawowych pojęć:

**Bezpieczeństwo informacji** - Ochrona informacji przed nieuprawnionym dostępem, ujawnieniem, zmianą, zniszczeniem, utratą lub niedostępnością.

**Informacja** - Każda treść, dane, dokument, wiadomość, plik, rysunek, model, zestawienie, raport, korespondencja lub inny materiał związany z HOCHTIEF Polska S.A., Partnerem Biznesowym, klientem, projektem lub prowadzoną działalnością.

**Dokumentacja** - Informacje utrwalone w dowolnej formie, w szczególności jako dokumenty papierowe, pliki elektroniczne, wiadomości e-mail, zapisy systemowe, modele, rysunki, raporty, zestawienia, protokoły, oferty, umowy, notatki lub inne materiały związane ze współpracą.

**Informacja poufna** - Informacja, która nie jest publicznie dostępna i której ujawnienie osobom nieuprawnionym mogłoby narazić HOCHTIEF Polska S.A., Partnera Biznesowego, klienta lub inne osoby na szkodę, stratę, naruszenie prawa, utratę przewagi konkurencyjnej lub ryzyko wizerunkowe.

**Poufność** - Zasada, zgodnie z którą dostęp do informacji mają wyłącznie osoby uprawnione.

**Integralność** - Zasada, zgodnie z którą informacja powinna być kompletna, poprawna i niezmieniona w sposób nieuprawniony.

**Dostępność** - Zasada, zgodnie z którą informacja, system lub usługa powinny być dostępne wtedy, gdy są potrzebne do realizacji uzgodnionych zadań.

**Incydent bezpieczeństwa informacji** - Każde zdarzenie, które narusza lub może naruszyć bezpieczeństwo informacji, w szczególności: nieuprawniony dostęp, utrata danych, wysłanie informacji do niewłaściwego odbiorcy, podejrzenie wycieku danych, utrata nośnika danych, zainfekowanie systemu złośliwym oprogramowaniem, przejęcie konta użytkownika lub naruszenie zasad dostępu do systemów HOCHTIEF Polska S.A.

**Zasoby HOCHTIEF Polska S.A.** - Systemy informatyczne, konta użytkowników, aplikacje, urządzenia, dokumentacja, dane, sieci, środowiska chmurowe, repozytoria plików, poczta elektroniczna, platformy współpracy oraz inne środki wykorzystywane w działalności HOCHTIEF Polska S.A.

**Partner Biznesowy** - Każdy dostawca, podwykonawca, usługodawca, konsultant, doradca, wykonawca lub inny podmiot współpracujący z HOCHTIEF Polska S.A., który uzyskuje dostęp do informacji, danych, systemów lub zasobów HOCHTIEF Polska S.A.

---

## 5. Klasyfikacja informacji i dokumentacji

HOCHTIEF Polska S.A. stosuje model klasyfikacji informacji, którego celem jest określenie, jak należy chronić informacje i dokumentację w zależności od ich znaczenia, poufności oraz potencjalnych skutków ich nieuprawnionego ujawnienia, zmiany, utraty lub niedostępności.

Partner Biznesowy zobowiązuje się traktować informacje oraz dokumentację HOCHTIEF Polska S.A. zgodnie z oznaczoną lub przekazaną klasyfikacją oraz stosować zasady ochrony adekwatne do danej klasy informacji.

W modelu klasyfikacji HOCHTIEF Polska S.A. wyróżnia się następujące poziomy informacji:

- **Informacje Ogólnodostępne** - Informacje zatwierdzone do udostępnienia publicznego, takie jak opublikowane materiały PR, dane teleadresowe lub komunikaty publiczne. Ich publikacja powinna następować wyłącznie po zatwierdzeniu przez właściciela treści.
- **Informacje Wewnętrzne** - Informacje służbowe przeznaczone do użytku wewnętrznego lub dla uprawnionych partnerów, takie jak procedury, notatki, robocza korespondencja lub standardowe dokumenty projektowe. Dostęp do nich powinien być ograniczony do uprawnionych użytkowników, a ich przechowywanie powinno odbywać się w zatwierdzonych repozytoriach.
- **Informacje Zastrzeżone** - Informacje, których ujawnienie może spowodować szkodę biznesową, prawną, finansową, kontraktową, organizacyjną lub reputacyjną. Mogą to być w szczególności oferty, kalkulacje, informacje kontraktowe, negocjacje, ryzyka, dokumenty sporne lub wybrane dane projektowe. Wymagają ograniczonej dystrybucji, kontroli dostępu, oznaczenia oraz zastosowania środków ochrony adekwatnych do nośnika i sposobu przekazania.
- **Informacje Krytyczne** - Informacje o wysokim wpływie, których ujawnienie może spowodować istotną szkodę, sankcje, roszczenia, utratę przewagi konkurencyjnej lub

naruszenie praw osób. Mogą to być w szczególności dane logowania, informacje płacowe, szczególne dane osobowe, strategie, kluczowe spory lub materiały objęte najwyższą poufnością. Dostęp do takich informacji powinien być imienny, kontrolowany i ograniczony do niezbędnego minimum, a ich przekazywanie powinno odbywać się wyłącznie zatwierdzonymi i odpowiednio zabezpieczonymi kanałami.

