Polityka bezpieczeństwa informacji

Mice Media Sp z o. o.

(Nazwa firmy)

28.02.2019

Data

Spis treści

1. Wprowadzenie 3
2. Polityka bezpieczeństwa informacji 3
3. Polityka dozwolonego użytku 5
4. Kroki dyscyplinarne 5
5. Ochrona przechowywanych danych 5
6. Klasyfikacja informacji 6
7. Dostęp do poufnych danych właścicieli kart 6
8. Bezpieczeństwo fizyczne 7
9. Ochrona danych podczas przesyłania 8
10. Usuwanie przechowywanych danych 9
11. Świadomość i procedury bezpieczeństwa 9
12. Bezpieczeństwo sieci 10
13. System i polityka haseł 11
14. Polityka antywirusowa 12
15. Polityka zarządzania poprawkami 13
16. Polityka dostępu zdalnego 13
17. Polityka zarządzania podatnościami 14
18. Standardy konfiguracji: 14
19. Proces kontroli zmian 15
20. Kontrola i przegląd dziennika 16
21. Wytwarzanie bezpiecznych aplikacji 19
22. Metodologia testów penetracyjnych 20
23. Plan reagowania na incydenty 23
24. Role i obowiązki 25
25. Dostęp niezależnych podmiotów do danych właścicieli kart 26
26. Zarządzanie dostępem użytkowników 26
27. Polityka kontroli dostępu 27
28. Polityka bezprzewodowego dostępu 28

Załącznik A 30

Załącznik B..... 31

1. Wprowadzenie

Niniejszy dokument dotyczący polityki bezpieczeństwa informacji obejmuje wszelkie aspekty bezpieczeństwa dotyczące informacji poufnych o firmie i musi zostać przekazany wszystkim pracownikom firmy. Wszyscy pracownicy firmy muszą zapoznać się w całości z tym dokumentem i podpisać oświadczenie potwierdzające zapoznanie się z niniejszą polityką i całkowite jej zrozumienie. Niniejszy dokument będzie poddawany weryfikacji i aktualizacji przez Zarząd corocznie lub gdy jest to istotne dla włączenia nowo opracowanych standardów bezpieczeństwa do tej polityki i przekazania ich wszystkim pracownikom i odpowiednim zleceniobiorcom.

2. Polityka bezpieczeństwa informacji

MICE MEDIA SP Z O. O. przetwarza codziennie poufne informacje właścicieli kart. Informacje poufne muszą posiadać odpowiednie zabezpieczenia w celu ich ochrony, ochrony prywatności właścicieli kart, zapewnienia zgodności z różnymi przepisami i zabezpieczenia przyszłości organizacji.

MICE MEDIA SP Z O. O. zobowiązuje się do poszanowania prywatności wszystkich swoich klientów oraz do ochrony wszelkich danych o klientach przed podmiotami zewnętrznymi. W tym celu kierownictwo jest zobowiązane do zachowania bezpiecznego środowiska, w którym mają być przetwarzane informacje o właścicielu karty, dzięki czemu możemy dotrzymać tych obietnic.

Pracownicy zajmujący się przetwarzaniem poufnych danych właścicieli kart powinni zapewnić następujące środki bezpieczeństwa:

- Przetwarzać informacje o Firmie i właścicielach kart w sposób odpowiadający ich poufności;
- Ograniczyć korzystanie z systemów informatycznych i telekomunikacyjnych MICE MEDIA SP Z O. O. w celach prywatnych oraz zapewnić, aby nie kolidowało ono z wykonywaniem obowiązków zawodowych;
- MICE MEDIA SP Z O. O. **(dalej nazywana firmą)** zastrzega sobie prawo do monitorowania, uzyskiwania dostępu, dokonywania oceny, przeprowadzania audytu, kopiowania, przechowywania i usuwania wszelkich usług łączności elektronicznej, urządzeń, systemów i ruchu sieciowego w dowolnym celu;
- Nie wykorzystywać poczty elektronicznej, Internetu ani innych zasobów Firmy do prowadzenia jakichkolwiek działań mających obraźliwy, stanowiący zagrożenie, dyskryminujący, niezgodny ze stanem faktycznym, oszczerczy, pornograficzny, obsceniczny, napastliwy lub niezgodny z prawem charakter;
- Nie ujawniać informacji o personelu bez upoważnienia;
- Chronić poufne informacje właścicieli kart;
- Przechowywać hasła i konta w bezpieczny sposób;
- Wystąpić do kierownictwa z prośbą o wyrażenie zgody przed nawiązaniem połączeń z nowym oprogramowaniem lub sprzętem, zewnętrznym podmiotem itd.;
- Nie instalować nieautoryzowanego oprogramowania ani sprzętu, w tym modemów i punktów dostępu bezprzewodowego, bez uzyskania wyraźnej zgody ze strony kierownictwa;
- Zawsze pozostawiać biurka bez poufnych danych właścicieli kart oraz ustawiać blokady ekranów komputerów w przypadku pozostawienia ich bez nadzoru;
- Incydenty związane z bezpieczeństwem informacji należy zgłaszać bezzwłocznie osobie odpowiedzialnej za lokalne reagowanie na zdarzenia — należy dowiedzieć się, kim jest ta osoba.

Każdy z nas ma obowiązek zabezpieczenia systemów i danych firmy przed nieupoważnionym dostępem i niewłaściwym wykorzystaniem. W przypadku niejasności co do zasad przedstawionych w niniejszym dokumencie należy zasięgnąć porad i wskazówek od swojego bezpośredniego przełożonego.

3. Polityka dozwolonego użytku

Intencją opublikowania przez kierownictwo Polityki dozwolonego użytku nie jest nałożenie ograniczeń stojących w sprzeczności z ugruntowaną w Firmie kulturą otwartości, zaufania i uczciwości. Kierownictwo jest zobowiązane do ochrony pracowników, partnerów i Firmy przed niezgodnymi z prawem lub szkodliwymi działaniami ze strony osób — świadomymi lub nieświadomymi. Firma będzie prowadzić zatwierdzony wykaz technologii i urządzeń oraz pracowników mających dostęp do takich urządzeń wymienionych w Załączniku B.

- Pracownicy są odpowiedzialni za dokonywanie właściwej oceny co do zasadności użytku osobistego.
- Pracownicy powinni upewnić się, że posiadają odpowiednie dane uwierzytelniające i są uwierzytelnieni do korzystania z technologii.
- Pracownicy powinni podjąć wszelkie niezbędne kroki, aby zapobiec nieupoważnionemu dostępowi do poufnych danych obejmujących dane właścicieli kart.
- Pracownicy powinni zadbać o to, aby technologie były wykorzystywane i konfigurowane w dozwolonych lokalizacjach sieciowych.
- Przechowywać hasła w bezpieczny sposób i nie udostępniać kont.
- Uprawnieni użytkownicy są odpowiedzialni za bezpieczeństwo swoich haseł i kont.
- Wszystkie komputery stacjonarne, komputery przenośne i stacje robocze powinny być zabezpieczone za pomocą wygaszacza ekranu chronionego hasłem z funkcją automatycznej aktywacji.
- Wszystkie terminale POS i urządzenia do wprowadzania kodu PIN powinny być odpowiednio chronione i zabezpieczone w taki sposób, aby nie można było przy nich manipulować ani ich modyfikować.
- Informacje zawarte na komputerach przenośnych są szczególnie podatne na zagrożenia, dlatego należy zachować szczególną ostrożność.
- Posty wysyłane przez pracowników z adresu e-mail Firmy na grupy dyskusyjne powinny zawierać zastrzeżenie o zrzeczeniu się odpowiedzialności stwierdzające, że wyrażone opinie są wyłącznie opiniami ich autorów i nie muszą stanowić opinii Firmy, chyba że zamieszczenie postu odbywa się w trakcie pełnienia obowiązków służbowych.
- Pracownicy muszą zachować szczególną ostrożność podczas otwierania załączników e-mail otrzymanych od nieznanych nadawców, które mogą zawierać wirusy, bomby pocztowe lub kod konia trojańskiego.

4. Kroki dyscyplinarne

Naruszenie standardów, zasad lub procedur przedstawionych w niniejszym dokumencie przez pracownika skutkuje podjęciem kroków dyscyplinarnych, od ostrzeżeń lub upomnień aż do rozwiązania stosunku pracy włącznie. Roszczenia z tytułu niewiedzy, dobrych intencji lub dokonania złej oceny sytuacji nie będą wykorzystywane jako pretekst do niewypełnienia zobowiązań.

5. Ochrona przechowywanych danych

- Wszystkie poufne dane właścicieli kart przechowywane i przetwarzane przez Firmę i jej pracowników muszą być przez cały czas skutecznie zabezpieczone przed nieupoważnionym wykorzystaniem. Wszelkie poufne dane kart, które nie są już wymagane przez Firmę z powodów

biznesowych, należy usunąć w bezpieczny i nieodwracalny sposób.

- Jeśli nie istnieje szczególna potrzeba wyświetlania pełnego numeru PAN (numer konta stałego), należy go zamaskować przy wyświetlaniu.
- Numerów PAN, które nie są chronione we wspomniany wyżej sposób, nie należy wysyłać do sieci zewnętrznej przy użyciu technologii przesyłu wiadomości do użytkownika końcowego, takich jak czaty, komunikator ICQ itd.

Zabrania się przechowywania:

1. Zawartości paska magnetycznego karty płatniczej (dane ścieżek) na jakichkolwiek nośnikach.
2. Kodu CVV/CVC (3- lub 4-cyfrowy numer na pasku podpisu na odwrocie karty płatniczej) na jakichkolwiek nośnikach.
3. Pod żadnym pozorem kodu PIN lub szyfrowanego bloku PIN.

6. Klasyfikacja informacji

Dane i nośniki zawierające dane muszą być zawsze oznakowane, wskazując poziom poufności.

- **Poufne dane** mogą obejmować zasoby informacyjne, w przypadku których istnieją wymogi prawne dotyczące zapobiegania ujawnieniu lub kar finansowych za ujawnienie, i dane, które mogłoby wyrządzić poważne szkody Firmie w przypadku ich ujawnienia lub modyfikacji. **Do poufnych danych należą dane właścicieli kart**.
- **Dane do użytku wewnętrznego** mogą obejmować informacje, które w opinii właściciela powinny być chronione, aby zapobiec nieupoważnionemu ujawnieniu;
- **Dane publiczne** to informacje, które mogą być rozpowszechniane w dowolny sposób.

