Załącznik nr 2 – Opis wdrożonych środków organizacyjnych i technicznych służących ochronie danych osobowych

Obszar	Środki bezpieczeństwa
System Zarządzania Bezpieczeństwem Informacji	**Polityki bezpieczeństwa.** Opracowano ogólną politykę bezpieczeństwa oraz szczegółowe polityki bezpieczeństwa dotyczące bezpieczeństwa organizacji, bezpieczeństwa informacji, bezpieczeństwa systemów informatycznych oraz bezpieczeństwa osób i mienia, w których określono podstawowe cele jakim maja służyć działania związane z realizacją polityk. Polityki podlegają okresowym przeglądom i aktualizacjom zatwierdzanym przez najwyższe kierownictwo Spółki. Określono role i zadania w procesach związanych z zarządzaniem bezpieczeństwem. Wyznaczono osoby odpowiedzialne za realizację każdej polityki bezpieczeństwa. **Standardy bezpieczeństwa.** Określono ogólne i szczególne standardy bezpieczeństwa realizujące założenia polityk bezpieczeństwa w zakresie bezpieczeństwa informacji, bezpieczeństwa systemów informatycznych, bezpieczeństwa osób i mienia. Opracowano program okresowych przeglądów i aktualizacji opracowanych standardów bezpieczeństwa. **Procedury i Instrukcje.** Opracowano szczegółowe procedury i instrukcje postępowania dotyczące realizacji standardów bezpieczeństwa w zakresie bezpieczeństwa informacji, bezpieczeństwa systemów informatycznych, bezpieczeństwa osób i mienia. Opracowano program okresowych przeglądów i aktualizacji opracowanych procedur i instrukcji postępowania dotyczących realizacji standardów bezpieczeństwa. **Właściciele Zasobów.** Dla każdego zasobu (fizycznego i elektronicznego), mającego wartość dla organizacji, wyznaczono osobę odpowiedzialną (Właściciela Zasobu), której przypisano odpowiedzialność za zarządzanie bezpieczeństwem danego zasobu. Wdrożono procesy identyfikacji i zbierania zasobów od osób kończących stosunek pracy lub nie potrzebujących już dostępu do danego zasobu. **Inspektor Ochrony Danych.** W celu zapewnienia właściwego poziomu realizacji ochrony danych osobowych wyznaczono i powołano niezależnego Inspektora Ochrony Danych. Zapewniono bezpośrednią podległość Inspektora Ochrony Danych pod najwyższe kierownictwo Spółki. Zapewniono włączenie Inspektora Ochrony Danych we wszystkie procesy związane z przetwarzaniem danych osobowych. Zapewniono Inspektorowi Ochrony Danych Osobowych odpowiedni dostęp do informacji i dokumentacji związanej z przetwarzaniem danych osobowych. **Osoby upoważnione do przetwarzania danych osobowych.** Osoby przetwarzające dane osobowe na zlecenie i w imieniu Spółki otrzymały imienne upoważnienie do przetwarzania danych osobowych. Opracowano i wdrożono system wewnętrznych szkoleń z zakresu bezpieczeństwa i ochrony danych osobowych. Wszystkie osoby upoważnione do przetwarzania danych osobowych zostały objęte systemem wewnętrznych szkoleń z zakresu bezpieczeństwa i ochrony danych osobowych. Osoby mające dostęp do danych

Obszar	Środki bezpieczeństwa
	zostały zobowiązane do zachowania poufności w czasie trwania stosunku pracy oraz po jego ustaniu. **Monitorowanie zmian prawa.** Opracowano, wdrożono i zapewniono utrzymanie ciągłości działania systemu monitorowania zmian w obowiązujących przepisach prawa dotyczących zasad przetwarzania danych osobowych. **Zarządzanie uprawnieniami dostępu.** Opracowano procedury zarządzania uprawnieniami dostępu do nośników danych, pomieszczeń, stref, budynków oraz systemów informatycznych i elementów infrastruktury informatycznej oraz sieci. Zapewniono, iż uprawnienia dostępu są doraźnie oraz okresowo monitorowane i kontrolowane. Zapewniono, iż osobom upoważnionym do przetwarzania danych osobowych przydzielane są minimalne prawa dostępu do danych w zależności od wymagań ich stanowiska pracy oraz realizowanych zadań. Wdrożono możliwość monitorowania operacji przetwarzania w odniesieniu do osób, które usuwają, dodają lub modyfikują dane osobowe. **Zabezpieczenie nośników danych osobowych.