**„Zasady bezpieczeństwa informacji dla partnerów biznesowych BGK”**

1. **Definicje**

Pojęcia użyte w niniejszym dokumencie oznaczają:

* 1. **BGK / Bank** – Bank Gospodarstwa Krajowego;
  2. **DB** – Departament Bezpieczeństwa w BGK;
  3. **Partner biznesowy** – strona umowy z BGK, świadcząca na rzecz Banku na podstawie umowy usługi lub zawierająca z Bankiem inną umowę niż umowa o produkty bankowe oferowane przez Bank;
  4. **Incydent bezpieczeństwa** – pojedyncze niepożądane lub niespodziewane zdarzenie lub seria takich zdarzeń, mających lub mogących mieć niekorzystny wpływ na integralność, poufność lub dostępność danych lub usług BGK w tym naruszenia poniższych zasad bezpieczeństwa;
  5. **Personel Partnera biznesowego [[1]](#footnote-1)** – wszystkie osoby, którym Partner biznesowy powierzył realizację umowy, niezależnie od podstawy prawnej ich zaangażowania,   
     w tym w szczególności: umów zlecenia lub umów o dzieło, jak również w ramach prowadzonej osobiście działalności gospodarczej (np. jednoosobowa działalność gospodarcza, spółka cywilna), o ile osobiście wykonują całość lub część powierzonych w umowie prac na rzecz Partnera biznesowego.

**Cel i Zakres**

1. Celem dokumentu jest zdefiniowanie obowiązków i odpowiedzialności Partnerów biznesowych   
   w zakresie ochrony zasobów informacyjnych BGK, do których będą mieli oni dostęp w toku świadczenia swoich usług.
2. Dokument określa minimalne wymagania techniczne i organizacyjne zapewniające bezpieczeństwo informacji przetwarzanych przez Partnerów biznesowych w toku realizacji umowy z BGK.
3. Zasady przetwarzania danych osobowych przez Partnerów biznesowych regulują postanowienia umowy.
4. Zasady zapewnienia ciągłości usług świadczonych dla BGK regulują postanowienia umowy.
5. W przypadku zawierania umowy na świadczenie usług z zakresu cyberbezpieczeństwa, Partnerzy biznesowi niezależnie od obowiązków określonych w niniejszym dokumencie, stosują się do wymogów określonych w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (dalej „Ustawa”).
6. Określone zasady bezpieczeństwa obowiązują wszystkich Partnerów biznesowych świadczących usługi na rzecz BGK z wyłączeniem usług sponsoringowych i partnerskich.
7. Dla umów na podstawie, których następuje powierzenie wykonywania czynności (tj. outsourcing lub podoutsourcing bankowy), w rozumieniu ustawy z dnia 29 sierpnia 1997 r. prawo bankowe, wytycznych EBA w zakresie outsourcingu, wszelkich innych regulacji, w tym wytycznych czy stanowisk organów nadzoru europejskiego i krajowego dotyczących outsourcingu lub przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej nie stosuje się zasad określonych w § 7 (kwestie te uregulowane są w umowie).

