Załącznik nr 11 do Umowy

Warunki dotyczące zapewnienia cyber bezpieczeństwa infrastruktury do rejestracji i przesłania obrazu oraz monitorowania wizyjnego:

1. Wszystkie elementy infrastruktury CCTV (Closed Circuit Television) w pojedynczej lokalizacji  
   powinny być podłączone w jednej, dedykowanej do tego celu sieci lokalnej, która powinna  
   być fizycznie odseparowana od innych sieci, a w szczególności tych, pozwalających na  
   komunikację z siecią Internet. W przypadku braku takiej możliwości niezbędne jest logiczne  
   oddzielenie od innych sieci poprzez zastosowanie np. VLAN (Virtual Local Area NetWork).
2. Jeżeli w szczególnych, uzasadnionych i popartych szacowaniem ryzyka przypadkach  
   komponenty infrastruktury CCTV mają być dostępne poprzez sieć Internet lub WAN (Wide  
   Area NetWork), to dostęp do takich komponentów powinien odbywać się poprzez VPN  
   z silnym mechanizmem szyfrowania.
3. W szczególnych, uzasadnionych i popartych szacowaniem ryzyka przypadkach gdy  
   występuje konieczność dostępu do infrastruktury CCTV z innych sieci lub dostępu zdalnego  
   należy zastosować mechanizmy kontroli dostępu w oparciu o zaporę sieciową blokującą  
   każdą komunikację za wyjątkiem tej, która jest niezbędna. Powinny być również  
   zastosowane silne mechanizmy uwierzytelnienia i rejestracji zdarzeń.
4. Rekomendowane jest, aby komponenty CCTV były połączone przewodowo do infrastruktury  
   sieciowej i jeżeli nie ma takiej konieczności, nie powinny posiadać możliwości komunikacji  
   bezprzewodowej (wbudowanych modemów) aby uniknąć ich niezamierzonego  
   wykorzystania takiej funkcjonalności.
5. Przełączniki sieciowe wykorzystywane do podłączenia kamer CCTV powinny zapewniać  
   kontrolę dostępu do portów (np. 802.1x, port security).
6. W szczególnych, uzasadnionych i popartych szacowaniem ryzyka przypadkach gdy  
   występuje konieczność połączenia elementów infrastruktury CCTV bezprzewodowo należy  
   stosować połączenia z przetestowanymi i silnymi mechanizmami uwierzytelnienia oraz  
   szyfrowania, odpornymi na ataki polegające na ich przełamaniu.
7. Rekomendowane jest wyłączenie wszystkich nie wykorzystywanych funkcjonalności, usług  
   i portów w infrastrukturze CCTV. W przypadku interfejsów fizycznych (np. USB) wskazane  
   jest również ich zablokowanie (np. plomba, blokada fizyczna).
8. Wszystkie kamery CCTV powinny posiadać włączone uwierzytelnianie z silnym unikalnym  
   hasłem dostępowym.
9. Kamery CCTV należy umieszczać w sposób ograniczający fizyczny dostęp osób  
   nieuprawnionych, a jeśli jest to niemożliwe, to rekomendowane jest wyłączenie możliwości  
   resetu haseł kamer CCTV oraz dodatkowe monitorowanie zdarzeń generowanych przez  
   kamery przez dedykowany do tego celu personel.
10. W przypadku gromadzenia nagrań lub utrzymywania kopii zapasowych konfiguracji urządzeń  
    bądź zarejestrowanego obrazu rekomendowane jest wykorzystanie do tego celu  
    infrastruktury (serwery, chmura prywatna) w lokalizacji należącej do podmiotu, który jest  
    właścicielem infrastruktury CCTV i znajdującej się na terenie Europejskiego Obszaru  
    Gospodarczego (EOG), a dane powinny być wysyłane w sposób szyfrowany.
11. Rekomendowane jest wyłączenie protokołów nie zapewniających szyfrowania lub  
    rozgłaszających dane np. HTTP, RTSP (Real-Time Streaming Protocol) lub, gdy to  
    niemożliwe, blokowanie ruchu na zaporze sieciowej.
12. Oprogramowanie kamer CCTV oraz innych elementów infrastruktury CCTV powinno być  
    aktualizowane i pozyskiwane z zaufanych źródeł, tj. od znanych producentów.
13. Elementów infrastruktury CCTV działające w oparciu osprzęt komputerowy powinny  
    posiadać zainstalowane i aktualne oprogramowanie chroniące przed szkodliwym  
    oprogramowaniem.
14. Podmioty dostarczające i wdrażające infrastrukturę CCTV powinny posiadać Koncesję  
    Ministerstwa Spraw Wewnętrznych i Administracji na usługi instalowania oraz naprawiania  
    systemów alarmowych.
15. Pracownicy podmiotów realizujących instalację lub obsługę infrastruktury CCTV powinni  
    posiadać Legitymację Kwalifikowanego Pracownika Zabezpieczenia Technicznego.
16. Producent elementów infrastruktury CCTV powinien zapewniać poprawki bezpieczeństwa  
    w przypadku stwierdzenia podatności. Nie powinny być akceptowane kamery CCTV  
    zawierające krytyczne podatności według skali CVSS (Common Vulnerability Sconng  
    System), które nie zostały usunięte lub, które charakteryzują się dużą ilością wykrytych CVE  
    (Common Vulnerabilities and Exposures).
17. Wybór kamery CCTV powinien uwzględniać ocenę ryzyka dotyczącego celowego  
    umieszczania przez producenta lub dystrybutora ukrytych funkcjonalności, tzw. „tylnych  
    furtek/backdoor”, podatności lub nie spełniania wymagań cyberbezpieczeństwa. Ocena