7. Dostęp do poufnych danych właścicieli kart

Każdy dostęp do poufnych danych właścicieli kart powinien być kontrolowany i autoryzowany. Wszelkie obowiązki zawodowe wymagające dostępu do danych właścicieli kart powinny być wyraźnie określone.

- Każdy ekran właściciela karty powinien być ograniczony do co najmniej 6 pierwszych i 4 ostatnich cyfr danych właściciela karty.
- Prawa dostępu do identyfikatora uprzywilejowanego użytkownika powinny być ograniczone do najmniejszych uprawnień niezbędnych do wykonywania obowiązków zawodowych.
- Uprawnienia powinny być przyznawane osobom na podstawie klasyfikacji zawodowej i funkcji (kontrola dostępu oparta na rolach).
- Dostęp do poufnych informacji właścicieli kart, takich jak numer PAN, dane osobowe i dane biznesowe jest ograniczony do pracowników mających uzasadnioną potrzebę przejrzenia takich informacji.
- Żadni inni pracownicy nie mogą mieć dostępu do tych poufnych danych, chyba że mają prawdziwą potrzebę biznesową.

- W przypadku udostępnienia danych właściciela karty Dostawcy usług (podmiot zewnętrzny) prowadzony będzie wykaz takich Dostawców usług wymieniony w Załączniku B.
- Firma sporządzi pisemną umowę zawierającą potwierdzenie odpowiedzialności Dostawcy usług za dane właścicieli kart, którymi będzie dysponować.
- Firma zadba o to, aby przed skorzystaniem z usług Dostawcy usług przeprowadzona została ustalona procedura, w tym odpowiednia analiza przedinwestycyjna.
- Firma przeprowadzi procedurę monitorowania statusu zgodności Dostawcy usług ze standardem PCI DSS.

8. Bezpieczeństwo fizyczne

Dostęp do poufnych informacji w postaci nośników zarówno sprzętowych, jak i programowych należy ograniczyć fizycznie, aby uniemożliwić nieupoważnionym osobom uzyskanie poufnych danych.

- Pracownicy są odpowiedzialni za dokonywanie właściwej oceny co do zasadności użytku osobistego.
- Pracownicy powinni upewnić się, że posiadają odpowiednie dane uwierzytelniające i są uwierzytelnieni do korzystania z technologii.
- Pracownicy powinni podjąć wszelkie niezbędne kroki, aby zapobiec nieupoważnionemu dostępowi do poufnych danych obejmujących dane właścicieli kart.
- Pracownicy powinni zadbać o to, aby technologie były wykorzystywane i konfigurowane w dozwolonych lokalizacjach sieciowych.
- Należy prowadzić wykaz urządzeń akceptujących dane kart płatniczych.
- Na wykazie tym powinny znajdować się marka, model i lokalizacja urządzenia.
- Wykaz powinien zawierać numer seryjny lub unikatowy identyfikator urządzenia.
- Wykaz powinien być aktualizowany w przypadku dodania, usunięcia lub zmiany lokalizacji urządzeń.
- Urządzenia POS powinny być okresowo sprawdzane w celu wykrycia prób manipulacji lub zamiany.
- Pracownicy korzystający z tych urządzeń powinni być przeszkoleni i zdawać sobie sprawę ze sposobu obsługi urządzeń POS.
- Pracownicy korzystający z tych urządzeń powinni sprawdzić tożsamość wszystkich pracowników zewnętrznych podających się za osoby wykonujące naprawy lub zadania związane z utrzymaniem urządzeń, instalację nowych urządzeń lub wymianę urządzeń.
- Pracownicy korzystający z tych urządzeń powinni być przeszkoleni w zakresie zgłaszania podejrzanych zachowań i śladów manipulacji przy urządzeniach odpowiednim pracownikom.
- „Odwiedzający" jest określany jako sprzedawca, gość pracownika, pracownik zajmujący się utrzymaniem lub każdy, kto musi wejść na krótki czas na teren siedziby, zwykle nie dłużej niż jeden dzień.
- Przechowywać hasła w bezpieczny sposób i nie udostępniać kont. Uprawnieni użytkownicy są odpowiedzialni za bezpieczeństwo swoich haseł i kont.
- Nośniki są określane jako dowolne drukowane lub wypisane ręcznie notatki na papierze, odebrane faksy, dyskietki, taśmy z kopiami zapasowymi, komputerowy dysk twardy itd.
- Nośniki zawierające poufne informacje właścicieli kart muszą być przetwarzane i rozpowszechniane w bezpieczny sposób przez zaufane osoby.

- Odwiedzającym musi zawsze towarzyszyć zaufany pracownik podczas przebywania w miejscach, w których przechowywane są poufne informacje właścicieli kart.
- Konieczne jest wdrożenie procedur ułatwiających wszystkim pracowników odróżnienie pracowników od odwiedzających, zwłaszcza w miejscach, w których możliwy jest dostęp do danych właścicieli kart. Określenie „Pracownik" odnosi się do pracowników pełnoetatowych i niepełnoetatowych, pracowników tymczasowych i personelu tymczasowego oraz konsultantów, którzy są „gośćmi" w siedzibach Firmy. „Odwiedzający" jest określany jako sprzedawca, gość pracownika, pracownik zajmujący się utrzymaniem lub każdy, kto musi wejść na krótki czas na teren siedziby, zwykle nie dłużej niż jeden dzień.
- Gniazda sieciowe znajdujące się w miejscach publicznych i miejscach dostępnych dla odwiedzających muszą być wyłączone lub włączone w przypadku udzielenia wyraźnego zezwolenia na dostęp do sieci.
- Wszystkie terminale POS i urządzenia do wprowadzania kodu PIN powinny być odpowiednio chronione i zabezpieczone w taki sposób, aby nie można było przy nich manipulować ani ich modyfikować.
- Prowadzona jest ścisła kontrola nad rozpowszechnianiem wewnętrznym i zewnętrznym wszelkich nośników zawierających dane właścicieli kart, które wymaga zatwierdzenia przez kierownictwo.
- Prowadzona jest ścisła kontrola nad przechowywaniem i dostępnością nośników.
- Na wszystkich komputerach przechowujących poufne dane właścicieli kart musi być włączony wygaszacz ekranu chroniony hasłem, aby zapobiec ich nieupoważnionemu wykorzystaniu.

9. Ochrona danych podczas przesyłania

Wszystkie poufne dane właścicieli kart muszą być skutecznie zabezpieczone w przypadku przesyłania ich drogą fizyczną lub elektroniczną.

- Danych właścicieli kart (numer PAN, dane ścieżek itd.) nie wolno przesyłać przez Internet za pośrednictwem poczty elektronicznej, czatu do przesyłania wiadomości błyskawicznych ani innych technologii przesyłania wiadomości do użytkownika końcowego.
- Jeżeli przesłanie danych właściciela karty za pośrednictwem poczty elektronicznej, przez Internet lub innymi sposobami jest uzasadnione biznesowo, należy go dokonać po uzyskaniu autoryzacji i przy użyciu silnego mechanizmu szyfrowania (tj. szyfrowania AES, szyfrowania z użyciem klucza PGP, protokołu IPSEC, technologii GSM, technologii GPRS, technologii bezprzewodowych itd).
- Transport nośników zawierających poufne dane właścicieli kart do innej lokalizacji musi zostać zatwierdzony przez kierownictwo, zarejestrowany i zinwentaryzowany przed opuszczeniem terenu siedziby. Przy transporcie takich nośników można korzystać wyłącznie z bezpiecznych usług kurierskich. Status przesyłki należy monitorować do momentu dostarczenia jej do nowej lokalizacji.
- UŻYTKOWNICY TALECH ORAZ MOBILE MERCHANT Bezpieczeństwo płatności jest ściśle powiązane z połączeniem danych mobilnych urządzenia użytkownika, ponieważ połączenie to jest wykorzystywane do przesyłania danych płatniczych. Korzystanie z aplikacji podczas połączenia z publiczną siecią Wi-Fi zagraża bezpieczeństwu transmisji, ponieważ nie ma możliwości zagwarantowania, że wspomniane połączenie Wi-Fi zostało odpowiednio zabezpieczone przed kradzieżą danych oraz ich wykorzystaniem. W przypadku korzystania z własnego połączenia Wi-Fi do wysyłania danych transakcji należy upewnić się, że jest poprawnie skonfigurowane i zabezpieczone oraz odpowiedzieć na odpowiednie pytania SAQ C.

10. Usuwanie przechowywanych danych

- Wszystkie dane należy bezpiecznie usunąć, gdy nie będą już potrzebne Firmie, niezależnie od rodzaju nośników lub aplikacji, w których są przechowywane.
- Należy zapewnić automatyczny proces usuwania niepotrzebnych już danych w sieci.
- Wszystkie wydruki z danymi właścicieli kart należy zniszczyć ręcznie, gdy nie będą już potrzebne z ważnych i uzasadnionych powodów biznesowych. Konieczne jest wdrożenie procesu wykonywanego co kwartał pozwalającego potwierdzić, że wszystkie nieelektroniczne dane właścicieli kart zostały właściwie usunięte w odpowiednim czasie.
- Firma dysponuje procedurami niszczenia materiałów w postaci drukowanej (papierowej). Wymagają one, aby wszystkie materiały w postaci drukowanej były niszczone dwukierunkowo w niszczarce, palone lub przetwarzane na masę celulozową w taki sposób, aby nie można było ich odtworzyć.
- Firma będzie dysponowała udokumentowanymi procedurami niszczenia nośników elektronicznych. Będą one wymagać następujących środków bezpieczeństwa:
    - Wszystkie dane właścicieli kart na nośnikach elektronicznych muszą być kasowane w sposób nieodwracalny, np. przez rozmagnesowanie lub wymazywanie elektroniczne z zastosowaniem bezpiecznych procedur kasowania klasy wojskowej lub fizycznego niszczenia nośników;
    - W przypadku korzystania z programów do bezpiecznego wymazywania procedura ta musi określać uznane w branży standardy bezpiecznego kasowania.
- Wszystkie informacje właścicieli kart oczekujące na zniszczenie należy przechowywać w zamykanych pojemnikach do przechowywania wyraźnie oznaczonych jako „Przeznaczone do zniszczenia” — należy ograniczyć dostęp do tych pojemników.

