Wirtualna Polska Media S.A.
ul. Żwirki i Wigury 16
02-092 Warszawa
tel.: (+48 22) 57 63 900
fax: (+48 22) 57 63 901

Wykaz wdrożonych środków organizacyjnych i technicznych służących ochronie informacji, w tym danych osobowych

OBSZAR	OPIS ŚRODKA BEZPIECZEŃSTWA
Polityki bezpieczeństwa informacji	Został opracowany, zatwierdzony przez kierownictwo, opublikowany i zakomunikowany pracownikom oraz właściwym stronom zewnętrznym zbiór polityk ochrony danych osobowych (w tym m.in. polityka realizacji praw podmiotów danych, procedura postępowania z incydentem bezpieczeństwa, procedura wyboru procesora).
	Polityki ochrony danych osobowych są poddawane przeglądom w zaplanowanych odstępach czasu oraz wtedy, gdy wystąpią istotne zmiany.
	Została opracowana procedura nadawania uprawnień do przetwarzania danych osobowych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osób odpowiedzialnych za te czynności.
	Została opracowana procedura tworzenia i testowania kopii zapasowych zbiorów danych osobowych.
	Zostały opracowane zasady postępowania z komputerami przenośnymi (prywatne, służbowe).
	Została opracowana procedura rozpoczęcia, zawieszenia i zakończenia pracy przeznaczona dla użytkowników systemu informatycznego.
Organizacja bezpieczeństwa informacji	Została określona i przypisana odpowiedzialność za ochronę danych osobowych.
	Są utrzymywane stosowne kontakty z grupami zainteresowanych specjalistów lub innymi specjalistycznymi forami oraz stowarzyszeniami zawodowymi z obszaru bezpieczeństwa i ochrony danych osobowych.
	Wdrożono politykę oraz wspierające ją zabezpieczenia w celu ochrony informacji pobieranych, przetwarzanych i przechowywanych w miejscach wykonywania pracy zdalnej.
	Polityka stosowania urządzeń mobilnych uwzględnia ryzyko związane z pracą na mobilnych urządzeniach w niechronionych środowiskach.
	Ochrona danych osobowych jest uwzględniana w zarządzaniu projektami niezależnie od rodzaju projektu.

Wirtualna Polska Media S.A.
ul. Żwirki i Wigury 16
02-092 Warszawa
tel.: (+48 22) 57 63 900
fax: (+48 22) 57 63 901

Bezpieczeństwo zasobów ludzkich	Kierownictwo wymaga, aby wszyscy pracownicy i kontrahenci stosowali zasady ochrony danych osobowych zgodnie z obowiązującymi w organizacji politykami i procedurami.
	Wszyscy pracownicy organizacji oraz, w stosownych wypadkach, kontrahenci przechodzą stosowne kształcenie i szkolenie uświadamiające z zakresu ochrony danych osobowych oraz regularnie otrzymywać aktualizacje polityk i procedur związanych z bezpieczeństwem informacji na ich stanowiskach pracy.
Bezpieczeństwo fizyczne i środowiskowe	Wprowadzono politykę czystego biurka dla dokumentów papierowych i przenośnych nośników pamięci oraz politykę czystego ekranu dla środków przetwarzania informacji.
	Przed zbyciem lub przekazaniem sprzętu do ponownego użycia są sprawdzane wszystkie jego składniki zawierające nośniki informacji, dla zapewnienia, że wszystkie wrażliwe dane i licencjonowane programy zostały usunięte lub bezpiecznie nadpisane.
	Sprzęt umieszcza się i chroni w taki sposób, aby zredukować ryzyka wynikające z zagrożeń i niebezpieczeństw środowiskowych oraz okazje do nieuprawnionego dostępu.
	Sprzęt chroni się przed awariami zasilania oraz innymi przerwami dostaw spowodowanymi awariami systemów wspomagających.
	Określono granice bezpieczeństwa i wykorzystuje się je do zabezpieczenia obszarów zawierających wrażliwe lub krytyczne informacje oraz środki przetwarzania informacji.
	Zapewniono, że bezpieczne strefy są chronione odpowiednimi zabezpieczeniami wejść zapewniającymi dostęp wyłącznie osobom uprawnionym.
	Zaprojektowano i stosuje się fizyczne zabezpieczenia biur, pomieszczeń i obiektów.
	Zaprojektowano i stosuje się fizyczne zabezpieczenia przed katastrofami naturalnymi, wrogim atakiem lub wypadkami.
	Jest sprawowany nadzór nad punktami dostępu takimi jak obszary dostaw i załadunku oraz innymi punktami, przez które nieuprawnione osoby mogą wejść do pomieszczeń i jeśli to możliwe, izoluje się je od środków przetwarzania informacji, aby zapobiec nieuprawnionemu dostępowi.