** Zapewniono, iż klucze oraz kody dostępu do szaf iprzydzielane są osobom upoważnionym do przetwarzania danych osobowych zgodnie z zakresem upoważnienia i zakresem zadań realizowanych na danym stanowisku pracy. **Zabezpieczenie budynków, stref, pomieszczeń lub części pomieszczeń w których są przetwarzane dane osobowe.** Zapewniono, iż: (i) klucze, kody dostępu oraz uprawnienia dostępu w systemie kontroli dostępu do budynków, stref, pomieszczeń lub części pomieszczeń, w których przetwarzane są dane osobowe, przydzielane są osobom upoważnionym do przetwarzania danych osobowych zgodnie z zakresem upoważnienia i zakresem zadań realizowanych na danym stanowisku pracy; (ii) budynki, strefy, pomieszczenia lub części pomieszczeń, w których przetwarzane są dane osobowe, zabezpiecza się przed dostępem osób nieuprawnionych, w czasie nieobecności osób uprawnionych do przebywania w tych pomieszczeniach. Osoby nieuprawnione do przebywania w pomieszczeniach służących do przetwarzania danych osobowych mogą przebywać w nich jedynie pod nadzorem osób uprawnionych. **Dostęp do systemów informatycznych, elementów infrastruktury informatycznej i sieci.** Zapewniono, iż dla każdej osoby uprawnionej do dostępu do systemu informatycznego, elementu infrastruktury informatycznej lub sieci: (i) nadawany jest unikalny identyfikator, który nie może zostać przypisany innej osobie; (ii) autoryzacja realizowana jest przy użyciu bezpiecznych metod transmisji danych służących do uwierzytelnienia; (iii) hasło dostępu podlega procedurom audytu oraz zmianie w ustalonym okresie czasu. **Zarządzanie zagrożeniami i podatnością na atak.** Przeprowadzane jest okresowe skanowanie luk bezpieczeństwa na platformach i sieciach przetwarzających dane osobowe w celu zapewnienia zgodności z powszechnymi normami bezpieczeństwa związanymi konkretnie z wzmocnieniem systemu. W wyniku testów penetracyjnych, skanowania podatności na atak oraz oceny zgodności prowadzony jest okresowo program naprawczy w podejściu opartym o ryzyko w celu wykorzystania uzyskanych

Obszar	Środki bezpieczeństwa
	wniosków. **Bezpieczeństwo dostawców usług i podwykonawców.** Opracowano zasady wyboru podwykonawców i dostawców gwarantujące zapewnienie odpowiedniego poziomu bezpieczeństwa technicznego i organizacyjnego świadczonych usług i realizowanych zadań. Opracowano standardy i mechanizmy kontroli podwykonawców i dostawców usług oraz zagwarantowano ich realizację. **Zarządzanie zmianą.** Wdrożono udokumentowaną politykę kontroli zmian obejmującą wymagania w zakresie zatwierdzania, klasyfikacji, testowania i testowania planu back-out oraz rozdzielenie obowiązków pomiędzy wniosek, zatwierdzenie a wdrożenie. Wdrożono procedury zarządzania i reagowania na incydenty naruszenia bezpieczeństwa, które umożliwiają rozsądne wykrywanie, badanie, reagowanie, łagodzenie skutków i powiadamianie o zdarzeniach, które obejmują zagrożenie dla poufności, integralności i/lub dostępności do danych osobowych. Procedury reagowania i zarządzania są udokumentowane, sprawdzone i przynajmniej raz do roku podlegają przeglądom. **Dodatkowe środki bezpieczeństwa aplikacji ClickMeeting.** Opracowano i wdrożono standardy: (i) bezpiecznego wytwarzania oprogramowania. (ii) dotyczące analizy ryzyka naruszenia praw podstawowych i wolności osób których dane dotyczą oraz utraty poufności, dostępności i integralności danych osobowych na każdym etapie cyklu życia produktu; (iii) dotyczące zachowania zasady ochrony prywatności w fazie projektowania oprogramowania; (iv) dotyczące zachowania zasady ochrony prywatności w ustawieniach domyślnych w fazie projektowania oprogramowania. Opracowano i zapewniono program szkoleń z zakresu zasad bezpiecznego wytwarzania oprogramowania, program testów bezpieczeństwa oprogramowania.