11. Świadomość i procedury bezpieczeństwa

Opisane poniżej zasady i procedury należy uwzględnić w działalności firmy w celu zachowania wysokiego stopnia świadomości bezpieczeństwa. Ochrona poufnych danych wymaga regularnego szkolenia wszystkich pracowników i kontrahentów.

- Dokonać oceny procedur przetwarzania poufnych informacji i organizować regularne spotkania poświęcone świadomości bezpieczeństwa w celu uwzględnienia tych procedur w codziennej działalności firmy.
- Przekazać niniejszy dokument dotyczący polityki bezpieczeństwa wszystkim pracowników do przeczytania. Wymagane jest, aby wszyscy pracownicy potwierdzili zrozumienie treści niniejszego dokumentu dotyczącego polityki bezpieczeństwa, podpisując formularz potwierdzenia (patrz Załącznik A).
- Wszyscy pracownicy zajmujący się przetwarzaniem poufnych informacji zostaną poddani kontrolom przeszłości (takim jak kontrole wpisów w rejestrach kryminalnych i kredytowych, w granicach miejscowego prawa) przed rozpoczęciem zatrudnienia w Firmie.
- Wszystkie podmioty zewnętrzne mające dostęp do numerów rachunków kart kredytowych są zobowiązane umową do przestrzegania standardów bezpieczeństwa stowarzyszeń kart płatniczych (PCI/DSS).
- Polityka bezpieczeństwa Firmy musi być poddawana corocznej ocenie i aktualizowana w miarę potrzeb.

12. Bezpieczeństwo sieci

- Dla każdego połączenia z Internetem należy wprowadzić zapory oraz dowolną strefę zdemilitaryzowaną i wewnętrzną sieć firmową.
- Należy prowadzić i sprawdzać co 6 miesięcy diagram sieci ze szczegółowymi informacjami o wszystkich połączeniach przychodzących i wychodzących.
- Należy prowadzić dokumentację zapór sieciowych i routerów zawierającą udokumentowany wykaz usług, protokołów i portów, łącznie z uzasadnieniem biznesowym.
- Konfiguracje routerów i zapór muszą ograniczać połączenia między sieciami niezaufanymi a wszelkimi systemami w środowisku przetwarzania danych właścicieli kart.
- Należy wprowadzić technologię zapór z analizą stanów połączeń w lokalizacjach, w których Internet łączy się z siecią kart Firmy w celu ograniczenia znanych i stałych zagrożeń. Należy również wprowadzić zapory chroniące lokalne segmenty sieci i zasoby informatyczne dołączone do tych segmentów, takie jak sieci firmowe i sieci otwarte.
- Wszystkie połączenia przychodzące i wychodzące należy ograniczyć do połączeń wymaganych w środowisku przetwarzania danych właścicieli kart.
- Wszystkie przychodzące połączenia sieciowe są domyślnie blokowane, o ile nie są wyraźnie dozwolone, a ograniczenia w tym zakresie muszą być udokumentowane.
- Wszystkie połączenia wychodzące muszą być zatwierdzone przez kierownictwo (tzn. witryny z białej listy, które mogą być odwiedzane przez pracowników), a ograniczenia w tym zakresie muszą być udokumentowane.
- Firma będzie stosować zapory między dowolnymi sieciami bezprzewodowymi a środowiskiem przetwarzania danych właścicieli kart.
- Firma podda kwarantannie użytkowników sieci bezprzewodowych wchodzących do strefy zdemilitaryzowanej, w której będą oni poddawani uwierzytelnianiu i blokowani przez zaporę tak, jak gdyby przychodzili z Internetu.
- Ujawnianie prywatnych adresów IP podmiotom zewnętrznym wymaga uzyskania zgody.
- Topologia środowiska zapory musi być udokumentowana i aktualizowana zgodnie ze zmianami w sieci.
- Reguły zapory będą poddawane ocenie co sześć miesięcy w celu zapewnienia ich poprawności. Zapora musi ponadto zawierać regułę czyszczenia na końcu bazy reguł.
- Firma musi poddawać kwarantannie użytkowników sieci bezprzewodowych wchodzących do strefy zdemilitaryzowanej, w której zostali oni poddani uwierzytelnianiu i zablokowani przez zaporę tak, jak gdyby przyszli z Internetu.
- Nie będą dozwolone żadne bezpośrednie połączenia z Internetu ze środowiskiem przetwarzania danych właścicieli kart. Cały ruch musi przechodzić przez zaporę.

Reguły	Źródłowy adres IP	Docelowy adres IP	Działanie

13. System i polityka haseł

Wszyscy użytkownicy, w tym kontrahenci i dostawcy mający dostęp do systemów Firmy są odpowiedzialni za podjęcie odpowiednich kroków, opisanych poniżej, w celu wybrania i zabezpieczenia swoich haseł.

- Standard konfiguracji systemów musi być opracowany według uznanych w branży standardów ograniczenia funkcjonalności (SANS, NIST, ISO).
- Konfiguracje systemowe powinny być aktualizowane w miarę rozpoznawania nowych problemów (jak określono w wymaganiu 6.1 standardu PCI DSS).
- Konfiguracje systemowe muszą zawierać powszechnie znane ustawienia parametrów bezpieczeństwa.
- Standard konfiguracji systemów powinien być stosowany we wszystkich nowo skonfigurowanych systemach.
- W momencie włączenia systemu/urządzenia do sieci Firmy należy zmienić wszystkie domyślne konta i hasła dostawców w systemach oraz wyłączyć niepotrzebne usługi i konta użytkowników/systemowe.
- Wszystkie niepotrzebne konta domyślne należy usunąć lub wyłączyć przed zainstalowaniem systemu w sieci.
- Ustawienia parametrów bezpieczeństwa należy odpowiednio ustawić w składnikach systemowych.
- Wszystkie niepotrzebne funkcje (skrypty, sterowniki, funkcje, podsystemy, systemy plików, serwery sieci Web itd.) należy usunąć.
- Wszystkie nieużywane przez system, niepotrzebne usługi, protokoły, demony itd. należy wyłączyć.
- Wszelkie niezabezpieczone protokoły, demony, usługi znajdujące się w użyciu muszą być udokumentowane i uzasadnione.
- Wszyscy użytkownicy mający dostęp do danych właścicieli kart muszą mieć unikatowy identyfikator.
- Wszyscy użytkownicy muszą użyć hasła, aby uzyskać dostęp do sieci firmowej lub dowolnych innych zasobów elektronicznych.
- Wszystkie identyfikatory byłych użytkowników należy bezzwłocznie dezaktywować lub usunąć.
- Identyfikator użytkownika zostanie zablokowany w przypadku wystąpienia więcej niż 5 nieudanych prób. Zablokowane konto może zostać włączone jedynie przez administratora systemu. Zablokowane konta użytkowników zostaną wyłączone na okres co najmniej 30 minut lub do momentu włączenia konta przez administratora.
- Wszystkie hasła na poziomie systemu i użytkownika należy zmieniać na co najmniej raz na kwartał.
- Należy wprowadzić funkcję zapamiętywania historii co najmniej czterech ostatnich haseł.
- Należy skonfigurować unikatowe hasło dla nowych użytkowników i użytkowników proszonych o zmianę hasła przy pierwszym logowaniu.
- Nie wolno używać uwierzytelniania za pomocą grupowych, udostępnionych lub standardowych kont lub haseł użytkownika ani innych metod uwierzytelniania do zarządzania składnikami

systemowymi.

- W lokalizacjach wykorzystujących protokół SNMP należy zdefiniować ciąg identyfikacyjny inny niż standardowe ciągi domyślne „publiczny”, „prywatny” i „systemowy” oraz różniący się od haseł używanych do logowania interaktywnego.
- We wszystkich metodach uzyskiwania dostępu administracyjnego bez użycia konsoli wykorzystywane będą odpowiednie technologie, takie jak SSH, VPN itd. Ewentualnie przed żądaniem podania hasła administratora wywoływany będzie mechanizm silnego szyfrowania.
- Usługi i parametry systemowe zostaną skonfigurowane w sposób uniemożliwiający korzystanie ze słabo zabezpieczonych technologii, takich jak Telnet i innych niebezpiecznych poleceń zdalnego logowania.
- Dostęp administratora do interfejsów zarządzania opartych na sieci Web jest szyfrowany za pomocą silnego szyfrowania.
- Odpowiedzialność za wybór hasła trudnego do odgadnięcia na ogół spoczywa zazwyczaj na użytkownikach. Silne hasło musi:

a) Być możliwie jak najdłuższe (nie krótsze niż 6 znaków).
b) Zawierać wielkie i małe litery, o ile to możliwe.
c) Zawierać cyfry i znaki interpunkcyjne, o ile to możliwe.
d) Nie może opierać się na żadnych danych osobowych.
e) Nie może opierać się na żadnym słowie ze słownika, w dowolnym języku.

- W przypadku korzystania z systemu operacyjnego pozbawionego funkcji bezpieczeństwa (takiego jak DOS, Windows lub MacOS) intruz potrzebuje jedynie uzyskać jedynie chwilowy i fizyczny dostęp do konsoli, aby móc wprowadzić program do monitorowania klawiatury. Jeżeli stacja robocza nie jest zabezpieczona fizycznie, intruz może wówczas uruchomić ponownie nawet zabezpieczony system operacyjny, uruchomić ponownie stację roboczą z własnego nośnika, a następnie wprowadzić program przeznaczony do celów przestępczych.
- Aby zapewnić ochronę przed atakami opartymi na analizie sieci, zarówno stacja robocza, jak i serwer powinny być zabezpieczone kryptograficznie. Przykładami silnych protokołów są protokoły NetWare z zaszyfrowanym identyfikatorem logowania i Kerberos.

14. Polityka antywirusowa

- Konfiguracja wszystkich urządzeń musi pozwalać na uruchamianie najnowszej wersji oprogramowania antywirusowego zatwierdzonego przez Firmę. Zalecaną aplikacją do użycia jest oprogramowanie antywirusowe XXXX, które należy skonfigurować w sposób umożliwiający automatyczne i codzienne pobieranie najnowszych aktualizacji programu antywirusowego. W programie antywirusowym należy włączyć okresowe skanowanie wszystkich systemów.
- Używane oprogramowanie antywirusowe powinno umożliwiać wykrywanie wszystkich znanych rodzajów złośliwego oprogramowania (wirusy, konie trojańskie, oprogramowanie z reklamami (adware), programy szpiegujące (spyware), robaki i programy typu rootkit).
- Wszystkie nośniki wymienne (na przykład dyskietki i inne) należy przeskanować przed użyciem w poszukiwaniu wirusów.
- Wszystkie dzienniki tworzone przez rozwiązania antywirusowe muszą być przechowywane zgodnie z wymogami prawnymi/regulacyjnymi/umownymi lub co najmniej zgodnie z wymaganiem 10.7 3 standardu PCI DSS przez 3 miesięcy w trybie on-line i 1 rok w trybie offline.
- Instalacje główne oprogramowania antywirusowego należy skonfigurować na aktualizacje automatyczne i okresowe operacje skanowania.
- Użytkownicy końcowi nie mogą mieć możliwości zmiany jakichkolwiek ustawień ani wprowadzania

zmian w oprogramowaniu antywirusowym.

