1. Przedmiot

Celem niniejszego dokumentu jest ustanowienie ram regulacyjnych dotyczących bezpieczeństwa informacji dla organizacji będących dostawcami Grupy Azpiaran, które mają dostęp do jej informacji, systemów informatycznych lub zasobów, w celu ochrony ich poufności, integralności i dostępności.

W tym celu organizacje dostawcze są odpowiedzialne za poinformowanie swoich pracowników i podwykonawców świadczących usługi na rzecz Grupo Azpiaran.

2. Zakres

Wszystkie działania wykonywane dla Grupo Azpiaran przez organizacje dostawcze, które mają dostęp do jej informacji, systemów informatycznych lub zasobów.

Punkt „3. Wytyczne ogólne" ma zastosowanie do każdej organizacji dostawczej, niezależnie od rodzaju świadczonych usług.

Punkt „4. Wytyczne szczegółowe" ma zastosowanie wyłącznie do tych organizacji dostawców, których świadczone usługi odpowiadają rodzajowi usługi wskazanej w każdym przypadku, zgodnie z informacją podaną na początku wspomnianego punktu.

3. Wytyczne ogólne

3.1. Świadczenie usług

Organizacje świadczące usługi mogą wykonywać dla Grupy Azpiaran wyłącznie czynności objęte odpowiednią umową o świadczenie usług.

Organizacja świadcząca usługi będzie okresowo dostarczać Grupie Azpiaran wykaz osób, profili, funkcji i obowiązków związanych ze świadczoną usługą oraz będzie na bieżąco informować o wszelkich zmianach (przyjęcie, odejście, zastąpienie lub zmiana funkcji lub obowiązków) zachodzących w tym wykazie.

Zgodnie z postanowieniami klauzul związanych z umową o świadczenie usług, wszystkie osoby zewnętrzne wykonujące prace dla Grupy Azpiaran muszą przestrzegać zasad bezpieczeństwa zawartych w niniejszym dokumencie. W przypadku naruszenia któregokolwiek z tych obowiązków Grupo Azpiaran zastrzega sobie prawo do zawieszenia osoby, która dopuściła się naruszenia, a także do podjęcia środków karnych, które uzna za stosowne w odniesieniu do organizacji świadczącej usługi.

Organizacja świadcząca usługi musi zapewnić, że wszystkie jej osoby posiadają odpowiednie kwalifikacje do wykonywania świadczonych usług.

Wszelka wymiana informacji między Grupo Azpiaran a organizacją dostawczą będzie rozumiana jako odbywająca się w ramach ustalonych w odpowiedniej umowie o świadczenie usług, tak więc informacje te nie mogą być wykorzystywane poza tymi ramami ani do innych celów.

T.I. centralizuje globalne działania w zakresie ochrony aktywów Grupo Azpiaran

Ogólnie rzecz biorąc, aktywa obejmują:

- Informacje chronione, tj. informacje umożliwiające identyfikację osób fizycznych i/lub prawnych oraz informacje dotyczące konfiguracji systemów informatycznych i sieci komunikacyjnych.
- Podmioty współpracujące w zakresie przetwarzania informacji chronionych (oprogramowanie, sprzęt komputerowy, sieci komunikacyjne, nośniki informacji, wyposażenie pomocnicze i instalacje).

3.2. Poufność informacji

Osoby zewnętrzne mające dostęp do informacji Grupo Azpiaran powinny traktować te informacje jako domyślnie chronione. Za informacje niechronione można uznać wyłącznie te informacje, do których dostęp uzyskano za pośrednictwem środków publicznego rozpowszechniania informacji udostępnionych w tym celu przez Grupo Azpiaran.

Należy unikać ujawniania, modyfikowania, niszczenia lub niewłaściwego wykorzystywania informacji, niezależnie od nośnika, na którym się znajdują.

Informacje chronione będą przechowywane przez czas nieokreślony z zachowaniem maksymalnej poufności i nie będą ujawniane na zewnątrz, chyba że zostanie to odpowiednio zatwierdzone.

Należy zminimalizować liczbę raportów w formie papierowej zawierających informacje chronione i przechowywać je w bezpiecznym miejscu, niedostępnym dla osób trzecich.

W przypadku, gdy z powodów bezpośrednio związanych z miejscem pracy pracownik organizacji dostawczej wejdzie w posiadanie informacji chronionych zawartych na dowolnym nośniku, powinien on zrozumieć, że posiadanie to ma charakter ściśle tymczasowy, wiąże się z obowiązkiem zachowania tajemnicy i nie daje mu żadnych praw do posiadania, własności lub kopiowania tych informacji. Ponadto pracownik musi zwrócić wspomniane nośniki natychmiast po zakończeniu zadań, które spowodowały ich tymczasowe wykorzystanie, a w każdym razie po zakończeniu współpracy jego firmy z Grupo Azpiaran.

Wszystkie te obowiązki pozostają w mocy po zakończeniu działalności prowadzonej przez osoby zewnętrzne na rzecz Grupo Azpiaran.

Niewypełnienie tych obowiązków może stanowić przestępstwo ujawnienia tajemnic.

Aby zapewnić bezpieczeństwo danych osobowych, osoby z organizacji dostawczej powinny przestrzegać następujących zasad postępowania, oprócz wyżej wymienionych zasad:

- Mogą tworzyć pliki tylko wtedy, gdy jest to konieczne do wykonywania ich pracy. Te tymczasowe pliki nie mogą być nigdy zapisywane na lokalnych dyskach komputerów użytkowników i muszą być niszczone, gdy przestaną być przydatne do celów, dla których zostały utworzone.
- Dane osobowe nie mogą być przechowywane na lokalnych dyskach twardych komputerów użytkowników.
- Wynoszenie nośników i dokumentów (w tym wysyłanie wiadomości e-mail) poza pomieszczenia, w których znajdują się te informacje, może być dozwolone wyłącznie przez Grupo Azpiaran i odbywa się zgodnie z określoną procedurą.