Bezpieczeństwo operacji przetwarzania danych osobowych	**Bezpieczeństwo zbierania danych.** Dane osobowe zabezpiecza się przed utratą rozliczalności poprzez zastosowanie rozwiązań pozwalających przypisać określone działania konkretnej osobie lub systemowi informatycznemu. **Bezpieczeństwo dostępu do danych.** Dane osobowe zabezpiecza się przed utratą poufności za pomocą: (i) bezpiecznych metod uwierzytelniania dostępu dla osób i systemów informatycznych; (ii) monitorowania poprawności działania oraz sposobu użycia bezpiecznych metod uwierzytelniania dostępu dla osób i systemów informatycznych; (iii) przeprowadzanych i dokumentowanych okresowych (przynajmniej raz do roku) przeglądów dostępu wszystkich użytkowników, kont systemowych, kont testowych oraz kont ogólnych; (iv) wdrożenie mechanizmów kontroli sesji, w tym blokadę konta i wygaśnięcie sesji po ustalonym czasie. **Bezpieczeństwo przesyłania/transmisji danych.** Dane osobowe przekazywane drogą teletransmisji zabezpiecza się przed utratą poufności i integralności przy pomocy kryptograficznych środków ochrony danych osobowych (szyfrowanie danych w tranzycie), a także poprzez zastosowanie segmentacji sieci teleinformatycznych (segmentacja sieci). **Bezpieczeństwo przechowywania danych.** Dane osobowe przechowywane na

Obszar	Środki bezpieczeństwa
	nośnikach danych zabezpiecza się przed utratą poufności, dostępności i integralności poprzez zastosowanie: (i) fizycznej lub logicznej separacji danych (separacja danych); (ii) mechanizmów tworzących kopie danych w czasie rzeczywistym (replikacja danych); (iii) mechanizmów tworzących przyrostowe lub całościowe kopie bezpieczeństwa danych w ustalonym interwale czasowym (backup danych); (iv) mechanizmów i procedur przywracania danych, przełączania źródeł danych oraz odtwarzania kopii bezpieczeństwa danych. Dane osobowe przechowywane w bazach danych zabezpiecza się przed utratą integralności poprzez zastosowanie reguł spójności w zakresie semantycznym (definicja typu danych), zakresie encji (definicja kluczy podstawowych) oraz w zakresie referencyjnym (definicja kluczy obcych). **Bezpieczeństwo opracowywania danych.** Dane osobowe zabezpiecza się: (i) przed utratą poufności poprzez zapewnienie dostępu do danych wyłącznie uprawnionym osobom i systemom informatycznym; (ii) przed utratą dostępności i integralności poprzez zastosowanie mechanizmów tworzących kopie robocze danych; (iii) przed utratą rozliczalności poprzez zastosowanie rozwiązań pozwalających przypisać określone działania konkretnej osobie lub systemowi informatycznemu. **Bezpieczeństwo modyfikowania danych.** Dane osobowe zabezpiecza się przed utratą poufności poprzez zapewnienie dostępu do danych wyłącznie uprawnionym osobom i systemom informatycznym. Rozliczalność operacji modyfikowania danych osobowych zapewnia się poprzez zastosowanie rozwiązań pozwalających przypisać określone działania konkretnej osobie lub systemowi informatycznemu. **Bezpieczeństwo usuwania danych.** Dane osobowe zabezpiecza się przed utratą poufności i dostępności poprzez zapewnienie dostępu do danych wyłącznie uprawnionym osobom i systemom informatycznym. Rozliczalność operacji usuwania danych osobowych zapewnia się poprzez zastosowanie rozwiązań pozwalających przypisać określone działania konkretnej osobie lub systemowi informatycznemu.