- Nie należy otwierać wiadomości e-mail z załącznikami pochodzących z podejrzanych lub nieznanych źródeł. Wszystkie takie wiadomości e-mail wraz z ich załącznikami należy usuwać z systemu pocztowego oraz z kosza. Nie wolno nikomu przekazywać wiadomość e-mail, co do których podejrzewa się, że mogą zawierać wirusy.
- UŻYTKOWNICY TALECH ORAZ MOBILE MERCHANT Obowiązkiem użytkownika jest okresowe przeprowadzanie skanowania antywirusowego na urządzeniu mobilnym (jeśli dotyczy). Dodatkowo. jako właściciel i menedżer oprogramowania urządzenia, użytkownik ma obowiązek aktualizowania systemu operacyjnego i wszystkich aplikacji, natychmiastowego stosowania wszystkich poprawek zabezpieczeń sugerowanych przez dostawców oraz unikania instalowania jakiegokolwiek oprogramowania, którego zabezpieczeń nie można ocenić jako odpowiadających aktualnym normom branżowym

15. Polityka zarządzania poprawkami

- Wszystkie stacje robocze, serwery, oprogramowanie, składniki systemowe itd. stanowiące własność Firmy muszą mieć zainstalowane aktualne poprawki bezpieczeństwa systemu w celu ochrony zasobów przed znanymi podatnościami.
- W miarę możliwości wszystkie systemy i całe oprogramowanie muszą mieć włączone automatyczne aktualizacje poprawek systemu publikowanych przez ich odpowiednich dostawców. Poprawki bezpieczeństwa muszą być instalowane w ciągu jednego miesiąca od dnia ich opublikowania przez odpowiedniego dostawcę, a ich instalacja musi przebiegać zgodnie z procesem kontroli zmian.
- Wszelkie wyjątki od tego procesu muszą być udokumentowane.

16. Polityka dostępu zdalnego

- Obowiązkiem pracowników, kontrahentów, dostawców Firmy oraz agentów posiadających uprawnienia zdalnego dostępu do sieci firmowej Firmy jest dopilnowanie, aby połączenie zdalnego dostępu było brane pod uwagę tak samo jak lokalne połączenie użytkownika z Firmą.
- Należy ściśle kontrolować bezpieczny dostęp zdalny. Kontrolę tę będzie wzmacniać uwierzytelnianie dwuskładnikowe za pomocą uwierzytelniania hasłem jednorazowym lub kluczy publicznych/prywatnych z silnymi hasłami szyfrowania.
- Konta dostawców z dostępem do sieci Firmy będą włączane tylko w określonym czasie, gdy wymagany będzie dostęp, i będą wyłączane lub usuwane, gdy dostęp nie będzie już wymagany.
- Połączenie zdalnego dostępu będzie skonfigurowane na automatyczne rozłączanie się po 30 minutach bezczynności.
- Wszystkie hosty podłączone do sieci wewnętrznych Firmy za pomocą technologii zdalnego dostępu będą regularnie monitorowane.

- Wszystkie konta dostępu zdalnego używane przez dostawców lub podmioty zewnętrzne będą uzgadniane w ramach regularnych wywiadów, a konta niemające dalszego uzasadnienia biznesowego będą unieważniane.
- Konta dostawców z dostępem do sieci Firmy będą włączane tylko w określonym czasie, gdy wymagany będzie dostęp, i będą wyłączane lub usuwane, gdy dostęp nie będzie już wymagany.

17. Polityka zarządzania podatnościami

- Wszystkie podatności będą miały przypisaną klasyfikację ryzyka, taką jak wysokie, średnie lub niskie w oparciu o najlepsze praktyki branżowe, np. wynik podstawowy oceny CVSS.
- W ramach wymogów zgodności ze standardem PCI-DSS Firma będzie uruchamiać operacje skanowania podatności sieci na zagrożenia wewnętrzne i zewnętrzne co najmniej raz na kwartał oraz po wprowadzeniu wszelkich istotnych zmian w sieci (np. instalacje nowych składników systemowych, zmiany w topologii sieci, modyfikacje reguł zapory, uaktualnienia produktów).
- Kwartalne operacje skanowania podatności na zagrożenia wewnętrzne muszą być wykonywane przez personel wewnętrzny lub zewnętrznego dostawcę Firmy, a proces skanowania musi uwzględniać wykonywanie operacji ponownego skanowania do momentu uzyskania pozytywnych wyników lub naprawienia podatności określonych w wymaganiu 6.2 standardu PCI DSS.
- Kwartalne operacje skanowania podatności na zagrożenia zewnętrzne muszą być wykonywane przez Zatwierdzonego dostawcę skanowania (ASV) akredytowanego przez organizację PCI SSC. Operacje skanowania prowadzone po wprowadzeniu zmian w sieci mogą być wykonywane przez personel wewnętrzny Firmy. Proces skanowania powinien uwzględniać operacje ponownego skanowania do momentu uzyskania pozytywnych wyników.

18. Standardy konfiguracji:

- Systemy informatyczne przetwarzające przesyłane lub przechowywane dane właścicieli kart muszą być skonfigurowane zgodnie z obowiązującym standardem dla urządzenia lub systemu tej klasy. Standardy muszą być opracowane i prowadzone przez zespół odpowiedzialny za zarządzanie systemem we współpracy z Biurem ds. bezpieczeństwa informacji.
- Wszystkie konfiguracje urządzeń sieciowych należy dostosować do odpowiednich standardów Firmy przed umieszczeniem ich w sieci, zgodnie z informacjami podanymi w przewodniku po konfiguracji Firmy. Korzystając z tego przewodnika, utworzono standardową konfigurację, która będzie miała zastosowanie do wszystkich urządzeń sieciowych przed umieszczeniem ich w sieci.
- Przed wdrożeniem do produkcji system musi uzyskać potwierdzenie spełnienia wymogów obowiązującego standardu konfiguracji.
- Aktualizacje systemu operacyjnego i/lub ustawień konfiguracyjnych urządzeń sieciowych objęte standardami Firmy są ogłaszane przez Biuro ds. bezpieczeństwa informacji. Aktualizacje muszą być wprowadzane w terminie określonym przez Biuro ds. bezpieczeństwa informacji.
- Administratorzy urządzeń sieciowych nieprzestrzegający standardów Firmy (określeni w poprzednim wyjątku) muszą udokumentować i śledzić proces oceny aktualizacji systemu operacyjnego i/lub ustawień konfiguracyjnych ogłaszanych przez dostawcę. Proces ten musi uwzględniać harmonogram oceny, metodę analizy ryzyka oraz metodę aktualizacji.

- Należy sprawdzać corocznie wszystkie konfiguracje urządzeń sieciowych z konfiguracją standardową, aby mieć pewność, że dana konfiguracja nadal spełnia odpowiednie standardy.
- W miarę możliwości używane będzie oprogramowanie do zarządzania konfiguracjami sieciowymi w celu zautomatyzowania procesu potwierdzania zgodności z konfiguracją standardową.
- W przypadku innych urządzeń co kwartał przeprowadzany będzie kontrola dla porównania konfiguracji standardowej z obecną.
- Wszelkie rozbieżności będą poddawane ocenie i korygowane przez Administratora sieci.
- UŻYTKOWNICY TALECH ORAZ MOBILE MERCHANT Jako właściciel i menedżer oprogramowania urządzenia, użytkownik ma obowiązek aktualizowania systemu operacyjnego i wszystkich aplikacji, natychmiastowego stosowania wszystkich poprawek zabezpieczeń sugerowanych przez dostawców oraz unikania instalowania jakiegokolwiek oprogramowania, którego zabezpieczeń nie można ocenić jako odpowiadających aktualnym normom branżowym

19. Proces kontroli zmian

- Zmiany w zasobach informacyjnych powinny być zarządzane i wykonywane zgodnie z formalnym procesem kontroli zmian. Proces kontroli będzie gwarantować ocenę, zatwierdzanie, testowanie, wdrażanie i publikowanie proponowanych zmian w sposób kontrolowany oraz monitorowanie statusu każdej proponowanej zmiany.
- Proces kontroli zmian powinien być formalnie określony i udokumentowany. Proces kontroli zmian powinien być stosowany w celu kontroli zmian we wszystkich krytycznych zasobach informacyjnych firmy (takich jak sprzęt, oprogramowanie, dokumentacja systemu i procedury operacyjne). Ten udokumentowany proces powinien obejmować zadania i procedury zarządzania. W miarę możliwości należy zintegrować procedury kontroli zmian operacyjnych i zmian w aplikacji.
- Wszystkie żądania zmiany powinny być rejestrowane, bez względu na to, czy zostały przyjęte, czy też odrzucone w ujednoliconym i centralnym systemie. Zatwierdzenie wszystkich żądań zmiany powinno być udokumentowane wraz z ich wynikami. Przez cały czas powinien być prowadzony na poziomie jednostki biznesowej udokumentowany dziennik kontroli zawierający istotne informacje. Powinien on zawierać dokumentację żądań zmiany, autoryzację zmiany i wynik danej zmiany. Żadna osoba nie powinna móc dokonywać zmian w produkcyjnych systemach informatycznych bez zgody innych osób upoważnionych.
- Ocena ryzyka powinna być przeprowadzana dla wszystkich zmian oraz powinna być uzależniona od wyniku. Ponadto należy przeprowadzić ocenę wpływu.
- Ocena wpływu powinna obejmować potencjalny wpływ na inne zasoby informacyjne i potencjalne skutki finansowe. Ocena wpływu powinna uwzględniać w stosownych przypadkach zgodność z wymogami prawnymi i standardami.
- Wszystkie żądania zmiany powinny być uszeregowane pod względem korzyści, pilności, wymaganego nakładu pracy i potencjalnego wpływu na operacje.
- Zmiany powinny być testowane w izolowanym, kontrolowanym i reprezentatywnym środowisku (tam, gdzie takie środowisko jest możliwe) przed ich wdrożeniem w celu ograniczenia do

minimum wpływu na dany proces biznesowy, oceny jego wpływu na operacje i bezpieczeństwo oraz sprawdzenia, czy dokonano tylko planowanych i zatwierdzonych zmian. (Więcej informacji można znaleźć w publikacji pt. Cykl rozwoju systemu [przytoczenie w tym miejscu]).