Jeżeli Partner Biznesowy otrzyma informację lub dokumentację HOCHTIEF Polska S.A., której klasyfikacja nie została jednoznacznie wskazana, powinien traktować ją co najmniej jako **Informację Zastrzeżoną**. Oznacza to w szczególności ograniczenie dostępu do osób uprawnionych, ostrożne przekazywanie informacji oraz stosowanie bezpiecznych miejsc przechowywania, chyba że HOCHTIEF Polska S.A. wskaże inaczej.

Udostępnienie Partnerowi Biznesowemu informacji sklasyfikowanych jako **Informacje Zastrzeżone** lub **Informacje Krytyczne** może wiązać się z dodatkowymi wymaganiami bezpieczeństwa określonymi przez HOCHTIEF Polska S.A., w szczególności dotyczącymi sposobu przekazania, przechowywania, ograniczenia dostępu, szyfrowania, zwrotu, usunięcia lub potwierdzenia zniszczenia informacji.

Powyższy model klasyfikacji, wraz z przykładami i minimalnymi zasadami ochrony, stanowi podstawę postępowania z informacjami HOCHTIEF Polska S.A. przekazywanymi Partnerom Biznesowym. Informacje niejawne w rozumieniu przepisów o ochronie informacji niejawnych, w tym informacje przetwarzane w Kancelarii Tajnej, podlegają odrębnym zasadom wynikającym z przepisów prawa i nie są objęte niniejszą Klauzulą.

---

## 6. Zasady ogólne

HOCHTIEF Polska S.A. traktuje bezpieczeństwo informacji jako jeden z priorytetów organizacyjnych i oczekuje takiego samego podejścia od swoich Partnerów Biznesowych.

Partner Biznesowy zobowiązuje się do:

- ochrony informacji powierzonych mu przez HOCHTIEF Polska S.A.,
- wykorzystywania informacji wyłącznie w celu realizacji uzgodnionej współpracy,
- zapewnienia, że dostęp do informacji mają wyłącznie osoby, którym taki dostęp jest niezbędny do wykonania powierzonych zadań,
- stosowania adekwatnych środków organizacyjnych, technicznych i prawnych chroniących informacje,
- nieujawniania informacji osobom trzecim bez uprzedniej zgody HOCHTIEF Polska S.A., chyba że obowiązek taki wynika z przepisów prawa,
- zapewnienia, że osoby działające po stronie Partnera Biznesowego zostały poinformowane o obowiązku ochrony informacji,
- niezwłocznego informowania HOCHTIEF Polska S.A. o incydentach lub podejrzaniach incydentów bezpieczeństwa informacji.

W praktyce oznacza to, że Partner Biznesowy powinien chronić informacje HOCHTIEF Polska S.A. przed dostępem osób nieuprawnionych oraz nie przekazywać ich dalej bez podstawy wynikającej z umowy, uzgodnień z HOCHTIEF Polska S.A. albo przepisów prawa.

---

## **7. Minimalne wymagania wobec Partnera Biznesowego**

Partner Biznesowy powinien zapewnić co najmniej wymagania określone w poniższych punktach.

### **7.1. Ograniczenie dostępu do informacji**

Partner Biznesowy zobowiązuje się udostępniać informacje HOCHTIEF Polska S.A. wyłącznie osobom, które potrzebują ich do realizacji powierzonych zadań.

Dostęp do informacji powinien być nadawany zgodnie z zasadą minimalnych uprawnień, czyli tylko w takim zakresie, jaki jest niezbędny do wykonania pracy.

Partner Biznesowy powinien ograniczyć dostęp do informacji także we własnej organizacji, w szczególności wobec osób, które nie uczestniczą bezpośrednio w realizacji współpracy z HOCHTIEF Polska S.A.