- Nośniki i dokumenty muszą umożliwiać identyfikację rodzaju zawartych w nich informacji, być zinwentaryzowane i przechowywane w miejscu o ograniczonym dostępie dla osób upoważnionych.
- Przekazywanie danych osobowych objętych szczególną ochroną (np. dotyczących zdrowia) za pośrednictwem sieci telekomunikacyjnych (np. poczty elektronicznej) odbywa się poprzez szyfrowanie tych danych lub stosowanie innych mechanizmów gwarantujących, że informacje nie będą zrozumiałe ani nie będą mogły być manipulowane przez osoby trzecie.

3.3. Własność intelektualna

Zapewnione zostanie przestrzeganie ograniczeń prawnych dotyczących wykorzystania materiałów chronionych przepisami dotyczącymi własności intelektualnej.

Użytkownicy mogą korzystać wyłącznie z materiałów zatwierdzonych przez Grupo Azpiaran do wykonywania swoich obowiązków.

Surowo zabrania się korzystania z oprogramowania bez odpowiedniej licencji w systemach informatycznych Grupo Azpiaran.

Zabrania się również wykorzystywania, reprodukcji, przekazywania, przekształcania lub publicznego udostępniania wszelkiego rodzaju dzieł lub wynalazków chronionych prawem własności intelektualnej bez odpowiedniej pisemnej zgody.

Grupo Azpiaran zezwala wyłącznie na wykorzystanie materiałów wyprodukowanych przez siebie lub materiałów autoryzowanych lub dostarczonych mu przez ich właściciela, zgodnie z uzgodnionymi warunkami i przepisami obowiązującego prawa.

3.4. Wymiana informacji

W żadnym wypadku nikt nie może ukrywać ani manipulować swoją tożsamością.

Dystrybucja informacji w formie elektronicznej lub fizycznej będzie odbywać się za pomocą środków określonych w umowie o świadczenie usług w tym celu i wyłącznie w celu ułatwienia wykonywania funkcji związanych z tą umową. Grupa Azpiaran zastrzega sobie prawo, w zależności od zidentyfikowanego ryzyka, do wprowadzenia środków kontroli, rejestracji i audytu tych środków rozpowszechniania.

W odniesieniu do wymiany informacji w ramach umowy o świadczenie usług za nieuprawnione uznaje się następujące działania:

- Przesyłanie lub odbieranie materiałów chronionych prawem autorskim z naruszeniem ustawy o ochronie własności intelektualnej.
- Przesyłanie lub odbieranie wszelkiego rodzaju materiałów pornograficznych, o charakterze jednoznacznie seksualnym, oświadczeń o charakterze dyskryminacji rasowej oraz wszelkiego rodzaju oświadczeń lub wiadomości, które można zaklasyfikować jako obraźliwe lub niezgodne z prawem.
- Przekazywanie chronionych informacji nieuprawnionym osobom trzecim.
- Przesyłanie lub odbieranie aplikacji niezwiązanych z działalnością firmy.

- Uczestnictwo w działaniach internetowych, takich jak grupy dyskusyjne, gry lub inne działania, które nie są bezpośrednio związane ze świadczeniem usług.

Wszelkie działania, które mogą zaszkodzić wizerunkowi i reputacji Grupo Azpiaran, są zabronione w Internecie i w każdym innym miejscu.

3.5. Właściwe wykorzystanie zasobów

Organizacja świadcząca usługi zobowiązuje się do okresowego informowania Grupo Azpiaran o zasobach, za pomocą których świadczy usługi.

Organizacja dostawcza zobowiązuje się do wykorzystywania zasobów przeznaczonych do świadczenia usługi zgodnie z warunkami, dla których zostały one zaprojektowane i wdrożone.

Zasoby, które Grupo Azpiaran udostępnia osobom zewnętrznym, niezależnie od ich rodzaju (sprzęt komputerowy, dane, oprogramowanie, sieci, systemy komunikacyjne itp.), są dostępne wyłącznie w celu wypełnienia obowiązków i realizacji celów operacyjnych, dla których zostały dostarczone. Grupo Azpiaran zastrzega sobie prawo do wdrożenia mechanizmów kontroli i audytu w celu weryfikacji właściwego wykorzystania tych zasobów.

Wszystkie urządzenia dostawcy, które łączą się z siecią produkcyjną Grupo Azpiaran, będą pochodzić od zatwierdzonych marek i modeli. Dostawca udostępni Grupo Azpiaran te urządzenia, aby ta mogła koordynować instalację zatwierdzonego oprogramowania i odpowiednio je skonfigurować.

Każdy plik wprowadzony do sieci Grupo Azpiaran lub do dowolnego urządzenia podłączonego do niej za pośrednictwem nośników automatycznych, Internetu, poczty elektronicznej lub innych środków musi spełniać wymagania określone w niniejszych zasadach, a w szczególności te dotyczące własności intelektualnej, ochrony danych osobowych i kontroli złośliwego oprogramowania.

Wszystkie aktywa należy zwrócić Grupo Azpiaran bez nieuzasadnionej zwłoki po zakończeniu umowy. Wszystkie komputery osobiste, na których Grupo Azpiaran zainstalowało oprogramowanie, należy dostarczyć do Grupo Azpiaran w celu sformatowania dysku twardego po zakończeniu świadczenia usługi.

Wyraźnie zabrania się:

- Wykorzystywanie zasobów dostarczonych przez Grupo Azpiaran do działań niezwiązanych z celem usługi.
- Podłączanie do sieci produkcyjnej Grupo Azpiaran urządzeń i/lub aplikacji, które nie są określone jako część oprogramowania lub standardów własnych zasobów informatycznych.
- Wprowadzanie do systemów informatycznych lub sieci korporacyjnej Grupo Azpiaran treści obscenicznych, zawierających groźby, niemoralnych lub obraźliwych.
- Celowe wprowadzanie do sieci korporacyjnej Grupo Azpiaran jakiegokolwiek złośliwego oprogramowania (wirusów, robaków, trojanów, programów szpiegujących, oprogramowania ransomware itp.), urządzeń logicznych, urządzeń fizycznych lub jakichkolwiek innych sekwencji poleceń, które powodują lub mogą powodować jakiekolwiek zakłócenia lub uszkodzenia zasobów

informatycznych. Wszystkie osoby mające dostęp do sieci Grupy Azpiaran są zobowiązane do korzystania z aktualnych programów antywirusowych.