- Każda zmiana i/lub aktualizacja oprogramowania powinna być kontrolowana za pomocą funkcji kontroli wersji. Starsze wersje powinny być przechowywane zgodnie z zasadami zatrzymywania i przechowywania firmy. (Więcej informacji można znaleźć w publikacji pt. Cykl rozwoju systemu [przytoczenie w tym miejscu]).
- Wszystkie zmiany powinny być zatwierdzane przed ich wdrożeniem. Zatwierdzanie zmian powinno odbywać się w oparciu o formalne kryteria akceptacji, tzn. upoważniony użytkownik zgłosił żądanie zmiany, przeprowadzono ocenę skutków i przetestowano proponowane zmiany.
- Wszyscy użytkownicy, na których istotny wpływ ma zmiana, powinni być o niej powiadomieni. Przedstawiciel użytkownika powinien wylogować się na czas wprowadzenia zmiany. Użytkownicy powinni być zobowiązani do złożenia opinii i uwag przed przyjęciem zmiany.
- Wdrożenie będzie następować dopiero po przeprowadzeniu odpowiednich testów i zatwierdzeniu przez strony zainteresowane. Wszelkie istotne zmiany powinny być traktowane jako wdrożenie nowego systemu i powinny być ustanowione jako projekt. Istotne zmiany będą klasyfikowane według nakładu pracy potrzebnego do opracowania i wdrożenia tych zmian. (Więcej informacji można znaleźć w publikacji pt. Cykl rozwoju systemu [przytoczenie w tym miejscu]).
- Procedury przerywania i powrotu po nieudanych zmianach powinny być udokumentowane. Jeżeli wynik zmiany będzie inny od oczekiwanego rezultatu (określonego w testach zmiany), należy odnotować procedury i zadania powrotu i zapewnienia ciągłości narażonych obszarów. Procedury powrotu będą stosowane w celu zapewnienia możliwości powrotu systemów do stanu sprzed wprowadzenia zmian.
- Dokumentacja zasobów informacyjnych powinna być aktualizowana po wprowadzeniu każdej zmiany. Dawna dokumentacja powinna być natomiast archiwizowana lub usuwana zgodnie z zasadami przechowywania dokumentacji i danych.
- Należy stosować określone procedury zapewniające właściwą kontrolę, autoryzację i dokumentację zmian w nagłych wypadkach. Standardowo zostaną określone specjalne parametry klasyfikacji zmian jako zmiany w nagłych wypadkach.
- Wszystkie zmiany będą monitorowane po ich wprowadzeniu do środowiska produkcyjnego. Odstępstwa od specyfikacji projektowych i wyników testów zostaną udokumentowane i przekazane właścicielowi rozwiązania w celu potwierdzenia.

20. Kontrola i przegląd dziennika

- Niniejsza procedura obejmuje wszystkie dzienniki tworzone dla systemów w środowisku przetwarzania danych właścicieli kart, w zależności od przepływu danych właścicieli kart w sieci Firmy, w tym następujące składniki:

- Dzienniki systemu operacyjnego (dzienniki zdarzeń i dzienniki polecenia su).
- Dzienniki kontroli baz danych.
- Dzienniki zapór i przełączników sieciowych.
- Dzienniki systemów wykrywania nieautoryzowanego dostępu (IDS).
- Dzienniki programów antywirusowych.
- Nagrania z kamer wideo CCTV.
- Dzienniki systemu monitorowania integralności plików.

- Dzienniki kontroli muszą być przechowywane przez okres co najmniej 3 miesięcy w trybie online (gotowe do natychmiastowej analizy) oraz 12 miesięcy w trybie offline.
- Analiza dzienników musi być przeprowadzana za pomocą systemu monitorowania sieci Firmy (nazwa hosta jest określana przez Firmę) sterowanego z poziomu konsoli Firmy (nazwa hosta jest określana przez Firmę). Konsola zainstalowana jest na serwerze (nazwa hosta/adres IP jest określany przez Firmę) znajdującym się w środowisku hostingowym Firmy.
- Przedstawieni poniżej pracownicy są jedynymi osobami posiadającymi uprawnienia dostępu do plików dzienników (Firma określa, które osoby mają potrzebę przeglądania plików dzienników kontroli i dzienników dostępu związaną z obowiązkami zawodowymi).
- Oprogramowanie systemu monitorowania sieci (określone przez Firmę) jest skonfigurowane na powiadamianie [WYZNACZONY ZESPÓŁ] Firmy o wszelkich sytuacjach uznanych za potencjalnie podejrzane w celu ich dalszego zbadania. Skonfigurowane są następujące alerty:
- Interfejsu opartego na przeglądarce pulpitu nawigacyjnego, monitorowanego przez [WYZNACZONY ZESPÓŁ] Firmy.
- Alerty przesyłane pocztą elektroniczną/SMS na skrzynkę pocztową [WYZNACZONY ZESPÓŁ] Firmy wraz z podsumowaniem incydentu. [NAZWA STANOWISKA] Firmy otrzymuje również szczegółowe informacje o alertach przesyłanych pocztą elektroniczną w celach informacyjnych.
- Przedstawione poniżej zdarzenia systemu operacyjnego są skonfigurowane na rejestrowanie oraz są monitorowane przez konsolę (nazwa hosta jest określana przez Firmę):

  a) Wszelkie operacje dodania, modyfikacje i operacje kasowania kont użytkowników.
  b) Wszelkie nieudane i nieautoryzowane próby logowania użytkownika.
  c) Wszelkie zmiany w plikach systemowych.
  d) Każdy dostęp do serwera lub aplikacji uruchomionej na serwerze, w tym plików przechowujących dane właścicieli kart.
  e) Akcje podejmowane przez każdą osobę z uprawnieniami administratora lub administracyjnymi.
  f) Każdy dostęp użytkownika do dzienników kontroli.
  g) Każda operacja tworzenia/kasowania obiektów systemowych zainstalowanych w systemie Windows. (Prawie wszystkie obiekty systemowe uruchamiane są z uprawnieniami administratora, a niektóre z nich mogą zostać wykorzystane w celu uzyskania uprawnień administratora do systemu).

- Przedstawione poniżej zdarzenia systemu bazy danych są skonfigurowane na rejestrowanie oraz są monitorowane przez system monitorowania sieci (oprogramowanie i nazwa hosta są określane przez Firmę):

  a) Wszelkie nieudane próby uzyskania uprawnień użytkownika w celu zalogowania się do bazy

danych Oracle.
b) Każda operacja logowania, którą dodano lub usunięto z uprawnieniami użytkownika bazy danych do bazy danych.
c) Każda operacja logowania, którą dodano lub usunięto z roli.
d) Każda rola bazy danych, którą dodano lub usunięto z bazy danych.
e) Każde hasło, które zmieniono dla roli aplikacji.
f) Każda baza danych, którą utworzono, zmodyfikowano lub usunięto.
g) Każdy obiekt bazy danych, taki jak schemat, z którym utworzono powiązanie.
h) Akcje podejmowane przez każdą osobę z uprawnieniami administratora bazy danych (DBA).

- Przedstawione poniżej zdarzenia zapory są skonfigurowane na rejestrowanie oraz są monitorowane przez system monitorowania sieci (oprogramowanie i nazwa hosta są określane przez Firmę):

  a) Naruszenia listy kontroli dostępu (ACL).
  b) Nieudane próby uwierzytelnienia użytkownika.
  c) Operacje logowania i akcje podejmowane przez każdą osobę korzystającą z kont z uprawnieniami.
  d) Zmiany konfiguracji wprowadzone w zaporze (np. wyłączone, dodane, skasowane lub zmodyfikowane zasady).

- Przedstawione poniżej zdarzenia przełącznika muszą być skonfigurowane na rejestrowanie oraz monitorowane przez system monitorowania sieci (oprogramowanie i nazwa hosta są określane przez Firmę):

  a) Nieudane próby uwierzytelnienia użytkownika.
  b) Operacje logowania i akcje podejmowane przez każdą osobę korzystającą z kont z uprawnieniami.
  c) Zmiany konfiguracji wprowadzone w przełączniku (np. wyłączona, dodana, skasowana lub zmodyfikowana konfiguracja).

- Przedstawione poniżej zdarzenia wykrywania nieautoryzowanego dostępu muszą być skonfigurowane na rejestrowanie oraz są monitorowane przez system monitorowania sieci (oprogramowanie i nazwa hosta są określane przez Firmę):

  a) Każda podatność wymieniona w bazie danych identyfikatorów CVE (z ang. Common Vulnerability Entry).
  b) Wszelkie ogólne ataki niewymienione w bazie danych identyfikatorów CVE.
  c) Wszelkie znane ataki typu „odmowa usługi”.
  d) Wszelkie wzorce ruchu wskazujące na przeprowadzenie rozpoznania przed atakiem.
  e) Wszelkie próby wykorzystania błędów konfiguracyjnych związanych z bezpieczeństwem.
  f) Wszelkie błędy uwierzytelnienia, które mogą wskazywać na atak.
  g) Każdy ruch wychodzący lub przychodzący z programu typu „backdoor”.
  h) Każdy ruch typowy dla znanych ataków ukrytych.

- Przedstawione poniżej zdarzenia związane z integralnością plików muszą być skonfigurowane na rejestrowanie oraz monitorowane przez system monitorowania sieci (oprogramowanie i nazwa hosta są określane przez Firmę):

a) Wszelkie zmiany w plikach systemowych.
b) Akcje podejmowane przez każdą osobę z uprawnieniami administratora.
c) Każdy dostęp użytkownika do dzienników kontroli.
d) Każda operacja tworzenia/kasowania obiektów systemowych zainstalowanych w systemie Windows. (Prawie wszystkie obiekty systemowe uruchamiane są z uprawnieniami administratora, a niektóre z nich mogą zostać wykorzystane w celu uzyskania uprawnień administratora do systemu).