ryzyka może opierać się na dostępnych informacjach w tym zakresie (np. certyfikaty  
bezpieczeństwa, publikacje) lub wynikach przeprowadzonych badań cyberbezpieczeństwa  
kamer CCTV.

1. Rekomendowane jest prowadzenie okresowych audytów (min. raz w roku) na terenie  
   obiektu/infrastruktury w celu identyfikacji działających urządzeń CCTV, ustalenia ich  
   właścicieli, przeznaczenia i zakresu rejestracji obrazu, sposobu wykorzystania  
   i postępowania z zarejestrowanym obrazem/nagraniami oraz zweryfikowania stanu  
   bezpieczeństwa teleinformatycznego (z uwzględnieniem skanowania podatności).
2. W ramach audytu wskazane jest pozyskanie i ocena m.in. następujących informacji:
3. Czy wykorzystywana jest sieć Wi-Fi lub inna komunikacja bezprzewodowa do rejestracji  
   i przesyłania obrazu oraz monitorowania wizyjnego?
4. W jaki sposób jest zabezpieczona sieć bezprzewodowa (szyfrowanie, uwierzytelnienie  
   i kontrola dostępu)?
5. Czy urządzenia CCTV są umieszczone w dedykowanej do tego celu sieci, która jest  
   odseparowana od innych sieci np. sieci kontroli dostępu, sieci biurowej?
6. Czy sieć CCTV jest chroniona w zakresie dostępu (dostęp do sieci poprzez przełączniki  
   sieciowe z kontrolą dostępu do portów (np. 802.1x, port security), zapora sieciowa przy  
   dostępie z innych segmentów, uwierzytelnienie)?
7. Czy zarejestrowany obraz/nagrania są udostępniane lub transmitowane poza  
   infrastrukturę dedykowanej sieci CCTV np. do chmury producenta urządzeń CCTV, firmy  
   utrzymującej urządzenia CCTV lub zewnętrznej firmy prowadzącej monitorowanie?
8. Czy możliwy jest zdalny dostęp do kamery CCTV, sieci CCTV?
9. Jaka firma jest producentem urządzeń CCTV oraz urządzeń na których gromadzone są  
   nagrania?
10. Czy urządzenia w sieci CCTV posiadają zaktualizowane oprogramowanie (w tym  
    firmware)?
11. Jakie podmioty odpowiadają za utrzymanie urządzeń CCTV i ich naprawy?
12. Czy wykorzystywane są urządzenia udostępniające publicznie obraz tzw. „Iive  
    streaming”?
13. Czy protokół RTSP jest włączony na urządzeniach?
14. Czy na każdym urządzeniu CCTV dostęp do obrazu jest możliwy wyłącznie po przejściu  
    panelu logowania?