- Uzyskiwanie bez wyraźnej zgody innych praw lub dostępu niż te, które zostały im przydzielone przez Grupo Azpiaran.
- Uzyskiwanie bez wyraźnej zgody dostępu do obszarów o ograniczonym dostępie w systemach informatycznych Grupo Azpiaran.
- Zniekształcanie lub fałszowanie rejestrów „log" systemów informatycznych Grupo Azpiaran.
- Odszyfrowywanie bez wyraźnej zgody haseł, systemów lub algorytmów szyfrujących oraz wszelkich innych elementów bezpieczeństwa wykorzystywanych w procesach telematycznych Grupo Azpiaran
- Posiadanie, opracowywanie lub uruchamianie programów, które mogłyby zakłócać pracę innych użytkowników lub uszkadzać lub zmieniać zasoby informatyczne Grupo Azpiaran
- Niszczenie, modyfikowanie, unieruchamianie lub inne formy uszkadzania danych, programów lub dokumentów elektronicznych zawierających informacje chronione (czynności te mogą stanowić przestępstwo).
- Przechowywanie chronionych informacji na lokalnych dyskach komputerów użytkowników.

3.6. Obowiązki użytkownika

Organizacje świadczące usługi muszą zapewnić, aby wszystkie osoby wykonujące zadania dla Grupo Azpiaran przestrzegały następujących podstawowych zasad w ramach swojej działalności:

- Każda osoba mająca dostęp do informacji Grupo Azpiaran jest odpowiedzialna za działalność wykonywaną przy użyciu swojego identyfikatora użytkownika i wszystko, co z tego wynika. Dlatego też konieczne jest, aby każda osoba kontrolowała systemy uwierzytelniania powiązane z jej identyfikatorem użytkownika, gwarantując, że hasło powiązane z tym identyfikatorem jest znane wyłącznie użytkownikowi i nie może być ujawniane innym osobom pod żadnym pozorem.
- Użytkownicy nie powinni używać identyfikatora innego użytkownika, nawet jeśli posiadają zgodę właściciela.
- Użytkownicy znają i stosują istniejące wymagania i procedury dotyczące przetwarzanych informacji.

Każda osoba mająca dostęp do chronionych informacji musi przestrzegać następujących wytycznych dotyczących zarządzania hasłami:

- Wybierać hasła wysokiej jakości, czyli trudne do odgadnięcia przez innych użytkowników.
- W przypadku podejrzenia, że hasło jest znane innym użytkownikom, należy poprosić o jego zmianę.
- Zmieniaj hasła co najmniej raz na 90 dni i unikaj ponownego używania starych haseł.
- Zmieniać domyślne i tymczasowe hasła przy pierwszym logowaniu.
- Unikaj umieszczania haseł w automatycznych procesach logowania (np. tych przechowywanych w przeglądarkach).

- Zgłaszać wszelkie incydenty związane z bezpieczeństwem haseł, takie jak utrata, kradzież lub podejrzenie naruszenia poufności.

Każda osoba mająca dostęp do informacji chronionych powinna zadbać o to, aby sprzęt był zabezpieczony, gdy pozostaje bez nadzoru.

Każda osoba mająca dostęp do informacji chronionych powinna przestrzegać co najmniej poniższych zasad dotyczących czystego biurka, aby chronić dokumenty papierowe, nośniki komputerowe i przenośne urządzenia pamięci masowej oraz zmniejszyć ryzyko nieuprawnionego dostępu, utraty i uszkodzenia informacji, zarówno w normalnych godzinach pracy, jak i poza nimi:

- Przechowywać dokumenty papierowe i nośniki danych pod kluczem, gdy nie są używane, zwłaszcza poza godzinami pracy.
- Blokować sesje użytkownika lub wyłączać komputer, gdy pozostawia się go bez nadzoru.
- Zabezpieczyć zarówno punkty odbioru i wysyłki informacji (poczta tradycyjna, skanery i faksy), jak i urządzenia do kopiowania (kserokopiarki, faksy i skanery). Odpowiedzialność za powielanie lub wysyłanie informacji za pomocą tego typu urządzeń spoczywa na użytkowniku.
- Bez zbędnej zwłoki usuwać wszelkie chronione informacje po ich wydrukowaniu.
- Niszczenie informacji chronionych, gdy nie są już potrzebne.
- Osoby mające dostęp do systemów i/lub informacji Grupo Azpiaran nie mogą, bez pisemnej zgody, przeprowadzać testów w celu wykrycia i/lub wykorzystania domniemanej słabości, zdarzenia lub incydentu związanego z bezpieczeństwem.
- Żadna osoba mająca dostęp do systemów i/lub informacji Grupo Azpiaran nie będzie próbowała bez wyraźnej, pisemnej zgody naruszać systemu bezpieczeństwa i uprawnień. Zabrania się przechwytywania ruchu sieciowego przez użytkowników, chyba że przeprowadzane są zadania audytowe zatwierdzone na piśmie.

Wszystkie osoby mające dostęp do chronionych informacji muszą przestrzegać następujących zasad postępowania:

- Chronić chronione informacje przed nieuprawnionym ujawnieniem, modyfikacją, zniszczeniem lub niewłaściwym wykorzystaniem, zarówno przypadkowym, jak i umyślnym.
- Chronić wszystkie systemy informatyczne i sieci telekomunikacyjne przed nieuprawnionym dostępem lub wykorzystaniem, przerwami w działaniu, zniszczeniem, niewłaściwym wykorzystaniem lub kradzieżą.
- Posiadać niezbędne uprawnienia, aby uzyskać dostęp do systemów informatycznych i/lub informacji.

3.7. Sprzęt użytkownika

Organizacje świadczące usługi muszą zapewnić, że cały sprzęt komputerowy użytkownika wykorzystywany do uzyskiwania dostępu do chronionych informacji spełnia następujące normy:

- W przypadku braku aktywności użytkownika sprzęt powinien automatycznie zablokować się w ciągu maksymalnie 15 minut.
- Żadne urządzenie użytkownika nie może posiadać narzędzi, które mogłyby naruszyć systemy bezpieczeństwa i uprawnienia.