- W przypadku stwierdzenia podejrzanego zdarzenia należy zarejestrować następujące informacje w formularzu oceny dziennika — F17, i powiadomić [NAZWA STANOWISKA] Firmy:

a) Identyfikator użytkownika.
b) Typ zdarzenia.
c) Data i godzina.
d) Wskazanie powodzenia lub niepowodzenia.
e) Źródło zdarzenia (np. adres IP).
f) Odwołanie do zagrożonych danych, składnika systemowego lub zasobu.

21. Wytwarzanie bezpiecznych aplikacji

- Polityka wytwarzania bezpiecznych aplikacji to plan działania pozwalający na ukierunkowanie decyzji i działań podejmowanych przez deweloperów w trakcie cyklu rozwoju oprogramowania (SDLC) w celu zapewnienia bezpieczeństwa oprogramowania. Celem tej polityki jest uniezależnienie jej od języka i platformy, aby można było ją stosować we wszystkich projektach rozwoju oprogramowania.
- Przestrzeganie i stosowanie polityki wytwarzania bezpiecznych aplikacji stanowi wymóg na wszystkich etapach rozwoju oprogramowania w systemach informatycznych Firmy i zaufanych witrynach kontrahentów przetwarzających dane Firmy.
- Każdy etap cyklu SDLC odwzorowano za pomocą działań w zakresie bezpieczeństwa w sposób wyjaśniony poniżej:

a) Projektowanie

- Określenie wymagań projektowych z punktu widzenia bezpieczeństwa
- Przegląd architektury i projektu
- Modelowanie zagrożeń

b) Kodowanie

- Stosowanie najlepszych praktyk kodowania
- Przeprowadzenie analizy statycznej

c) Testowanie

- Ocena podatności na zagrożenia
- Testowanie odporności na błędne dane

d) Wdrożenie

- Przegląd konfiguracji serwera

- Przegląd konfiguracji sieci

- Rozwój kodu powinien być poddawany kontroli i walidacji z zastosowaniem najbardziej aktualnych wersji standardów kodowania Firmy dla zapewnienia wytwarzania bezpiecznych aplikacji. Wszyscy programiści powinni sprawdzić zgodność swojego kodu z najnowszymi i zatwierdzonymi standardami kodowania i wytycznymi.
- Tylko zatwierdzony kod zostanie wdrożony do środowiska produkcyjnego Firmy. Przegląd i walidacja gwarantuje, że kod wyróżnia się podstawowymi cechami bezpieczeństwa obejmującymi poprawność, przewidywalności i odporność na atak.

Programiści aplikacji powinni:

- Zadbać o to, aby kod zapewniał pewien poziom bezpieczeństwa pozwalający na wyeliminowanie luk w kodzie z oprogramowania, niezależnie od tego, czy wprowadzono go już do oprogramowania, czy też umieszczono go na późniejszym etapie cyklu jego rozwoju.
- Zadbać o to, aby kod zapewniał przewidywalność wykonania lub uzasadnione zaufanie oraz aby oprogramowanie w trakcie uruchomienia zapewniało funkcje bezpieczeństwa zgodnie z przeznaczeniem.
- Techniki kodowania muszą zapewniać możliwość usunięcia luk pozwalających na ataki wstrzyknięcia, zwłaszcza wstrzyknięcia kodu SQL, luk przepełnienia bufora, luk umożliwiających działanie skryptów między witrynami, kontroli przed niepowołanym dostępem (niezabezpieczone bezpośrednie odwołanie do obiektu, brak zabezpieczeń dostępu przez adres URL, przechodzenie po katalogach itd.), fałszowania żądań międzywitrynowych (CSRF), niepoprawnej obsługi uwierzytelniania i sesji.
- Nie wolno mieć zaufania do danych przychodzących do systemu, należy wprowadzić system kontroli tych danych.
- Nie wolno pozwalać klientowi na przechowywanie poufnych danych, bez względu na stopień ich istotności.
- Wyłączyć komunikaty o błędach zwracające wszelkie informacje dla użytkownika.
- Stosować dziedziczenie obiektów, hermetyzację oraz polimorfizm, o ile jest to możliwe.
- Używać ostrożnie zmiennych środowiskowych oraz zawsze sprawdzać ograniczenia i bufory.
- Aplikacje muszą sprawdzać poprawność danych wejściowych w celu zapewnienia poprawności ich sformułowania i istotności.

22. Metodologia testów penetracyjnych

- W tej sekcji powinny być wymienione ryzyka związane nieodłącznie z prowadzeniem testów penetracyjnych w systemach informatycznych Firmy. Dodatkowo dla każdego z nich powinny być wskazane środki łagodzące, które zostaną podjęte. Przykładami mogą być:

Przykład nr 1

Ryzyko: odmowa usługi w systemach lub urządzeniach sieciowych z powodu operacji skanowania sieci.

Środek łagodzący 1: operacje skanowania sieci muszą być przeprowadzane w sposób

kontrolowany. Godzinę rozpoczęcia i zakończenia skanowania należy zgłosić wyznaczonym pracownikom, aby umożliwić monitorowanie w trakcie wykonywania testów. W przypadku wystąpienia jakichkolwiek problemów trwające skanowanie zostanie przerwane.

Środek łagodzący 2: narzędzia do skanowania należy skonfigurować w sposób gwarantujący, że wielkość przesyłanych pakietów lub liczba sesji ustanawianych na minutę nie spowoduje problemów w działaniu elementów sieci. W tym przypadku trzeba najpierw wykonać operacje skanowania w bardzo kontrolowany sposób i zastosować minimalną konfigurację, którą będzie można rozszerzyć, gdy będzie oczywiste, że konfiguracja nie stanowi zagrożenia dla urządzeń sieciowych ani serwerów w organizacji.

- Wymienieni zostaną główni członkowie personelu uczestniczący w projekcie organizacji:

Kierownik techniczny projektu:
Dyrektor ds. bezpieczeństwa informacji:
Dyrektor ds. informacji:
Kierownik ds. komunikacji:
Osoba odpowiedzialna za witrynę internetową YYYY.com:

- Zewnętrzne testy penetracyjne będą wykonywane zdalnie z siedziby dostawcy. Wewnętrzne testy penetracyjne będą prowadzone w biurze Firmy Organizacji. Zespół kontrolny musi mieć dostęp do sieci Organizacji. Musi on zarządzać uprawnieniami dostępu do budynku z odpowiednim wyprzedzeniem, aby mógł uzyskać bezproblemowy dostęp w okresu planowania.
- Wszystkie testy będą prowadzone za pomocą sprzętu należącego do zespołu kontrolnego, dlatego do wykonania testów nie są wymagane żadne urządzenia. Jedynym wymogiem w tym zakresie będzie udostępnienie aktywnego połączenia sieciowego dla każdego członka zespołu kontrolnego. Połączenia te muszą zapewniać dostęp do docelowego segmentu sieci w każdym przypadku.
- W przypadku wystąpienia incydentu podczas wykonywania testów mającego wpływ na działanie systemów lub usług organizacji informację o incydencie należy bezzwłocznie przekazać do wiadomości osób odpowiedzialnych za zarządzanie incydentami w projekcie.
- Należy zauważyć, że w celu zapewnienia zgodności ze standardem PCI DSS zakres testów powinien obejmować co najmniej następujące elementy:
    - Wszystkie systemy i aplikacje stanowiące część sieci obwodowej środowiska przetwarzania danych właścicieli kart (CRP).

Przykład:

a) Systemy objęte zakresem testów

System 1: Adres IP: System: Opis systemu

System 2: Adres IP: System: Opis systemu

Sieć Wi-Fi Firmy

.....

b) Aplikacje objęte zakresem testów

Aplikacja 1: Adres URL: Opis aplikacji

.....

c) Systemy nieobjęte zakresem testów

System 5: Adres IP: System: Opis systemu

System 6: Adres IP: System: Opis systemu

.....

d) Aplikacje nieobjęte zakresem testów

Aplikacja 3: Adres URL: Opis aplikacji

.....

- Testy techniczne muszą być wykonywane zgodnie z metodologią OSSTMM. Testy muszą być prowadzone na poziomie sieci, systemu i aplikacji oraz muszą gwarantować co najmniej identyfikację luk udokumentowanych przez organizacje OWASP i SANS oraz tych określonych w wersji 3. standardu PCI DSS:

1. Ataki wstrzyknięcia: kodu, kodu SQL, poleceń systemowych, protokołu LDAP, języka XPath itd.
2. Przepełnienia buforu.
3. Niezabezpieczone przechowywanie kluczy kryptograficznych.
4. Niezabezpieczona komunikacja.
5. Niepoprawna obsługa błędów.
6. Działanie skryptów między witrynami (XSS).
7. Kontrola przed niepowołanym dostępem.
8. Fałszowanie żądań międzywitrynowych (CSRF).
9. Niepoprawna obsługa uwierzytelniania i sesji.
10. Każda inna luka uznana przez organizację za stwarzającą Wysokie ryzyko.

- Dla wszystkich poczynionych ustaleń i luk wykrytych podczas przeprowadzonych testów zostaną wygenerowane i udokumentowane wystarczające dowody potwierdzające ich istnienie. Dowody mogą być w postaci zmiennej w każdym przypadku, zrzutu ekranu, nieprzetworzonych danych wyjściowych narzędzi bezpieczeństwa, zdjęć, dokumentów papierowych itd.
- W wyniku przeprowadzonych testów powinien zostać wygenerowany dokument zawierający co najmniej następujące sekcje:

Wprowadzenie
Podsumowanie
Metodologia
Zidentyfikowane luki
Zalecenia dotyczące wyeliminowania luk
Wnioski
Dowody

23. Plan reagowania na incydenty

„Incydent bezpieczeństwa" oznacza każde zdarzenie (przypadkowe, celowe lub zamierzone) dotyczące systemów komunikacji lub przetwarzania informacji. Osobą atakującą może być obca osoba o złych zamiarach, konkurent lub niezadowolony pracownik, którego intencją może być kradzież informacji lub pieniędzy lub po prostu zniszczenie firmy.

Plan reagowania na incydenty musi być poddawany corocznym testom. Kopie tego planu należy udostępnić wszystkim zainteresowanym członkom personelu. Ponadto należy podjąć odpowiednie kroki, aby mogło one go zrozumieć oraz wiedziały, czego się od nich oczekuje.

Od pracowników firmy będzie oczekiwać się zgłaszania wszelkich problemów związanych z bezpieczeństwem wyznaczonemu pracownikowi ochrony.