**Postanowienia ogólne**

1. Informacje przetwarzane przez Partnera biznesowego w trakcie realizacji usług na rzecz BGK muszą być wykorzystywane przy użyciu, co najmniej minimalnych środków technicznych   
   i organizacyjnych chroniących przed zniszczeniem, uszkodzeniem oraz nieautoryzowanym dostępem.
2. Partner biznesowy zobowiązuje się do informowania BGK o wszelkich incydentach bezpieczeństwa lub zdarzeniach, które mogą stanowić Incydent bezpieczeństwa.
3. Wszelkie wątpliwości z zakresu stosowania zasad bezpieczeństwa nieuwzględnionych   
   w niniejszym dokumencie wyjaśniane są za pośrednictwem opiekuna umowy po stronie BGK przy wsparciu DB.
4. W przypadku zakończenia współpracy przez Partnera biznesowego z Personelem Partnera biznesowego, który posiadał dostęp do infrastruktury, systemów lub pomieszczeń BGK, Partner biznesowy musi niezwłocznie, nie później niż w terminie 3 dni kalendarzowych od zakończenia współpracy powyższy fakt zgłosić do BGK w celu uniemożliwienia dostępu i korzystania w sposób nieuprawniony z dostępu.
5. W przypadku wykrycia Incydentu bezpieczeństwa lub podejrzenia nie stosowania się Partnera biznesowego do niniejszych zasad bezpieczeństwa informacji dla Partnerów biznesowych, BGK ma prawo do zablokowania dostępów dla Partnera biznesowego, w tym Personelu Partnera biznesowego.
6. Postanowienia dokumentu w tym zakres obligatoryjnych minimalnych zabezpieczeń technicznych i organizacyjnych należy stosować adekwatnie do rodzaju i zakresu świadczonych usług na rzecz BGK, posiadanych dostępów do: informacji, systemów i infrastruktury BGK.
7. Personel Partnera biznesowego, który będzie realizować czynności wynikające z umowy zawartej z BGK zobowiązany jest do zapoznania się z niniejszym dokumentem, zaakceptowania jego zasad, jak i przestrzegania zasad w nim zawartych w trakcie realizacji umowy i po jej zakończeniu.

**Bezpieczeństwo informacji**

1. Partner biznesowy jest zobowiązany do zachowania w tajemnicy wszelkich informacji,   
   w których posiadanie wejdzie w związku lub przy okazji zawarcia lub wykonywania umowy oraz po zakończeniu wykonywania umowy, bez względu na formę ich utrwalenia lub przekazania,   
   w tym choćby nie były one oznaczone lub choćby przekazane były w formie ustnej.
2. Informacje o których mowa w ust. 1 uwzględniają w szczególności:
   1. tajemnicę przedsiębiorstwa BGK w rozumieniu ustawy z dnia 16 kwietnia 1993 r.   
      o zwalczaniu nieuczciwej konkurencji, która obejmuje wszelkie nieujawnione do wiadomości publicznej informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, co do których BGK podjął niezbędne działania w celu zachowania ich poufności;
   2. tajemnicę bankową w rozumieniu art. 104 ustawy z dnia 29 sierpnia 1997 r. prawo bankowe, która obejmuje wszystkie informacje dotyczące czynności bankowych realizacji umów, na podstawie których BGK te czynności wykonuje.
3. Z zastrzeżeniem postanowień umowy, Partner biznesowy może ujawnić informacje poufne:
   1. Personelowi Partnera biznesowego, przy czym jedynie tym spośród nich i w takim zakresie, w jakim jest to niezbędne dla celów wykonywania umowy, oraz po uprzednim pisemnym ich zobowiązaniu do przestrzegania poufności informacji oraz uzyskaniu oświadczenia, o którym mowa w ust. 4;
   2. gdy obowiązek taki będzie wynikał z powszechnie obowiązujących przepisów prawa, jednakże w takim przypadki Partner biznesowy uprzednio poinformuje BGK o takim obowiązku umożliwiając BGK podjęcie właściwych czynności mających na celu ochronę informacji,
   3. w innych przypadkach, jedynie po uprzednim uzyskaniu zgody BGK.
4. Personel Partnera biznesowego, mający uzyskać, w ramach realizacji prac związanych   
   z wykonywaniem umowy, dostęp do informacji poufnych BGK, zobowiązany jest do podpisania oświadczenia o zachowaniu poufności, zgodnie z wzorem dostarczonym przez BGK. Oświadczenie przekazywane jest BGK przez Partnera biznesowego najpóźniej w dniu podjęcia czynności wiążących się z dostępem do informacji BGK przez danego członka Personelu Partnera biznesowego.
5. W trakcie trwania umowy Partner biznesowy zobowiązany jest zapoznać nowy Personel Partnera biznesowego mający posiadać dostęp do informacji BGK z Zasadami bezpieczeństwa informacji dla Partnerów biznesowych BGK oraz dostarczyć do BGK podpisane oświadczenia   
   o zachowaniu poufności.
6. Partner biznesowy zobowiązuje się do przetwarzania powierzonych danych i informacji wyłącznie w celu realizacji umowy zawartej z BGK, z zachowaniem należytej staranności, działając zgodnie z obowiązującymi przepisami prawa.