- Sprzęt użytkownika będzie konserwowany zgodnie ze specyfikacjami producenta.
- Wszystkie urządzenia użytkowników będą odpowiednio chronione przed złośliwym oprogramowaniem:

o Oprogramowanie antywirusowe powinno być zainstalowane i używane na wszystkich komputerach osobistych w celu zmniejszenia ryzyka operacyjnego związanego z wirusami lub innym złośliwym oprogramowaniem.

o Należy aktualizować oprogramowanie do najnowszych dostępnych wersji zabezpieczeń.

o Oprogramowanie antywirusowe powinno być zawsze włączone i aktualizowane.

Należy zwrócić szczególną uwagę na bezpieczeństwo wszystkich urządzeń mobilnych użytkowników, które zawierają informacje chronione lub umożliwiają dostęp do nich w jakikolwiek sposób:

- Sprawdzając, czy nie zawierają one więcej informacji niż jest to absolutnie konieczne.
- Zapewniając stosowanie kontroli dostępu do tych informacji.
- Ograniczając dostęp do tych informacji w obecności osób niebędących zaangażowanych w świadczenie usługi.
- Transportując sprzęt w pokrowcach, walizkach lub podobnych opakowaniach, które zapewniają odpowiednią ochronę przed czynnikami środowiskowymi.

3.8. Zarządzanie sprzętem komputerowym

Organizacje świadczące usługi muszą zapewnić, że cały sprzęt dostarczony przez Grupo Azpiaran do świadczenia usług, niezależnie od jego rodzaju, jest odpowiednio zarządzany. W tym celu muszą przestrzegać następujących zasad:

- Organizacja świadcząca usługi powinna prowadzić aktualny wykaz sprzętu dostarczonego przez Grupo Azpiaran oraz osób korzystających z tych aktywów lub osób odpowiedzialnych za nie, w przypadku gdy aktywa nie są przeznaczone do użytku jednoosobowego. Wykaz ten może być wymagany przez Grupo Azpiaran.
- W przypadku gdy organizacja dostawcza chce ponownie przydzielić sprzęt Grupo Azpiaran, który zawierał informacje chronione, musi go tymczasowo zwrócić, aby przed ponownym przydzieleniem można było przeprowadzić niezbędne procedury bezpiecznego usuwania danych.
- W przypadku, gdy organizacja dostawcza chce wyrejestrować niektóre z urządzeń Grupo Azpiaran, które otrzymała, zawsze musi je zwrócić, aby Grupo Azpiaran mogło odpowiednio przetworzyć takie wyrejestrowanie.
- W przypadku, gdy organizacja dostawcza zaprzestanie świadczenia usług, musi zwrócić Grupo Azpiaran wszystkie otrzymane urządzenia, zgodnie z postanowieniami odpowiednich umów o świadczenie usług. Tylko w przypadku dokumentów papierowych i nośników informatycznych organizacja dostawcza może przystąpić do ich bezpiecznego usunięcia, o czym musi powiadomić Grupo Azpiaran.

4. Szczegółowe wytyczne

4.1. Zakres stosowania

Wszystkie organizacje świadczące usługi muszą przestrzegać, oprócz ogólnych zasad, szczegółowych zasad zawartych w niniejszym paragrafie, które mają zastosowanie w każdym przypadku, w zależności od charakterystyki usług świadczonych na rzecz Grupo Azpiaran.

Rodzaje usług, które są brane pod uwagę, są wskazane poniżej.

- Miejsce świadczenia usługi: W zależności od głównego miejsca świadczenia usług rozróżnia się dwa przypadki:
  - Grupo Azpiaran: Organizacja świadcząca usługi świadczy je głównie z siedzibą Grupo Azpiaran.
  - Zdalnie: Organizacja świadcząca usługi świadczy je głównie we własnych siedzibach, mimo że niektóre działania mogą być wykonywane w siedzibie Grupo Azpiaran.
- Własność wykorzystywanej infrastruktury ICT: W zależności od tego, kto jest właścicielem głównej infrastruktury ICT (komunikacja, sprzęt użytkowników, oprogramowanie) wykorzystywanej do świadczenia usługi, rozróżnia się dwa przypadki:
  - Grupo Azpiaran
  - Organizacja świadcząca usługi.
- Poziom dostępu do systemów Grupo Azpiaran: W zależności od poziomu dostępu do systemów informatycznych Grupo Azpiaran wyróżnia się trzy przypadki:
  - Z dostępem uprzywilejowanym: Świadczona usługa wymaga uprzywilejowanego dostępu do systemów informatycznych Grupo Azpiaran, z możliwością zarządzania tymi systemami i/lub przetwarzanymi przez nie danymi produkcyjnymi.
  - Z dostępem na poziomie użytkownika: Świadczona usługa wymaga korzystania z systemów informatycznych Grupo Azpiaran, dlatego osoby świadczące usługę posiadają konta użytkowników, które umożliwiają im dostęp do niektórych z tych systemów z typowymi uprawnieniami.
  - Bez dostępu: Świadczona usługa nie wymaga korzystania z systemów informatycznych Grupo Azpiaran, więc osoby świadczące usługę nie mają kont użytkowników w tych systemach.