Wirtualna Polska Media S.A.
ul. Żwirki i Wigury 16
02-092 Warszawa
tel.: (+48 22) 57 63 900
fax: (+48 22) 57 63 901

	Okablowanie zasilające oraz telekomunikacyjne, przenoszące dane lub wspomagające usługi informacyjne jest chronione przed przechwyceniem, przechwyceniem sygnału, zakłóceniem lub uszkodzeniem.
	Użytkownicy zapewniają odpowiednią ochronę sprzętu pozostawianego bez opieki.
Relacje z dostawcami	Uzgadnia się z dostawcą i udokumentowuje wymagania dotyczące ochrony danych osobowych celem zmniejszenia ryzyk związanych z dostępem dostawcy do aktywów organizacji.
Zarządzanie incydentami związanymi z bezpieczeństwem informacji	Pracownicy oraz kontrahenci korzystający z systemów i usług informacyjnych organizacji zostali zobowiązani do odnotowania i zgłaszania wszelkich zaobserwowanych lub podejrzewanych słabości związanych z bezpieczeństwem danych osobowych w systemach lub usługach.
	Wiedzę zdobytą podczas analizy i rozwiązywania incydentów związanych z ochroną danych osobowych wykorzystuje się do zredukowania prawdopodobieństwa wystąpienia lub skutków przyszłych incydentów.
	Ustanowiono odpowiedzialność kierownictwa oraz procedury zapewniające szybką, skuteczną i zorganizowaną reakcję na incydenty związane z bezpieczeństwem danych osobowych.
	Organizacja określiła i stosuje procedury identyfikacji, gromadzenia, pozyskiwania i utrwalania informacji, które mogą stanowić materiał dowodowy.
	Zdarzenia związane z bezpieczeństwem danych osobowych są zgłaszane odpowiednimi kanałami zarządczymi tak szybko, jak tylko to jest możliwe.
	Zdarzenia związane z bezpieczeństwem danych osobowych są oceniane i są podejmowane decyzje w sprawie zakwalifikowania ich jako incydentów lub naruszeń ochrony danych osobowych.
	Reakcja na incydenty związane z bezpieczeństwem danych osobowych są zgodne z udokumentowanymi procedurami
Kontrola dostępu	Użytkownicy mają dostęp wyłącznie do tych sieci i usług sieciowych, do których otrzymali wyraźne uprawnienia.
	W celu umożliwienia przydzielania praw dostępu wdrożono formalny proces rejestrowania i wyrejestrowywania użytkowników.

Wirtualna Polska Media S.A.
ul. Żwirki i Wigury 16
02-092 Warszawa
tel.: (+48 22) 57 63 900
fax: (+48 22) 57 63 901

	Wdrożono formalny proces przydzielania dostępu użytkownikom w celu nadawania lub odbierania praw dostępu do wszystkich systemów i usług wszystkim kategoriom użytkowników.
	Przydzielanie i wykorzystanie praw uprzywilejowanego dostępu jest ograniczone i nadzorowane.
	Przydzielanie poufnych informacji uwierzytelniających powinno podlegać formalnemu procesowi zarządzania.
	Przegląd praw dostępu użytkowników w zakresie sprzętu i oprogramowania użytkownika, takie jak tablety, przeglądarki internetowe, telewizory z dostępem do Internetu itp., komputery przekaźniki telekomunikacyjne, napędy USB, dyski twarde itp.
	Przydzielone pracownikom i użytkownikom zewnętrznym prawa dostępu do informacji i środków przetwarzania informacji są odbierane po zakończeniu zatrudnienia, umowy lub porozumienia lub są dostosowywane do zaistniałych zmian.
	Użytkownicy mają obowiązek przestrzegania przyjętych w organizacji zasad stosowania poufnych informacji uwierzytelniających (polityka haseł).
	Dostęp do informacji oraz funkcji systemu aplikacyjnego jest ograniczony zgodnie z Polityką kontroli dostępu
	Dostęp do kodu źródłowego programów jest ograniczony.
	Tam, gdzie polityka kontroli dostępu tego wymaga, dostęp do systemów i aplikacji jest kontrolowany przez procedurę bezpiecznego logowania.
	Systemy zarządzania hasłami są interaktywne i zapewniają wybór haseł dobrej jakości.
Zarządzanie aktywami	Inwentaryzacja aktywów w zakresie sprzętu użytkownika, takie jak tablety, przeglądarki internetowe, telewizory z dostępem do Internetu itp. oraz oprogramowanie użytkownika takie jak systemy operacyjne, komunikatory, bazy danych, aplikacje biznesowe itp. oraz kanały łączności komputerowej: przewodowe, bezprzewodowe, światłowodowe itp.
	Określona została własność aktywów w zakresie sprzętu użytkownika takiego jak smartfony, tablety, przeglądarki internetowe, telewizory z dostępem do Internetu itp. oraz oprogramowanie użytkownika takie jak systemy operacyjne, komunikatory, bazy danych, aplikacje biznesowe itp. oraz kanały łączności komputerowej: przewodowe, bezprzewodowe, światłowodowe itp.
	Nośniki, które nie będą dłużej wykorzystywane, są bezpiecznie wycofywane, zgodnie z formalnymi procedurami.