### **7.2. Ochrona dokumentów, plików i nośników**

Partner Biznesowy zobowiązuje się chronić dokumenty, pliki, wiadomości, wydruki, kopie, nośniki danych oraz inne materiały zawierające informacje HOCHTIEF Polska S.A. przed utratą, kradzieżą, zniszczeniem, nieuprawnionym kopiowaniem, zmianą lub ujawnieniem.

Dokumenty i nośniki zawierające **Informacje Zastrzeżone** lub **Informacje Krytyczne** powinny być przechowywane w sposób ograniczający dostęp osób nieuprawnionych. W przypadku innych informacji zakres ochrony powinien odpowiadać ich klasyfikacji oraz ustaleniom z HOCHTIEF Polska S.A.

W przypadku utraty dokumentu, pliku, urządzenia lub nośnika zawierającego informacje HOCHTIEF Polska S.A., Partner Biznesowy zobowiązany jest niezwłocznie zgłosić ten fakt zgodnie z zasadami określonymi w rozdziale dotyczącym incydentów bezpieczeństwa informacji.

### **7.3. Bezpieczne przekazywanie informacji**

Partner Biznesowy zobowiązuje się przekazywać informacje HOCHTIEF Polska S.A. w sposób bezpieczny i adekwatny do ich charakteru oraz klasyfikacji.

Informacje **Zastrzeżone** lub **Krytyczne** nie powinny być przesyłane przez nieautoryzowane kanały komunikacji, prywatne skrzynki pocztowe, publiczne komunikatory lub niezabezpieczone repozytoria plików, chyba że zostało to uprzednio uzgodnione z HOCHTIEF Polska S.A.

W przypadku informacji sklasyfikowanych jako **Informacje Zastrzeżone** lub **Informacje Krytyczne** Partner Biznesowy zobowiązuje się stosować kanały przekazania i środki ochrony uzgodnione z HOCHTIEF Polska S.A. albo wynikające z przekazanej klasyfikacji informacji.

### **7.4. Ochrona kont użytkowników i haseł**

Jeżeli Partner Biznesowy otrzymuje dostęp do systemów, aplikacji, sieci lub zasobów HOCHTIEF Polska S.A., zobowiązuje się do ochrony przydzielonych kont, haseł, tokenów, certyfikatów oraz innych środków uwierzytelnienia.

Zabronione jest:

- udostępnianie kont innym osobom,
- korzystanie ze wspólnych kont bez zgody HOCHTIEF Polska S.A.,
- zapisywanie haseł w miejscach dostępnych dla osób nieuprawnionych,
- obchodzenie mechanizmów bezpieczeństwa,
- wykorzystywanie dostępu w celu innym niż realizacja uzgodnionych zadań.

Partner Biznesowy zobowiązuje się niezwłocznie poinformować HOCHTIEF Polska S.A. o utracie kontroli nad kontem, hasłem, tokenem, certyfikatem, urządzeniem lub innym środkiem dostępu do zasobów HOCHTIEF Polska S.A.

#### **7.5. Korzystanie z własnych podwykonawców**

Partner Biznesowy może powierzyć realizację części zadań podwykonawcom wyłącznie wtedy, gdy jest to zgodne z umową oraz ustaleniami z HOCHTIEF Polska S.A.

Partner Biznesowy odpowiada za działania swoich podwykonawców w zakresie ochrony informacji HOCHTIEF Polska S.A. i zobowiązuje się zapewnić, że podwykonawcy stosują wymagania bezpieczeństwa nie niższe niż określone w niniejszej Klauzuli.

Partner Biznesowy powinien zapewnić, że podwykonawcy mają dostęp wyłącznie do tych informacji, które są niezbędne do wykonania powierzonych im zadań.

#### **7.6. Ochrona przed nieuprawnionym ujawnieniem**

Partner Biznesowy zobowiązuje się nie ujawniać, nie publikować, nie udostępniać, nie kopiować ani nie wykorzystywać informacji HOCHTIEF Polska S.A. w celu innym niż realizacja uzgodnionej współpracy.

Dotyczy to również informacji uzyskanych przypadkowo lub omyłkowo.

Jeżeli Partner Biznesowy otrzyma informację HOCHTIEF Polska S.A., która nie była przeznaczona dla niego lub dla osób działających po jego stronie, powinien niezwłocznie poinformować o tym HOCHTIEF Polska S.A. i powstrzymać się od dalszego wykorzystywania tej informacji.

#### **7.7. Usunięcie lub zwrot informacji po zakończeniu współpracy**

Po zakończeniu współpracy lub po ustaniu potrzeby przetwarzania informacji Partner Biznesowy zobowiązuje się, zgodnie z ustaleniami z HOCHTIEF Polska S.A., zwrócić, usunąć lub trwale zniszczyć informacje HOCHTIEF Polska S.A. oraz ich kopie, chyba że obowiązek dalszego przechowywania wynika z przepisów prawa lub odrębnych uzgodnień.