**Wymagania techniczne i organizacyjne**

1. Partner biznesowy zobowiązuje się do stosowania, co najmniej opisanych poniżej minimalnych wymagań technicznych i organizacyjnych zapewniających bezpieczeństwo informacji BGK.
2. Wymagany minimalny poziom bezpieczeństwa osiągany jest poprzez zastosowanie środków bezpieczeństwa w obszarach:
   1. Zarządzanie dostępami fizycznymi do pomieszczeń BGK:
      * 1. Opiekunowie umów zobowiązani są do przedstawienia Personelowi Partnera biznesowego zasad bezpieczeństwa fizycznego, zgodnych z przepisami wewnętrznymi Banku w zakresie ruchu osobowo-materiałowego;
   2. Personel Partnera biznesowego przebywający na terenie Banku zobowiązany jest stosować się do poleceń pracowników BGK koordynujących realizację umowy, pracowników ochrony Banku oraz DB , którzy przekazują polecenia zgodnych z przepisami wewnętrznymi Banku w zakresie ruchu osobowo-materiałowego;
   3. Zarządzanie uprawnieniami i dostępami technicznymi do infrastruktury i systemów BGK:
      * 1. Partner biznesowy może mieć dostęp do infrastruktury BGK:

* bezpośredni, z wykorzystaniem sprzętu, którego właścicielem jest BGK, pod nadzorem pracownika BGK w przypadku realizowania zadań   
  w siedzibie BGK;
* zdalny, z wykorzystaniem dedykowanego rozwiązania BGK. W celu dostępu zdalnego wymagane jest zainstalowanie dedykowanego oprogramowania BGK oraz zapewniać adekwatny poziom bezpieczeństwa sprzętu, z którego realizowany jest dostęp zdalny oraz na którym przetwarzane są informacje BGK. Zgoda na dostęp zdalny musi wynikać z postanowień umowy;
  + - 1. dostęp do informacji jest realizowany wyłącznie poprzez indywidualne konto   
         w domenie BGK dla każdej osoby wchodzącej do składu Personelu Partnera biznesowego, dla której dostęp do infrastruktury jest niezbędny do realizacji umowy;
      2. dostęp nadawany jest przez BGK wyznaczonym osobom z Personelu Partnera biznesowego w zakresie niezbędnym do świadczenia usług, wynikającym   
         z postanowień umowy;
      3. Partner biznesowy wnioskuje do BGK o potrzebę dostępu do zasobów,   
         z zastrzeżeniem prawa BGK do odrzucenia takiego wniosku;
      4. Partner biznesowy każdorazowo zgłosi do BGK potrzebę instalacji dodatkowego oprogramowania;
      5. Partner biznesowy może wykorzystywać otrzymane oprogramowanie, tylko  
          w celu i na zasadach ustalonych w umowie;
      6. Partner biznesowy nie może samodzielnie instalować żadnego oprogramowania na systemach stanowiących infrastrukturę BGK (komputery, laptopy, urządzenia mobilne, serwery, bazy danych, itp.);
      7. Partner biznesowy podczas realizacji prac w infrastrukturze BGK nie może korzystać z dostępu do sieci publicznej – Internetu, chyba że BGK wyrazi na to zgodę. BGK zastrzega sobie prawo do ograniczania, filtrowania oraz monitorowania takiego dostępu;
  1. Zarządzanie poświadczeniami i zasady uwierzytelniania:
     + 1. indywidualne konto w domenie BGK nie może być współdzielone;
       2. dane uwierzytelniające (w szczególności login i hasło) nie mogą być przekazywane innej osobie niż właściciel konta oraz muszą być chronione przed nieuprawnionym dostępem;
       3. w procesie uwierzytelniania mogą być wykorzystywane dopuszczone przez BGK metody MFA, tj. uwierzytelnianie wieloskładnikowe;
       4. Hasła muszą być:
* zgodne ze standardami ustanowionymi przez BGK;
* znane wyłącznie ich właścicielom;
* zmieniane okresowo;
* zmienianie również w przypadku wątpliwości dotyczących zachowania ich poufności;
  1. Monitoring działań:
     + 1. wszystkie działania Partnera biznesowego w infrastrukturze teleinformatycznej podlegają monitorowaniu przez systemy bezpieczeństwa BGK;
       2. Partner biznesowy nie może próbować pominąć zabezpieczeń BGK;
  2. Zarządzanie informacją w formie elektronicznej oraz nośnikami:
     + 1. wymiana informacji pomiędzy BGK a Partnerem biznesowym powinna być realizowana za pomocą:
* poczty elektronicznej;
* udostępnionego w sieci publicznej zasobu sieciowego, do którego dostęp zapewni BGK;
* dedykowanej platformy do obsługi technicznej;
* dedykowanego oprogramowania do zdalnego dostępu w przypadku konieczności pobierania plików na stacje Partnerów biznesowych;
* wszystkie inne kanały wymiany plików muszą zostać zaopiniowane   
  i zaakceptowane przez BGK;
  + - 1. w przypadku wymiany informacji za pomocą poczty elektronicznej, Partner biznesowy ma obowiązek zapewnienia poufności i integralności przesyłanej informacji zgodnie z postanowieniami umowy;
      2. Partner biznesowy, któremu utworzono skrzynkę pocztową w domenie BGK zabrania się przesyłania wiadomości e-mail poza domenę BGK;
      3. o sposobie wymiany informacji decyduje BGK;
      4. Partner biznesowy ma obowiązek przechowywania wszystkich plików na zasobach sieciowych BGK;
      5. BGK nie dopuszcza przetwarzania informacji na nośnikach innych niż przekazanych przez BGK;
      6. BGK nie dopuszcza podłączania jakichkolwiek urządzeń do sprzętu, którego właścicielem jest BGK;
  1. Zarządzanie informacją w formie papierowej:
     + 1. Partner biznesowy:
* nie może wynosić, poza siedzibę BGK lub poza budynki, w których realizowana jest umowa na rzecz BGK, żadnych dokumentów   
  w formie papierowej;
* pracując zdalnie nie drukuje dokumentów i innych informacji/danych objętych ochroną;
* przetwarza dokumenty w formie papierowej w zakresie koniecznym do wykonywania umowy oraz w sposób uniemożliwiający zapoznanie się   
  z ich treścią przez osoby do tego nieupoważnione;
* niepotrzebne kopie dokumentów roboczych w formie papierowej należy:
  + wyrzucać do dedykowanych kontenerów znajdujących się   
    w siedzibie BGK, lub
  + zniszczyć w niszczarce w sposób uniemożliwiający odtworzenie ich treści;
* jest zobowiązany do zachowania polityki czystego biurka oraz pulpitu podczas pracy w siedzibie BGK.