Wirtualna Polska Media S.A.
ul. Żwirki i Wigury 16
02-092 Warszawa
tel.: (+48 22) 57 63 900
fax: (+48 22) 57 63 901

	Nośniki zawierające informacje są chronione przed nieuprawnionym dostępem, nadużyciem oraz utratą integralności podczas transportu.
	Zidentyfikowano aktywa związane z informacjami i środkami przetwarzania informacji oraz sporządzono i utrzymuje się ewidencję tych aktywów.
	Wszyscy pracownicy i użytkownicy podmiotów zewnętrznych, w momencie zakończenia zatrudnienia, umowy lub porozumienia, powinni zwrócić wszystkie posiadane aktywa organizacji.
Bezpieczna eksploatacja	Monitoruje się i dostosowuje wykorzystanie zasobów oraz przewiduje wymaganą pojemność w przyszłości, dla zapewnienia właściwej wydajności systemu.
	Zapasowe kopie informacji, oprogramowania i obrazów systemów są regularnie wykonywane i testowane, zgodnie z ustaloną polityką kopii zapasowych.
	Zegary wszystkich istotnych systemów przetwarzania informacji w organizacji lub domenie bezpieczeństwa są zsynchronizowane z jednym wzorcowym źródłem czasu.
	Wdrożono procedury nadzoru nad instalacją oprogramowania w systemach produkcyjnych.
	Informacje o podatnościach technicznych wykorzystywanych systemów informacyjnych są niezwłocznie pozyskiwane, dokonuje się oceny stopnia narażenia organizacji na te podatności i podejmuje odpowiednie środki w celu przeciwdziałania związanemu z nimi ryzyku.
	Oddziela się środowiska deweloperskie, testowe i produkcyjne celem redukcji ryzyk związanych z nieuprawnionym dostępem lub zmianami w środowisku produkcyjnym.
	Wdrożono zabezpieczenia wykrywające, zapobiegające i odtwarzające, które służą ochronie przed szkodliwym oprogramowaniem, w połączeniu z właściwym uświadamianiem użytkowników.
	Środki służące rejestrowaniu zdarzeń oraz informacje w dziennikach zdarzeń są chronione przed manipulacją i nieuprawnionym dostępem.
Aspekty bezpieczeństwa informacji w zarządzaniu ciągłością działania	Organizacja określiła wymagania dotyczące ochrony danych osobowych i ciągłości zarządzania bezpieczeństwem informacji w niekorzystnych sytuacjach np. w czasie kryzysu lub katastrofy.
	Podejście organizacji do zarządzania bezpieczeństwem ochrony danych osobowych oraz jego wdrożenie (tzn. cele stosowania zabezpieczeń, zabezpieczenia polityki, procesy i procedury dotyczące ochrony danych osobowych) jest poddawane niezależnemu przeglądowi w zaplanowanych odstępach czasu lub wtedy, gdy nastąpią istotne zmiany.

Wirtualna Polska Media S.A.
ul. Żwirki i Wigury 16
02-092 Warszawa
tel.: (+48 22) 57 63 900
fax: (+48 22) 57 63 901

	Środki przetwarzania informacji są wdrażane z nadmiarem wystarczającym do spełnienia wymagań dostępności. Redundancja.
	Organizacja ustanowiła, udokumentowała, wdrożyła i utrzymuje procesy, procedury i zabezpieczenia dla zapewnienia w niekorzystnej sytuacji wymaganego poziomu ciągłości ochrony danych osobowych.
Pozyskiwanie, rozwój i utrzymanie systemów	Ustanowiono zasady prac nad rozwojem oprogramowania i systemów oraz stosuje się je w pracach rozwojowych prowadzonych wewnątrz organizacji.
	Nadzoruje się zmiany w systemach podczas ich cyklu rozwojowego przy użyciu formalnych procedur kontroli zmian.
	Ustanowiono, udokumentowano i utrzymuje się zasady projektowania bezpiecznych systemów oraz stosuje się je do wszystkich prac implementacyjnych nad systemami informacyjnymi.
	Organizacja nadzoruje i monitoruje prace rozwojowe nad systemami zlecone podmiotom zewnętrznym.
	Informacje przesyłane w sieciach publicznych, związane z usługami świadczonymi przez aplikacje, są chronione przed nieuczciwymi działaniami oraz z nieuprawnionym ujawnieniem i zmianami.
Bezpieczeństwo komunikacji	Wdrożono formalne polityki przesyłania informacji, procedury i zabezpieczenia, w celu ochrony wymiany informacji, przesyłanych przy użyciu wszystkich rodzajów środków łączności.
	Sieci są zarządzane i nadzorowane, w celu ochrony informacji, w tym danych osobowych, w systemach i aplikacjach.
	Umowy dotyczące wszystkich usług sieciowych, świadczonych wewnętrznie lub zlecanych na zewnątrz, zawierają zidentyfikowane mechanizmy zabezpieczeń, poziomy świadczenia usług i wymagania dotyczące zarządzania.
	Informacje, w szczególności dane osobowe, przekazywane w formie wiadomości elektronicznych, są odpowiednio chronione.