Na żądanie HOCHTIEF Polska S.A. Partner Biznesowy powinien potwierdzić wykonanie powyższych czynności.

---

## 8. Dostęp do systemów i zasobów HOCHTIEF Polska S.A.

W przypadku, gdy Partner Biznesowy uzyskuje dostęp do systemów, sieci, aplikacji, danych, dokumentacji lub innych zasobów HOCHTIEF Polska S.A., zobowiązuje się do przestrzegania zasad bezpieczeństwa określonych przez HOCHTIEF Polska S.A.

W szczególności Partner Biznesowy zobowiązuje się do:

- korzystania z dostępu wyłącznie w celu realizacji zadań wynikających z umowy lub uzgodnionej współpracy,
- niepodjęcia działań mogących zakłócić działanie systemów HOCHTIEF Polska S.A.,
- nieinstalowania nieautoryzowanego oprogramowania,
- niekopiowania danych poza uzgodniony zakres,
- nieudostępniania dostępu innym osobom,
- niezwłocznego informowania o utracie kontroli nad kontem, hasłem, urządzeniem lub nośnikiem danych,
- stosowania dodatkowych wymagań bezpieczeństwa przekazanych przez HOCHTIEF Polska S.A., jeśli są wymagane dla danego zakresu współpracy.

HOCHTIEF Polska S.A. może ograniczyć, zawiesić lub odebrać dostęp Partnera Biznesowego do swoich systemów, danych lub zasobów w przypadku stwierdzenia naruszenia zasad bezpieczeństwa, ryzyka naruszenia bezpieczeństwa lub zakończenia podstawy biznesowej do utrzymywania dostępu.

---

## 9. Prawo audytu i weryfikacji bezpieczeństwa

HOCHTIEF Polska S.A. zastrzega sobie prawo do przeprowadzenia audytu lub innej formy weryfikacji bezpieczeństwa informacji u Partnera Biznesowego, jeżeli zakres współpracy, rodzaj przetwarzanych informacji, dostęp do zasobów HOCHTIEF Polska S.A., znaczenie świadczonych usług albo wystąpienie incydentu uzasadnia taką weryfikację.

Audyt może obejmować w szczególności weryfikację stosowanych zasad, procedur, zabezpieczeń technicznych, zabezpieczeń organizacyjnych, uprawnień dostępu, sposobu przechowywania informacji, sposobu przekazywania informacji oraz sposobu reagowania na incydenty.

Audyt przeprowadzany jest na koszt HOCHTIEF Polska S.A., chyba że strony ustalą inaczej.

Partner Biznesowy zobowiązuje się do współpracy przy przeprowadzeniu audytu, w szczególności do udostępnienia niezbędnych informacji, wyjaśnień oraz dokumentów w zakresie uzasadnionym celem audytu.

Jeżeli w wyniku audytu zostaną stwierdzone nieprawidłowości, Partner Biznesowy zobowiązuje się do ich usunięcia na własny koszt, w terminie uzgodnionym z HOCHTIEF Polska S.A., adekwatnym do charakteru i poziomu ryzyka wykrytych nieprawidłowości.

W przypadku nieusunięcia istotnych nieprawidłowości lub odmowy współpracy w zakresie audytu, HOCHTIEF Polska S.A. może podjąć działania przewidziane w umowie, w tym ograniczyć lub odebrać dostęp do swoich systemów, danych lub zasobów.

---

## **10. Zgłaszanie incydentów bezpieczeństwa informacji**

Partner Biznesowy zobowiązuje się do niezwłocznego zgłaszania HOCHTIEF Polska S.A. każdego stwierdzonego lub podejrzewanego incydentu bezpieczeństwa informacji, który może dotyczyć informacji, systemów, zasobów, projektów lub interesów HOCHTIEF Polska S.A.

Zgłoszenie powinno nastąpić niezwłocznie, nie później niż w ciągu 24 godzin od wykrycia incydentu lub uzyskania informacji o podejrzeniu incydentu.

Zgłoszenia należy kierować:

- e-mail: **incydent@hochtief.pl**
- telefon: **+48 726667686**

Zgłoszenie powinno, w miarę możliwości, zawierać:

- krótki opis zdarzenia,
- datę i godzinę wykrycia zdarzenia,
- wskazanie, jakich informacji, systemów, usług lub dokumentów może dotyczyć zdarzenie,
- informację o działaniach już podjętych przez Partnera Biznesowego,
- dane osoby kontaktowej po stronie Partnera Biznesowego.