Bezpieczeństwo fizyczne	**Bezpieczeństwo nośników danych osobowych.** Nośniki danych osobowych (dokumenty, zewnętrzne nośniki danych) zabezpiecza się przed dostępem osób nieuprawnionych poprzez przechowywanie w szafach biurowych wyposażonych w zamki mechaniczne. Dodatkowy zakres zastosowanych środków technicznej ochrony nośników danych osobowych ustalany jest indywidualnie w zależności od zidentyfikowanych zagrożeń, wymaganego stopnia ochrony i możliwości technicznych. **Bezpieczeństwo pomieszczeń, w których przetwarzane są dane osobowe.** Pomieszczenia, w których przetwarzane są dane osobowe, zabezpiecza się: (i) przed dostępem osób nieuprawnionych poprzez zastosowanie zamków mechanicznych, zamków szyfrowych, systemu kontroli dostępu oraz systemu sygnalizacji włamania; (ii) przed zniszczeniem na skutek pożaru lub zalania poprzez zastosowanie systemu alarmu pożarowego oraz systemu sygnalizacji włamania i napadu. Dodatkowy zakres zastosowanych środków kontroli dostępu do pomieszczeń ustalany jest indywidualnie w zależności od

Obszar	Środki bezpieczeństwa
	zidentyfikowanych zagrożeń, wymaganego stopnia ochrony danego pomieszczenia i możliwości technicznych. **Bezpieczeństwo budynków i obszarów w których znajdują się pomieszczenia służące do przetwarzania danych osobowych.** Budynki i obszary w których znajdują się pomieszczenia służące do przetwarzania danych osobowych zabezpiecza się przed dostępem osób nieuprawnionych poprzez zastosowanie systemów kontroli dostępu, systemu sygnalizacji włamania i napadu oraz systemu dozoru realizowanego przez pracowników ochrony fizycznej. Strefy wewnętrzne oraz zewnętrzne, w których znajdują się pomieszczenia służące do przetwarzania danych osobowych, zabezpiecza się dodatkowo w celu monitorowania oraz identyfikowania zagrożeń i zdarzeń niepożądanych przez zastosowanie systemu telewizji przemysłowej. Zakres zastosowanych środków kontroli dostępu do budynków i obszarów w których znajdują się pomieszczenia służące do przetwarzania danych osobowych ustalany jest indywidualnie w zależności od zidentyfikowanych zagrożeń, wymaganego stopnia ochrony danego budynku lub strefy i możliwości technicznych.
Bezpieczeństwo teleinformatyczne	**Bezpieczeństwo nośników danych osobowych.** Nośniki danych służące do przetwarzania danych osobowych: (i) przed ich zainstalowaniem w urządzeniu zabezpiecza się przed dostępem osób nieuprawnionych poprzez ograniczenie i kontrolę dostępu realizowaną za pomocą szaf pancernych; (ii) zabezpiecza się przed utratą poufności danych przez zastosowanie wbudowanych procedur kryptograficznej ochrony danych (kryptograficzna ochrona nośników danych); (iii) zabezpiecza się przed utratą dostępności poprzez zastosowanie systemów automatycznego monitoringu działania, wykorzystania pojemności i czasu dostępności; (iv) zabezpiecza się przed niedozwolonym wykorzystaniem poprzez zastosowanie procedur użycia i konfiguracji elementów infrastruktury informatycznej (zarządzanie konfiguracją); (v) przeznaczone do ponownego wykorzystania zabezpiecza się przed ujawnieniem danych osobie nieuprawnionej lub systemowi informatycznemu poprzez zastosowanie bezpiecznych metod usuwania danych; (vi) przeznaczone do likwidacji zabezpiecza się przed ponownym wykorzystaniem poprzez trwałe i celowe mechaniczne uszkodzenie. **Bezpieczeństwo elementów infrastruktury sieciowej.