W zależności od jednej z trzech kategorii, do których należy dana usługa, organizacja świadcząca usługę musi spełniać, oprócz ogólnych norm bezpieczeństwa, również normy szczegółowe określone w sekcjach wskazanych w poniższej tabeli:

	MIEJSCE		INFRASTRUKTURA		DOSTĘP		
	Grupa Azpiaran	Zdalny	Grupa Azpiaran	Organizacja dostawcza	Uprzywilejowana	Normal	Brak dostępu
Wybór osób	NIE	NIE	NIE	NIE	TAK	NIE	NIE

	MIEJSCE		INFRASTRUKTURA		DOSTĘP		
	Grupa Azpiaran	Zdalny	Grupa Azpiaran	Organizacja dostawcza	Uprzywilejowana	Normal	Brak dostępu
audyt bezpieczeństwa	NIE	NIE	NIE	NIE	TAK	NIE	NIE
zgłaszanie incydentów	TAK	TAK	TAK	NIE	TAK	TAK	NIE
bezpieczeństwo fizyczne	NIE	TAK	NIE	NIE	NIE	NIE	NIE
zarządzanie aktywami	NIE	NIE	NIE	TAK	NIE	NIE	NIE
architektura bezpieczeństwo	NIE	NIE	NIE	TAK	TAK	TAK	NIE
bezpieczeństwo systemy	NIE	NIE	NIE	TAK	NIE	NIE	NIE
bezpieczeństwo sieci	NIE	NIE	NIE	TAK	NIE	NIE	NIE
identyfikowalność wykorzystania systemów	NIE	NIE	NIE	TAK	TAK	NIE	NIE
kontrola i zarządzanie tożsamością i dostępem	NIE	NIE	NIE	TAK	NIE	NIE	NIE
zarządzanie zmianami	NIE	NIE	NIE	TAK	TAK	TAK	NIE
zarządzanie zmianami technicznymi	NIE	NIE	NIE	NIE	TAK	NIE	NIE
bezpieczeństwo w rozwoju	NIE	NIE	NIE	NIE	TAK	TAK	NIE
zarządzanie sytuacjami awaryjnymi	NIE	NIE	NIE	TAK	NIE	NIE	NIE

4.2. Wybór osób

Organizacja świadcząca usługi musi zweryfikować doświadczenie zawodowe osób przydzielonych do świadczenia usług, gwarantując Grupo Azpiaran, że w przeszłości nie zostały one ukarane za nieprawidłowości w wykonywaniu zawodu ani nie były zamieszane w incydenty związane z poufnością przetwarzanych informacji, które skutkowały nałożeniem jakiejkolwiek kary.
Organizacja świadcząca usługi musi zagwarantować Grupo Azpiaran możliwość natychmiastowego zwolnienia osób przydzielonych do świadczenia usług, w przypadku których Grupo Azpiaran chce skorzystać z prawa weta, zgodnie z warunkami określonymi w punkcie „3.1. Świadczenie usług".

4.3. Audyt bezpieczeństwa

Organizacja świadcząca usługi musi umożliwić Grupo Azpiaran przeprowadzenie wymaganych audytów bezpieczeństwa, współpracując z zespołem audytowym i udostępniając wszystkie wymagane dowody i rejestry.
Zakres i zakres każdego audytu zostanie wyraźnie określony przez Grupo Azpiaran w każdym przypadku. Audyty będą przeprowadzane zgodnie z planem uzgodnionym w każdym przypadku z organizacją świadczącą usługę.
Grupo Azpiaran zastrzega sobie prawo do przeprowadzania dodatkowych audytów nadzwyczajnych, o ile istnieją ku temu konkretne powody.

4.4. Zgłaszanie incydentów

W przypadku wykrycia jakiejkolwiek luki w zabezpieczeniach, zdarzenia i/lub incydentu związanego z bezpieczeństwem informacji należy niezwłocznie powiadomić o tym Grupo Azpiaran za pośrednictwem skrzynki pocztowej.
Każdy użytkownik może zgłaszać za pośrednictwem wspomnianej skrzynki pocztowej wszelkie zdarzenia, sugestie, luki w zabezpieczeniach itp., które mogą mieć związek z bezpieczeństwem informacji i wytycznymi zawartymi w niniejszych przepisach, o których posiada wiedzę.
Za pośrednictwem wspomnianej skrzynki pocztowej należy zgłaszać wszelkie wykryte incydenty, które mają lub mogą mieć wpływ na bezpieczeństwo danych osobowych (np. utrata list i/lub nośników informatycznych, podejrzenia nadużycia dostępu autoryzowanego przez inne osoby, odzyskiwanie danych z kopii zapasowych itp.
Wspomniana skrzynka pocztowa centralizuje gromadzenie, analizę i zarządzanie zgłoszonymi incydentami.
W przypadku braku dostępu do skrzynki należy skorzystać z kanałów komunikacji ustanowionych w ramach samej usługi, tak aby to przedstawiciel Grupo Azpiaran zgłosił incydent związany z bezpieczeństwem.

4.5. Bezpieczeństwo fizyczne

Siedziba powinna być zamknięta i wyposażona w system kontroli dostępu.
Powinna istnieć jakaś forma kontroli odwiedzających, przynajmniej w obszarach ogólnodostępnych i/lub przeznaczonych do załadunku i rozładunku.

Siedziba powinna być wyposażona co najmniej w odpowiednie systemy wykrywania i gaszenia pożarów oraz powinna być zbudowana w taki sposób, aby zapewnić wystarczającą odporność na zalanie.

Jeśli przechowywane są jakiekolwiek kopie zapasowe, systemy przechowujące i/lub przetwarzające te informacje powinny znajdować się w specjalnie chronionym obszarze, który obejmuje co najmniej następujące środki bezpieczeństwa:

- Obszar specjalnie chroniony powinien posiadać system kontroli dostępu niezależny od systemu stosowanego w siedzibie.
- Dostęp osób z zewnątrz do obszarów specjalnie chronionych będzie ograniczony. Dostęp ten będzie przyznawany wyłącznie w razie konieczności i po uzyskaniu upoważnienia, zawsze pod nadzorem upoważnionych osób.
- Prowadzony będzie rejestr wszystkich wejść osób z zewnątrz.
- Osoby z zewnątrz nie będą mogły przebywać ani wykonywać prac w obszarach objętych szczególną ochroną bez nadzoru.
- Spożywanie posiłków lub napojów w tych specjalnie chronionych obszarach będzie zabronione.
- Systemy znajdujące się w tych obszarach muszą być wyposażone w zabezpieczenia przed awariami zasilania.

4.6. Zarządzanie aktywami

Organizacja świadcząca usługi powinna posiadać aktualny rejestr aktywów, w którym można zidentyfikować aktywa wykorzystywane do świadczenia usług.