Plan reagowania na incydenty bezpieczeństwa (PCI) Firmy przedstawia się następująco:

1. Każdy dział musi zgłaszać wszelkie incydenty dyrektorowi ds. bezpieczeństwa informacji (preferowane) lub innego członka zespołu ds. reagowania na incydenty PCI.
2. Członek zespołu, który otrzyma zgłoszenie, ma obowiązek powiadomić zespół ds. reagowania na incydenty PCI o takim incydencie.
3. Zespół ds. reagowania na incydenty PCI zbada incydent i udzieli pomocy odpowiedniemu działowi w celu ograniczenia ryzyka dla danych właścicieli kart oraz zagrożeń związanych z incydentem.
4. Zespół ds. reagowania na incydenty PCI opracuje rozwiązanie problemu ku satysfakcji wszystkich dotkniętych nim stron, a także zgłosi incydent oraz poczynione ustalenia odpowiednim podmiotom (stowarzyszeniom operatorów kart kredytowych, operatorom kart kredytowych), jeśli zostanie to uznane za konieczne.
5. Zespół ds. reagowania na incydenty PCI ustali, czy należy zaktualizować zasady i procesy w celu uniknięcia podobnych incydentów w przyszłości oraz czy należy wprowadzić dodatkowe zabezpieczenia w środowisku, w którym wystąpił incydent, bądź w całej instytucji.
6. W przypadku stwierdzenia lub wykrycia nieautoryzowanego bezprzewodowego punktu dostępowego lub urządzeń bezprzewodowych w ramach testu wykonywanego co kwartał informację o tym należy bezzwłocznie przekazać Dyrektorowi ds. bezpieczeństwa lub innej osobie posiadającej podobne uprawnienia, która jest uprawniona do natychmiastowego zatrzymania, przerwania działania, wyłączenia lub usunięcia urządzenia przeznaczonego do celów przestępczych.
7. Jeśli pracownicy działu mają uzasadnione podejrzenia, że doszło do włamania na konto, do środowiska danych właścicieli kart lub systemów powiązanych z takim środowiskiem, mają obowiązek powiadomić o tym zespół ds. reagowania na incydenty PCI w Firmie. Po otrzymaniu informacji o możliwym naruszeniu zabezpieczeń zespół ds. reagowania na incydenty PCI wraz z innymi wyznaczonymi pracownikami wdrożą plan reagowania na incydenty PCI, wspierający i uzupełniający plany działania opracowane przez dział.

Zespół ds. reagowania na incydenty bezpieczeństwa PCI Firmy: **(zaktualizować jeśli dotyczy)**

Dyrektor ds. informatycznych
Dyrektor ds. komunikacji
Dyrektor ds. zgodności

z przepisami
Radca prawny
Dyrektor ds. bezpieczeństwa informacji
Przedstawiciel działu płatności i usług akceptanta
Kierownik ds. ryzyka

Powiadamianie o reagowaniu na incydenty:

Członkowie ds. eskalacji

Eskalacja — pierwszy poziom
- Inspektor ds. bezpieczeństwa informacji
- Dyrektor projektowy ds. płatności kredytowych i radca prawny ds. usług akceptanta
- Kierownik ds. ryzyka
- Dyrektor ds. komunikacji w Firmie

Eskalacja — drugi poziom
- Prezes Firmy
- Zarząd
- Audytorzy wewnętrzni
- Dodatkowi pracownicy (jeśli jest to konieczne)

Zewnętrzne osoby kontaktowe (jeśli jest to konieczne)
- Operatorzy kart obsługiwanych przez akceptanta
- Dostawca usług internetowych (jeśli dotyczy)
- Dostawca usług internetowych intruza (jeśli dotyczy), operatorzy telekomunikacyjni (lokalni i ogólnokrajowi), partnerzy biznesowi
- Ubezpieczyciel
- Zewnętrzny zespół ds. reagowania, jeśli dotyczy (Centrum koordynacyjne CERT 1, itp.), służby ochrony porządku publicznego (w zależności od lokalnych regulacji)

W odpowiedzi na możliwe naruszenie zabezpieczeń systemu zespół ds. reagowania na incydenty PCI oraz wyznaczone przezeń osoby podejmą następujące działania:

1. Zapewnienie odizolowania systemów z naruszonymi zabezpieczeniami od sieci.
2. Zgromadzenie, przejrzenie i przeanalizowanie rejestrów i powiązanych informacji z różnych lokalnych i centralnych funkcji zabezpieczeń.
3. Przeprowadzenie odpowiedniej analizy kryminalistycznej systemu z naruszonymi zabezpieczeniami.
4. Nawiązanie kontaktu z odpowiednimi wewnętrznymi i zewnętrznymi działami oraz podmiotami.
5. Udostępnienie analizy kryminalistycznej i analizy rejestrów odpowiednim służbom ochrony

porządku publicznego lub pracownikom operatorów kart zajmującym się kwestiami bezpieczeństwa.

6. Służenie pomocą organom ochrony porządku publicznego oraz pracownikom operatorów kart zajmującym się kwestiami bezpieczeństwa w prowadzeniu dochodzenia, w tym również na drodze sądowej.

Sposób powiadamiania firmy Elavon o wystąpieniu incydentu

1. **Wielka Brytania:**
   - Adres e-mail: #ADCqueries-GB@elavon.com
   - Telefon: 0 1923 651 622
2. **Irlandia:**
   - Adres e-mail: #ADCqueries-IE@elavon.com
   - Telefon: 0402 25322

3. **Niemcy:**
   - #ADCqueries-DE@elavon.com
4. **Polska:**
   - #ADCqueries-PL@elavon.com
5. **Norwegia:**
   - #ADCqueries-NO@elavon.com
6. **Inne kraje:**
   - #ADCqueries-EU@elavon.com

24. Role i obowiązki

- Dyrektor ds. bezpieczeństwa (lub jego odpowiednik) jest odpowiedzialny za nadzorowanie wszystkich aspektów bezpieczeństwa informacji, w tym między innymi:
- Tworzenie i rozpowszechnianie zasad i procedur bezpieczeństwa.
- Monitorowanie i analizowanie alertów zabezpieczeń oraz przekazywanie informacji odpowiednim pracownikom zarządzającym bezpieczeństwem informacji i jednostkami biznesowymi.
- Tworzenie i rozpowszechnianie procedur reagowania na incydenty bezpieczeństwa i procedur ich eskalacji, które obejmują:
- Prowadzenie formalnego programu dotyczącego świadomości bezpieczeństwa dla wszystkich pracowników, zapewniającego wiele metod podnoszenia świadomości i edukowania pracowników (np. plakaty, listy, spotkania).
- Biuro ds. technologii informatycznych (lub jego odpowiednik) powinno prowadzić codzienne procedury bezpieczeństwa operacyjnego w zakresie administracyjnym i technicznym, które są zgodne ze standardem PCI-DSS (np. procedury prowadzenia kont użytkowników oraz procedury przeglądania dzienników).
- Administratorzy systemu i aplikacji powinni:
- monitorować i analizować alerty zabezpieczeń i informacje o zabezpieczeniach oraz przekazywać je odpowiednim pracownikom
- zarządzać kontami użytkowników i uwierzytelnianiem

- Monitorować i kontrolować każdy dostęp do danych.
- Prowadzić wykaz dostawców usług.
- Upewnić się, że istnieje proces angażowania dostawców usług, z odpowiednią analizą przedinwestycyjną przed zaangażowaniem włącznie.
- Prowadzić program pozwalający sprawdzić status zgodności dostawców usług ze standardem PCI-DSS, wraz z dołączoną dokumentacją.
- Biuro ds. zarządzania zasobami ludzkimi (lub jego odpowiednik) jest odpowiedzialne za śledzenie uczestnictwa pracowników w programie dotyczącym świadomości bezpieczeństwa, w tym:
- Ułatwienie wzięcia w nim udziału po zatrudnieniu oraz co najmniej raz w roku.
- Dopilnowanie, aby pracownicy co najmniej raz w roku oświadczali pisemnie fakt zapoznania się z polityką bezpieczeństwa informacji Firmy oraz jej zrozumienia.
- Radca prawny (lub jego odpowiednik) będzie gwarantować, że w przypadku dostawców usług, którym udostępniane są dane właścicieli kart:
- Umowy pisemne będą wymagać przestrzegania standardu PCI-DSS przez dostawcę usług.
- Umowy pisemne będą zawierać potwierdzenie lub zobowiązanie do zabezpieczenia danych właścicieli kart przez dostawcę usług.

25. Dostęp niezależnych podmiotów do danych właścicieli kart

- Wszystkie niezależne firmy świadczące na rzecz Firmy istotne usługi muszą podpisać odpowiednią umowę o poziomie usług.
- Wszystkie niezależne firmy udostępniające obiekty gościnne muszą przestrzegać polityki Firmy w zakresie zabezpieczeń fizycznych i kontroli dostępu.
- Wszystkie niezależne firmy mające dostęp do danych właścicieli kart muszą:

1. Przestrzegać wymagań bezpieczeństwa ujętych w standardzie PCI DSS.
2. Potwierdzić zobowiązanie do zabezpieczenia danych właścicieli kart.
3. Potwierdzić fakt, że dane właścicieli kart mogą być używane wyłącznie w celu ułatwienia realizacji transakcji, na potrzeby programu lojalnościowego, świadczenia usługi kontroli oszustw lub zastosowań wymaganych przez prawo.
4. Przestrzegać odpowiednich postanowień dotyczących zapewnienia ciągłości działalności na wypadek poważnych utrudnień, klęsk żywiołowych czy awarii.
5. Zapewnić pełną współpracę i dostęp na potrzeby przeprowadzenia przez przedstawiciela lub zatwierdzony niezależny podmiot branży kart płatniczych kompleksowego przeglądu zabezpieczeń po incydencie związanym z naruszeniem bezpieczeństwa.

26. Zarządzanie dostępem użytkowników

- Dostęp do Firmy jest kontrolowany poprzez formalny proces rejestracji użytkowników, zaczynający się od oficjalnego zawiadomienia przez dział kadr lub przez bezpośredniego przełożonego.
- Każdy użytkownik posiada unikatowy identyfikator, dzięki któremu można powiązać użytkowników z ich działaniami i rozliczać ich z nich. Stosowanie identyfikatorów grupowych jest dozwolone wyłącznie wówczas, gdy wymaga tego charakter wykonywanej pracy.