**Incydenty bezpieczeństwa**

1. Partner biznesowy jest zobowiązany do informowania BGK o wszelkich Incydentach bezpieczeństwa, mających lub mogących mieć niekorzystny wpływ na integralność, poufność lub dostępność danych lub usług BGK, niezwłocznie, nie później niż w terminie 24 godzin zegarowe od stwierdzenia danego Incydentu bezpieczeństwa. Incydenty bezpieczeństwa należy zgłaszać drogą mailową na adres: [csirt@bgk.pl](mailto:csirt@bgk.pl).
2. Informacja dotycząca Incydentu bezpieczeństwa, o której mowa w ust. 1 powinna obejmować, co najmniej datę i godzinę (format hh:mm) identyfikacji Incydentu bezpieczeństwa, opis Incydentu bezpieczeństwa, zakres danych lub usług objętych Incydentem bezpieczeństwa, oraz podejmowanych przez Partnera biznesowego działań zaradczych.
3. Partner biznesowy jest zobowiązany do:
   1. gromadzenia i przekazania do BGK materiałów z postępowania wyjaśniającego,
   2. przedstawienia BGK raportu z oceny i analizy Incydentu bezpieczeństwa.

**Audyty bezpieczeństwa**

1. Poniższe zasady, wskazane w niniejszym paragrafie dotyczą audytów bezpieczeństwa odnoszących się do umów innych niż umowy outsourcingowe lub podoutsourcingowe. Zasady audytów, w tym audytów bezpieczeństwa w ramach umów outsourcingowych lub podoutsourcingowe regulują odpowiednie postanowienia umowy.
2. W przypadku uzasadnionego podejrzenia naruszenia Zasad bezpieczeństwa informacji przez Partnera biznesowego, BGK lub osoby przez niego wskazane i pisemnie upoważnione są uprawnione do przeprowadzenia audytu bezpieczeństwa stosowanych przez Partnera biznesowego środków bezpieczeństwa. Audyt bezpieczeństwa może odbywać się w siedzibie Partnera biznesowego oraz we wszystkich miejscach wykonywania czynności na rzecz BGK lub w formie zdalnej za uprzednim uzgodnieniem terminu, przy czym nie później niż w terminie 14 (czternastu) dni od dnia poinformowania Partnera biznesowego przez BGK.
3. Partner biznesowy jest zobowiązany do współpracy z BGK i upoważnionymi przez BGK audytorami, w szczególności zapewniając dostęp do pomieszczeń, urządzeń, systemów   
   i sieci wykorzystywanych przez Partnera biznesowego w celu wykonywania umowy oraz do dokumentacji niezbędnej do przeprowadzenia audytu z uwzględnieniem wewnętrznych regulacji Partnera biznesowego dotyczących zasad bezpieczeństwa przebywania w biurach Partnera biznesowego lub miejscach wykonywania czynności na rzecz BGK, o których Partner biznesowy powiadomi uprzednio BGK.
4. BGK zobowiązuje się do przeprowadzania audytu bezpieczeństwa w godzinach pracy Partnera biznesowego oraz w sposób niezakłócający funkcjonowania Partnera biznesowego.
5. Partner biznesowy zobowiązuje się do niezwłocznego usuwania nieprawidłowości stwierdzonych podczas przeprowadzonych audytów bezpieczeństwa oraz do zrealizowania zaleceń poaudytowych na własny koszt.
6. Partner biznesowy jest zobowiązany do zapewnienia, w drodze umów zawieranych   
   z podwykonawcami, że obowiązki dotyczące audytów bezpieczeństwa, opisane w niniejszym paragrafie, będą miały zastosowanie również do jego podwykonawców w zakresie, w jakim biorą oni udział w wykonywaniu umowy.
7. Dopuszcza się odstąpienie od przeprowadzenie audytu bezpieczeństwa Partnera biznesowego w przypadku pozyskania potwierdzenia posiadania przez Partnera biznesowego aktualnego certyfikatu na zgodność z wymaganiami międzynarodowych standardów bezpieczeństwa. Decyzję w tym przypadku podejmuje każdorazowo DB.

1. W szczególności rozumiane jako Zleceniobiorca, Wykonawca, Dostawca, Sponsorowany. W zależności od określenia Stron w umowie z BGK. [↑](#footnote-ref-1)