Wszystkie aktywa wykorzystywane do świadczenia usług muszą mieć wyznaczoną osobę odpowiedzialną, która musi zapewnić, że aktywa te spełniają minimalne wymogi bezpieczeństwa ustanowione przez organizację świadczącą usługi, a przynajmniej wymogi określone w niniejszych przepisach.

Organizacja świadcząca usługi powinna powiadomić Grupo Azpiaran o wycofaniu aktywów wykorzystywanych do świadczenia usług. Jeśli dane aktywa zawierają inne mienie Grupo Azpiaran (sprzęt, oprogramowanie lub inne rodzaje aktywów), należy je przekazać Grupo Azpiaran przed wycofaniem, aby Grupo Azpiaran mogło przystąpić do wycofania aktywów będących jego własnością.

W przypadku gdy aktywa zawierały informacje chronione, organizacja dostawcza musi dokonać wycofania aktywów, zapewniając bezpieczne usunięcie tych informacji poprzez zastosowanie funkcji bezpiecznego kasowania lub fizyczne zniszczenie aktywów, tak aby informacje, które zawierały, nie mogły zostać odzyskane.

4.7. Architektura bezpieczeństwa

W przypadku gdy organizacja świadcząca usługi wykonuje prace związane z rozwojem i/lub testowaniem aplikacji dla Grupo Azpiaran lub z wykorzystaniem informacji chronionych,

środowiska, w których prowadzone są takie działania, muszą być odizolowane od siebie, a także od środowisk produkcyjnych, w których przechowywane lub przetwarzane są informacje chronione.

Wszelki dostęp do systemów informatycznych, w których przechowywane lub przetwarzane są informacje chronione, musi być zabezpieczony co najmniej zaporą ogniową, która ogranicza możliwość połączenia się z nimi.

Systemy informatyczne, w których przechowywane lub przetwarzane są informacje szczególnie wrażliwe, muszą być odizolowane od pozostałych.

4.8. Bezpieczeństwo systemów

Systemy informatyczne przechowujące lub przetwarzające informacje chronione muszą rejestrować najważniejsze zdarzenia związane z ich funkcjonowaniem. Rejestry tych działań będą uwzględnione w przepisach dotyczących kopii zapasowych organizacji dostawczej.

Zegary systemów organizacji dostawczej, które przetwarzają lub przechowują chronione informacje, będą zsynchronizowane między sobą oraz z czasem oficjalnym.

Organizacja świadcząca usługi zapewni odpowiednie zarządzanie wydajnością systemów informatycznych przechowujących lub przetwarzających informacje chronione, zapobiegając potencjalnym przestojom lub nieprawidłowemu działaniu tych systemów z powodu przeciążenia zasobów.

Systemy informatyczne przechowujące lub przetwarzające informacje chronione będą odpowiednio chronione przed złośliwym oprogramowaniem poprzez zastosowanie następujących środków ostrożności:

- Systemy będą aktualizowane do najnowszych dostępnych wersji zabezpieczeń w środowiskach programistycznych, testowych i produkcyjnych.
- Oprogramowanie antywirusowe powinno być zainstalowane i używane na wszystkich serwerach i komputerach osobistych w celu zmniejszenia ryzyka związanego ze złośliwym oprogramowaniem.
- Oprogramowanie antywirusowe powinno być zawsze włączone i aktualizowane.

Organizacja świadcząca usługi ustanowi zasady tworzenia kopii zapasowych, które zapewnią zabezpieczenie wszelkich danych lub informacji istotnych dla świadczonej usługi, z częstotliwością raz w tygodniu.

W przypadku korzystania z poczty elektronicznej w związku ze świadczoną usługą organizacja świadcząca usługi powinna przestrzegać następujących zasad:

- Nie zezwala się na przekazywanie informacji chronionych za pośrednictwem poczty elektronicznej, chyba że komunikacja elektroniczna jest szyfrowana, a wysyłka została zatwierdzona na piśmie.
- Nie zezwala się na przesyłanie pocztą elektroniczną informacji zawierających dane osobowe podlegające szczególnej ochronie (np. dotyczące zdrowia), chyba że komunikacja elektroniczna jest szyfrowana, a wysyłka została zatwierdzona na piśmie.

- W przypadku korzystania z poczty elektronicznej Grupo Azpiaran w celu świadczenia usług należy przestrzegać co najmniej następujących zasad:
- Poczta elektroniczna będzie traktowana jako kolejne narzędzie pracy udostępnione wyłącznie w celu świadczenia zamówionej usługi. Uznanie to uprawnia Grupo Azpiaran do wdrożenia systemów kontroli mających na celu zapewnienie ochrony i właściwego wykorzystania tego zasobu. Uprawnienie to będzie jednak wykonywane z poszanowaniem godności osób i ich prawa do prywatności.
- System poczty elektronicznej Grupo Azpiaran nie może być wykorzystywany do wysyłania wiadomości o charakterze oszukańczym, obscenicznym, zawierających groźby lub innych podobnych komunikatów.
- Użytkownicy nie powinni tworzyć, wysyłać ani przekazywać dalej wiadomości reklamowych lub piramidalnych (wiadomości rozsyłanych do wielu użytkowników).

Dostęp do systemów informatycznych, które przechowują lub przetwarzają informacje chronione, musi zawsze odbywać się w sposób uwierzytelniony, przynajmniej poprzez użycie identyfikatora osoby i powiązanego hasła.

Systemy informatyczne przechowujące lub przetwarzające informacje chronione muszą być wyposażone w systemy kontroli dostępu, które ograniczają dostęp do tych informacji wyłącznie do osób zatrudnionych w służbie.

Sesje dostępu do systemów informatycznych przechowujących lub przetwarzających informacje chronione powinny być automatycznie blokowane po upływie określonego czasu bezczynności użytkowników.