- Istnieje standardowy poziom dostępu; dostęp do innych usług można uzyskać na podstawie upoważnienia uzyskanego od działu kadr/bezpośredniego przełożonego.
- Poziom dostępu pracownika do danych właścicieli kart zależy od jego stanowiska.
- Wniosek o dostęp do usługi musi złożyć na piśmie (za pośrednictwem poczty e-mail lub wydruku) bezpośredni przełożony nowego pracownika lub dział kadr. Format wniosku jest dowolny, ale musi on zawierać następujące informacje:

  Imię i nazwisko osoby składającej wniosek:
  Stanowisko i grupa robocza nowego pracownika:
  Data rozpoczęcia:
  Wymagane usługi (usługi domyślne to: MS Outlook, MS Office i dostęp do Internetu):

- Każdy użytkownik otrzyma kopię formularza nowego użytkownika, który stanowi pisemne zestawienie jego praw dostępu, podpisane przez przedstawiciela działu informatycznego po przeprowadzeniu procedury wprowadzenia. Użytkownik podpisuje formularz, wskazując, że rozumie warunki dostępu.
- Dostępu do wszystkich systemów Firmy udziela dział informatyczny, po przeprowadzeniu odpowiednich procedur.
- Z chwilą odejścia użytkownika z Firmy jego wszystkie loginy muszą zostać natychmiast unieważnione.
- W ramach procesu rozwiązania umowy o pracę dział kadr (lub bezpośredni przełożeni w przypadku wykonawców) zawiadamia dział informatyczny o osobach odchodzących z firmy i o dacie odejścia.

27. Polityka kontroli dostępu

- Wdrożone systemy kontroli dostępu mają na celu ochronę interesów wszystkich użytkowników systemów komputerowych Firmy dzięki zapewnieniu im bezpiecznego i łatwo dostępnego środowiska pracy.
- Firma będzie przekazywać wszystkim pracownikom i innym użytkownikom informacje niezbędne im do wykonywania swoich obowiązków w sposób jak najbardziej efektywny i sprawny.
- Identyfikatory ogólne lub grupowe zasadniczo nie są dozwolone, ale mogą być przyznawane w wyjątkowych okolicznościach, o ile istnieją inne sposoby kontroli dostępu.
- Przyznawanie uprawnień (np. lokalnego administratora, administratora domeny, superużytkownika, dostępu głównego) będzie ograniczone i kontrolowane, a autoryzacje będą przyznawane wspólnie przez właściciela systemu i dział informatyczny. Zespoły techniczne powinny unikać przyznawania uprawnień całym zespołom, aby zapobiec utracie poufności.
- Prawa dostępu będą przyznawane na zasadach „najmniejszego uprawnienia” i „potrzeby posiadania informacji”.
- Każdy użytkownik powinien dążyć do utrzymania bezpieczeństwa danych na ich poziomie poufności, nawet w przypadku, gdy zabezpieczenia techniczne zawodzą lub nie są stosowane.
- Użytkownicy decydujący się na umieszczenie danych na nośnikach cyfrowych lub urządzeniach pamięci, albo w odrębnej bazie danych, mogą to zrobić tylko wówczas, gdy jest to zgodne z klasyfikacją danych.

- Użytkownicy mają obowiązek zgłaszania przypadków niezgodności dyrektorowi ds. bezpieczeństwa informacji Firmy.
- Dostęp do zasobów i usług informatycznych Firmy będzie przyznawany przez ustanowienie unikatowego konta Active Directory i złożonego hasła.
- Dostęp do zasobów i usług informatycznych Firmy nie będzie przyznawany bez wcześniejszego uwierzytelnienia i autoryzacji konta Windows Active Directory użytkownika w systemie Firmy.
- Wydawaniem haseł, wymogami dotyczącymi ich siły, zmianą i kontrolą będzie zarządzać się za pośrednictwem formalnych procesów. Długość haseł, ich złożoność i terminy ważności będą kontrolować obiekty zasad grupy Active Directory systemu Windows.
- Dostęp do informacji poufnych, zastrzeżonych i chronionych zostanie ograniczony do osób uprawnionych, których obowiązki zawodowe wymagają tego, wyznaczonych przez właściciela danych lub wskazanego przez niego przedstawiciela. Wnioski o udzielenie, zmianę lub odwołanie uprawnień dostępu muszą być składane w formie pisemnej.
- Od użytkowników oczekuje się poznania i przestrzegania zasad, standardów i wytycznych Firmy dotyczących stosownego i dopuszczalnego użytku sieci i systemów.
- Dostęp użytkowników zdalnych będzie podlegać autoryzacji przez dział informatyczny i będzie przyznawany zgodnie z polityką dostępu zdalnego oraz polityką bezpieczeństwa informacji. Nie będzie dozwolony niekontrolowany dostęp zewnętrzny do żadnych urządzeń czy systemów sieciowych.
- Dostęp do danych jest kontrolowany w sposób zależny od poziomów klasyfikacji danych opisanych w polityce zarządzania bezpieczeństwem informacji.
- Metody kontroli dostępu obejmują: prawa dostępu przez logowanie, uprawnienia udziałów i NTFS systemu Windows, uprawnienia kont użytkowników, prawa dostępu do serwerów i stacji roboczych, uprawnienia zapory, prawa uwierzytelniania IIS w sieciach intranet/extranet, prawa do baz danych SQL, sieci wydzielone i inne metody stosowne do potrzeb.
- W regularnych odstępach czasu właściciele systemów i danych, we współpracy z działem informatycznym, powinni przeprowadzać formalny proces przeglądu praw dostępu użytkowników. Przegląd należy zarejestrować w dzienniku, a dział informatyczny powinien go zatwierdzić celem utrzymania praw dostępu użytkowników.

28. Polityka bezprzewodowego dostępu

- Zabrania się instalacji i korzystania z jakichkolwiek urządzeń bezprzewodowych lub sieci bezprzewodowych przeznaczonych do łączenia się z dowolnymi sieciami lub środowiskami pracy Firmy.
- Należy uruchamiać co kwartał test pozwalający wykryć wszystkie bezprzewodowe punkty dostępowe połączone z siecią Firmy.
- Należy przeprowadzać raz na kwartał odpowiednie testy przy użyciu narzędzi, takich jak NetStumbler, Kismet itd., w celu upewnienia się, że:

- Wszelkie urządzenia obsługujące łączność bezprzewodową pozostają wyłączone lub zostały wycofane z eksploatacji.
- W przypadku wykrycia jakiegokolwiek naruszenia polityki bezprzewodowego dostępu w wyniku przeprowadzenia normalnych procesów kontrolnych dyrektor ds. bezpieczeństwa lub każda osoba zajmująca podobne stanowisko posiada uprawnienia do natychmiastowego zatrzymania, przerwania działania, wyłączenia lub usunięcia urządzenia przeznaczonego do celów przestępczych.

Jeżeli zachodzi potrzeba skorzystania z technologii bezprzewodowej, powinna ona zostać zatwierdzona przez Firmę. Ponadto należy przestrzegać następujących standardów łączności bezprzewodowej:

1. Domyślnie ciągi identyfikacyjne i hasła protokołu SNMP, hasła szyfrowania, klucze szyfrowania/ustawienia domyślne dostawcy związane z bezpieczeństwem (jeśli dotyczy) należy zmienić bezzwłocznie po zainstalowaniu urządzenia, a także po odejściu z firmy osoby posiadającej wiedzę w tym zakresie.
2. Oprogramowanie sprzętowe w urządzeniach bezprzewodowych musi być aktualizowane zgodnie z harmonogramem publikacji dostawców.
3. Oprogramowanie sprzętowe w urządzeniach bezprzewodowych musi obsługiwać silne szyfrowanie w celu uwierzytelniania i transmisji danych w sieciach bezprzewodowych.
4. Wszelkie inne ustawienia domyślne dostępu bezprzewodowego dostawcy związane z bezpieczeństwem należy zmienić w razie potrzeby.
5. W sieciach bezprzewodowych należy wprowadzić najlepsze praktyki branżowe (IEEE 802.11i) oraz silne szyfrowanie w celu uwierzytelniania i przekazywania danych właścicieli kart.
6. Należy prowadzić spis autoryzowanych punktów dostępowych wraz z uzasadnieniem biznesowym. (Zaktualizować załącznik B)

Załącznik A – Formularz zobowiązania do przestrzegania — Zobowiązanie do przestrzegania zasad bezpieczeństwa informacji

Piotr Wojsz

_____

Imię i nazwisko pracownika (drukowanymi literami)

Prezes Zarządu

_____

Dział

Zobowiązuję się do podjęcia wszelkich uzasadnionych środków ostrożności w celu zapewnienia poufności informacji wewnętrznych Firmy oraz informacji jej powierzonych przez osoby trzecie, np. klientów, oraz ich nieujawniania niepowołanym osobom. Po zakończeniu zatrudnienia w Firmie lub wygaśnięciu umowy z nią zawartej zobowiązuję się zwrócić wszelkie informacje, do których mam dostęp w związku z zajmowanym stanowiskiem. Przyjmuję do wiadomości fakt, że nie mam prawa wykorzystywać poufnych informacji do własnych celów ani ich udostępniać osobom trzecim bez uzyskania wyraźnej zgody na piśmie kierownika wewnętrznego, który jest wyznaczonym właścicielem takich informacji.

Oświadczam, że mam dostęp do zasad zabezpieczania informacji, potwierdzam fakt zapoznania się z nimi i zrozumienia ich wpływu na moją pracę. Zobowiązuję się do przestrzegania zasad i innych wymagań zawartych w polityce bezpieczeństwa firmy, co jest warunkiem ciągłości zatrudnienia w firmie. Przyjmuję do wiadomości fakt, że brak zgodności będzie skutkować postępowaniem dyscyplinarnym, z rozwiązaniem stosunku pracy włącznie, a potencjalnie także karami z powództwa karnego i/lub cywilnego. Zobowiązuję się także do niezwłocznego zgłaszania wszelkich faktycznych lub potencjalnych przypadków naruszenia zasad bezpieczeństwa wyznaczonemu pracownikowi ochrony.

_____

Podpis pracownika

Załącznik B

Nazwa zasobu/urządzenia	Opis	Właściciel/zatwierdzony użytkownik	Lokalizacja

Wykaz dostawców usług

Nazwa dostawcy usług	Dane kontaktowe	Dostarczane usługi	Zgodność PCI DSS	Data weryfikacji PCI DSS