** Elementy infrastruktury sieciowej służącej do przetwarzania danych osobowych zabezpiecza się: (i) przed dostępem osób nieuprawnionych oraz systemów informatycznych przez zastosowanie bezpiecznych metod uwierzytelniania dostępu; (ii) przed dostępem osób nieuprawnionych, systemów informatycznych oraz utratą dostępności poprzez monitorowanie aktualności systemu operacyjnego i zainstalowanego oprogramowania; (iii) przed dostępem osób nieuprawnionych, systemów informatycznych oraz utratą dostępności poprzez zastosowanie oprogramowania typu Firewall, Intrusion Detection Systems, Intrusion Prevention Systems, Anty DDOS; (iv) przed utratą dostępności poprzez zastosowanie zwielokrotnienia, wirtualizacji i automatycznych procedur skalowania, zastosowanie automatycznych procesów monitorowania dostępności, obciążenia i wydajności, zastosowanie zapasowych źródeł zasilania oraz automatycznych procedur zmiany źródła zasilania, zastosowanie

Obszar	Środki bezpieczeństwa
	i zapewnienie usług serwisowych świadczonych przez producentów i dystrybutorów. **Bezpieczeństwo serwerów.** Serwery służące do przetwarzania danych osobowych zabezpiecza się: (i) przed dostępem osób nieuprawnionych oraz systemów informatycznych przez zastosowanie bezpiecznych metod uwierzytelniania dostępu; (ii) przed dostępem osób nieuprawnionych, systemów informatycznych oraz utratą dostępności poprzez monitorowanie aktualności systemu operacyjnego i zainstalowanego oprogramowania, a także poprzez zastosowanie oprogramowania typu Firewall, Anty Virus (iii) przed utratą dostępności poprzez zastosowanie wirtualizacji i automatycznych procedur skalowania, zastosowanie automatycznych procesów monitorowania dostępności, obciążenia i wydajności, zastosowanie zapasowych źródeł zasilania oraz automatycznych procedur zmiany źródła zasilania, zastosowanie i zapewnienie usług serwisowych świadczonych przez producentów i dystrybutorów. **Bezpieczeństwo komputerów osobistych (stacjonarnych i przenośnych).** Komputery osobiste służące do przetwarzania danych osobowych zabezpiecza się: (i) przed dostępem osób nieuprawnionych poprzez zastosowanie bezpiecznych metod uwierzytelniania dostępu; (ii) przed dostępem osób nieuprawnionych oraz utratą dostępności poprzez monitorowanie aktualności systemu operacyjnego i zainstalowanego oprogramowania, zastosowanie oprogramowania typu Firewall, Anty Virus; (iii) przed utratą dostępności poprzez zastosowanie zapasowych źródeł zasilania oraz automatycznych procedur zmiany źródła zasilania, zastosowanie i zapewnienie usług serwisowych świadczonych przez producentów i dystrybutorów. Komputery osobiste służące do przetwarzania danych osobowych wyposaża się w nośniki danych zabezpieczone przy pomocy kryptograficznych środków ochrony danych. **Bezpieczeństwo sieci teleinformatycznych.** Sieci teleinformatyczne służące do przetwarzania danych osobowych zabezpiecza się: (i) przed dostępem nieuprawnionych osób oraz systemów informatycznych przez zastosowanie bezpiecznych metod uwierzytelniania dostępu; (ii) przed dostępem osób nieuprawnionych, systemów informatycznych oraz utratą dostępności poprzez zastosowanie oprogramowania typu Firewall, Intrusion Detection Systems, Intrusion Prevention Systems, Anty DDOS; (iii) przed utratą dostępności poprzez zastosowanie zwielokrotnienia łączy teleinformatycznych, zastosowanie automatycznych procesów monitorowania dostępności, obciążenia i wydajności, zastosowanie zapasowych źródeł zasilania urządzeń sieciowych oraz automatycznych procedur zmiany źródła zasilania, zastosowanie i zapewnienie usług serwisowych świadczonych przez producentów i dystrybutorów urządzeń sieciowych oraz dostawców łączy teleinformatycznych.