W przypadku korzystania z oprogramowania dostarczonego przez Grupo Azpiaran należy przestrzegać następujących zasad:

- Wszystkie osoby uzyskujące dostęp do systemów informatycznych Grupo Azpiaran powinny korzystać wyłącznie z dostarczonych wersji oprogramowania i przestrzegać zasad ich użytkowania.
- Wszyscy użytkownicy mają zakaz instalowania nielegalnych kopii jakiegokolwiek oprogramowania.
- Zabrania się korzystania z oprogramowania, które nie zostało zatwierdzone przez Grupo Azpiaran.
- Zabrania się również odinstalowywania jakichkolwiek programów zainstalowanych przez Grupo Azpiaran.

4.9. Bezpieczeństwo sieci

Sieci, przez które przepływają chronione informacje, muszą być odpowiednio zarządzane i kontrolowane, tak aby nie istniały żadne niekontrolowane dostępy ani połączenia, których ryzyko nie jest odpowiednio zarządzane przez organizację dostarczającą usługi.

Usługi dostępne w sieciach, przez które przepływają chronione informacje, powinny być w miarę możliwości ograniczone.

Sieci umożliwiające dostęp do infrastruktury ICT Grupo Azpiaran muszą być odpowiednio chronione i muszą spełniać następujące warunki:

- Dostęp osób, użytkowników zdalnych, do sieci Grupy Azpiaran będzie uzależniony od spełnienia procedur identyfikacji i uwierzytelniania oraz weryfikacji dostępu.
- Połączenia te będą realizowane przez ograniczony czas i za pośrednictwem prywatnych sieci wirtualnych lub linii dedykowanych.
- W przypadku tych połączeń nie będą dozwolone żadne urządzenia komunikacyjne (karty, modemy itp.), które umożliwiają alternatywne, niekontrolowane połączenia.

Dostęp do sieci, przez które przepływają chronione informacje, musi być ograniczony.

Wszystkie urządzenia podłączone do sieci, przez które przepływają chronione informacje, muszą być odpowiednio oznaczone, tak aby ruch sieciowy był identyfikowalny.

Praca zdalna, rozumiana jako dostęp do sieci firmowej z zewnątrz, regulowana jest poprzez zastosowanie następujących przepisów:

- Nie zezwala się na wykorzystywanie sprzętu niekontrolowanego przez Grupo Azpiaran do celów pracy zdalnej.
- Kryteria zezwolenia na pracę zdalną zostaną ustalone w oparciu o potrzeby danego stanowiska pracy.
- Ustanowione zostaną środki niezbędne do bezpiecznego połączenia z siecią firmową.
- Ustanowione zostaną systemy monitorowania i kontroli bezpieczeństwa ustanowionych połączeń.
- Będzie kontrolowane cofanie praw dostępu i zwrot sprzętu po zakończeniu okresu jego użytkowania.

W przypadku korzystania z dostępu do Internetu zapewnianego przez Grupo Azpiaran należy dodatkowo przestrzegać następujących przepisów:

- Internet jest narzędziem pracy. Wszystkie działania w Internecie muszą być związane z zadaniami i czynnościami służbowymi. Użytkownicy nie powinni wyszukiwać ani odwiedzać stron, które nie służą realizacji celów biznesowych Grupo Azpiaran lub wykonywania codziennych obowiązków służbowych.
- Dostęp do Internetu z sieci korporacyjnej będzie ograniczony za pomocą wbudowanych w nią urządzeń kontrolnych. Korzystanie z innych środków połączenia musi zostać wcześniej zatwierdzone i podlega powyższym zasadom dotyczącym korzystania z Internetu.
- Użytkownicy nie powinni używać nazwy, symbolu, logo lub symboli podobnych do symboli Grupo Azpiaran w żadnym elemencie Internetu (poczta elektroniczna, strony internetowe itp.), który nie jest uzasadniony ściśle zawodowymi działaniami.
- Przesyłanie danych z lub do Internetu będzie dozwolone wyłącznie w przypadku, gdy jest to związane z działalnością biznesową. Przesyłanie plików niezwiązanych z tą działalnością (np. pobieranie programów, plików multimedialnych itp.) będzie zabronione.

4.10. Identyfikowalność użytkowania systemów

Dostępy uprzywilejowane będą rejestrowane, a rejestry te będą przechowywane zgodnie z przepisami organizacji dotyczącymi kopii zapasowych.

Rejestrowana będzie aktywność systemów wykorzystywanych do uzyskania takiego uprzywilejowanego dostępu, a rejestry te będą przechowywane zgodnie z przepisami organizacji dotyczącymi kopii zapasowych.

Błędy i awarie zarejestrowane w działalności systemów będą analizowane, a następnie zostaną podjęte niezbędne działania w celu ich usunięcia.

4.11. Kontrola i zarządzanie tożsamością i dostępem

Wszyscy użytkownicy mający dostęp do systemu informatycznego będą dysponować jednym uprawnieniem dostępu składającym się z identyfikatora użytkownika i hasła.

Użytkownicy będą odpowiedzialni za wszelkie działania związane z korzystaniem z ich autoryzowanego dostępu.

Użytkownicy nie powinni korzystać z autoryzowanego dostępu innego użytkownika, nawet jeśli posiadają zgodę właściciela.

Użytkownicy nie powinni w żadnym wypadku ujawniać swojego identyfikatora i/lub hasła innej osobie, ani przechowywać go w formie pisemnej w miejscu widocznym lub dostępnym dla osób trzecich.

Minimalna długość hasła powinna wynosić 6 znaków i nie powinno ono zawierać imienia, nazwiska ani identyfikatora użytkownika. Należy je zmieniać co 45 dni i nie powtarzać co najmniej 8 poprzednich haseł.

Ponadto hasła powinny być złożone i trudne do odgadnięcia, dlatego też powinny składać się z kombinacji co najmniej 3 z 4 poniższych opcji w pierwszych 8 znakach:

- Wielkie litery
- Małe litery
- Cyfry
- Znaki specjalne

Zaleca się stosowanie następujących wytycznych dotyczących wyboru haseł:

- Nie należy używać znanych słów ani słów, które mogą być kojarzone z daną osobą, na przykład imienia.
- Hasło nie powinno odnosić się do żadnego rozpoznawalnego pojęcia, przedmiotu lub idei. Dlatego należy unikać używania w hasłach ważnych dat, dni tygodnia, miesięcy roku, imion osób, numerów telefonów itp.
- Hasło powinno być praktycznie niemożliwe do odgadnięcia. Jednocześnie powinno być łatwe do zapamiętania przez użytkownika. Dobrym przykładem jest użycie akronimu jakiegoś wyrażenia lub frazy.