Przykłady zdarzeń wymagających zgłoszenia:

- wysłanie wiadomości lub dokumentu do niewłaściwego odbiorcy,
- utrata laptopa, telefonu, nośnika danych lub dokumentacji,
- podejrzenie przejęcia konta użytkownika,
- podejrzenie wycieku informacji,
- infekcja złośliwym oprogramowaniem,
- nieuprawniony dostęp do systemu lub danych,
- naruszenie zasad dostępu do systemów HOCHTIEF Polska S.A.,
- utrata dostępności usługi istotnej dla HOCHTIEF Polska S.A.,
- przypadkowe ujawnienie informacji osobie nieuprawnionej.

Partner Biznesowy zobowiązuje się współpracować z HOCHTIEF Polska S.A. przy wyjaśnianiu incydentu, ograniczaniu jego skutków oraz wdrażaniu działań naprawczych.

---

## **11. Odpowiedzialność Partnera Biznesowego**

Partner Biznesowy odpowiada za zapewnienie, że jego pracownicy, współpracownicy, przedstawiciele oraz podwykonawcy, którzy mają dostęp do informacji HOCHTIEF Polska S.A., zostali poinformowani o obowiązujących zasadach bezpieczeństwa informacji i stosują je w praktyce.

Partner Biznesowy zobowiązuje się do podejmowania działań zapobiegających naruszeniom bezpieczeństwa informacji oraz do niezwłocznego usuwania wykrytych nieprawidłowości.

Partner Biznesowy ponosi odpowiedzialność za naruszenia bezpieczeństwa informacji wynikające z jego działania, zaniechania, niewłaściwej organizacji pracy, braku odpowiednich zabezpieczeń lub działania osób, którymi posługuje się przy realizacji współpracy z HOCHTIEF Polska S.A., z zastrzeżeniem postanowień właściwej umowy oraz obowiązujących przepisów prawa.

---

## **12. Poufność i wykorzystanie informacji**

Partner Biznesowy zobowiązuje się do zachowania w poufności informacji uzyskanych od HOCHTIEF Polska S.A. lub w związku ze współpracą z HOCHTIEF Polska S.A., niezależnie od sposobu ich przekazania.

Informacje te mogą być wykorzystywane wyłącznie w celu realizacji uzgodnionej współpracy.

Partner Biznesowy nie może kopiować, publikować, udostępniać, przekazywać ani wykorzystywać informacji HOCHTIEF Polska S.A. w innym celu bez uprzedniej zgody HOCHTIEF Polska S.A., chyba że obowiązek taki wynika z przepisów prawa.

Obowiązek zachowania poufności obowiązuje także po zakończeniu współpracy.

---

## **13. Zgodność z przepisami prawa i wymaganiami umownymi**

Partner Biznesowy zobowiązuje się do przestrzegania obowiązujących przepisów prawa, wymagań umownych oraz zasad bezpieczeństwa informacji uzgodnionych z HOCHTIEF Polska S.A.

Jeżeli Partner Biznesowy przetwarza dane osobowe w imieniu HOCHTIEF Polska S.A., zastosowanie mają również właściwe postanowienia dotyczące ochrony danych osobowych, w szczególności umowa powierzenia przetwarzania danych osobowych, jeżeli jest wymagana.

Jeżeli zakres współpracy obejmuje usługi informatyczne, usługi chmurowe, dostęp do systemów, dostęp do dokumentacji technicznej, integracje systemowe lub przetwarzanie informacji o podwyższonym znaczeniu dla HOCHTIEF Polska S.A., mogą zostać określone dodatkowe wymagania bezpieczeństwa, adekwatne do charakteru współpracy i poziomu ryzyka.

---

#### **14. Postanowienia końcowe**

Niniejsza Klauzula stanowi minimalny standard bezpieczeństwa informacji wymagany przez HOCHTIEF Polska S.A. wobec Partnerów Biznesowych.

W przypadku, gdy umowa, przepisy prawa lub odrębne uzgodnienia przewidują dalej idące wymagania bezpieczeństwa, zastosowanie mają wymagania bardziej rygorystyczne.

HOCHTIEF Polska S.A. zastrzega sobie prawo do aktualizacji niniejszej Klauzuli, w szczególności w przypadku zmian przepisów prawa, wymagań norm, zasad wewnętrznych, wyników audytów, incydentów bezpieczeństwa lub zmian w zakresie współpracy z Partnerami Biznesowymi.