Organizacja dostarczająca dane powinna zapewnić, że okresowo sprawdzane jest, czy dostęp do chronionych informacji mają wyłącznie osoby do tego uprawnione.

W przypadkach, w których dostęp uzyskuje się również do systemów informatycznych Grupo Azpiaran, należy dodatkowo uwzględnić następujące przepisy:

- Żaden użytkownik nie otrzyma identyfikatora dostępu do systemów Grupo Azpiaran, dopóki nie zaakceptuje na piśmie obowiązujących przepisów bezpieczeństwa.
- Użytkownicy będą mieli dostęp wyłącznie do tych danych i zasobów, które są im niezbędne do wykonywania swoich obowiązków.
- Jeśli system nie zażąda tego automatycznie, użytkownik musi zmienić tymczasowe hasło przypisane przy pierwszym prawidłowym logowaniu do systemu.
- Jeśli system nie zażąda tego automatycznie, użytkownik musi zmienić swoje hasło co najmniej raz na 90 dni.
- Tymczasowe uprawnienia dostępu będą konfigurowane na krótki okres czasu. Po upływie tego okresu zostaną one wyłączone w systemach.
- W odniesieniu do danych osobowych wyłącznie osoby upoważnione do tego mogą przyznawać, zmieniać lub cofać uprawnienia dostępu do danych i zasobów, zgodnie z kryteriami ustalonymi przez osobę odpowiedzialną za plik.
- Jeśli użytkownik podejrzewa, że jego uprawniony dostęp (identyfikator użytkownika i hasło) jest wykorzystywany przez inną osobę, powinien zmienić hasło i zgłosić ten incydent na adres e-mail Grupo Azpiaran

4.12. Zarządzanie zmianami

Wszelkie zmiany w infrastrukturze ICT muszą być kontrolowane i autoryzowane, aby zagwarantować, że nie zawiera ona elementów niekontrolowanych.

Należy sprawdzić, czy wszystkie nowe elementy wprowadzone do infrastruktury ICT organizacji dostawcy wykorzystywanej do świadczenia usług działają prawidłowo i spełniają cele, dla których zostały włączone.

4.13. Techniczne zarządzanie zmianami

Wszelkie zmiany należy wprowadzać zgodnie z formalnie ustaloną i udokumentowaną procedurą, która gwarantuje podjęcie odpowiednich kroków w celu wprowadzenia zmiany.

Procedura zarządzania zmianami powinna gwarantować minimalizację zmian w infrastrukturze ICT, ograniczając je do tych, które są absolutnie niezbędne.

Wszystkie zmiany należy przetestować przed ich wdrożeniem w środowisku produkcyjnym, aby sprawdzić, czy nie powodują one niepożądanych lub nieprzewidzianych skutków ubocznych dla funkcjonowania i bezpieczeństwa infrastruktury ICT.

Organizacje świadczące usługi powinny skanować i łagodzić podatności techniczne występujące w infrastrukturze wykorzystywanej do świadczenia usług, informując Grupo Azpiaran o wszystkich podatnościach związanych z komponentami krytycznymi.

4.14. Bezpieczeństwo w trakcie rozwoju

Cały proces rozwoju oprogramowania zlecany na zewnątrz będzie kontrolowany i nadzorowany przez Grupo Azpiaran.

W całym cyklu życia oprogramowania, od projektu, przez rozwój, wdrożenie i eksploatację, zostaną wdrożone mechanizmy identyfikacji, uwierzytelniania, kontroli dostępu, audytu i integralności.

Specyfikacje oprogramowania muszą wyraźnie zawierać wymagania bezpieczeństwa, które należy spełnić w każdym przypadku.

Opracowywane oprogramowanie będzie musiało zawierać funkcje sprawdzania poprawności danych wejściowych, które będą weryfikować, czy dane są prawidłowe i odpowiednie, oraz zapobiegać wprowadzaniu kodu wykonywalnego.

Procesy wewnętrzne opracowane przez aplikacje powinny zawierać wszystkie walidacje niezbędne do zapewnienia, że nie dochodzi do uszkodzenia informacji.

W razie potrzeby należy włączyć funkcje uwierzytelniania i kontroli integralności w komunikacji między różnymi komponentami aplikacji.

Należy ograniczyć informacje wyjściowe oferowane przez aplikacje, gwarantując, że oferowane są tylko te istotne i niezbędne.

Dostęp do kodu źródłowego aplikacji powinien być ograniczony do osób z działu serwisowego.

W środowisku testowym należy wykorzystywać rzeczywiste dane tylko wtedy, gdy zostały one odpowiednio oddzielone lub gdy można zagwarantować, że zastosowane środki bezpieczeństwa są równoważne środkom stosowanym w środowisku produkcyjnym.

Podczas testowania aplikacji należy sprawdzić, czy nie ma niekontrolowanych luk w informacjach i czy za pośrednictwem ustanowionych kanałów przekazywane są wyłącznie przewidziane informacje.

Do środowiska produkcyjnego przenoszone będzie wyłącznie oprogramowanie, które zostało wyraźnie zatwierdzone.

W odniesieniu do usług internetowych należy uwzględnić zarządzanie Top 10 Owasp.

4.15. Zarządzanie sytuacjami awaryjnymi

Usługa musi posiadać plan umożliwiający jej świadczenie nawet w przypadku sytuacji awaryjnych. Plan ten powinien być opracowany w oparciu o zdarzenia, które mogą spowodować przerwy w świadczeniu usługi, oraz prawdopodobieństwo ich wystąpienia.

Organizacja świadcząca usługę powinna być w stanie wykazać wykonalność istniejącego planu awaryjnego.

5. Monitorowanie i kontrola

W celu zapewnienia prawidłowego wykorzystania wyżej wymienionych zasobów, za pomocą odpowiednich mechanizmów formalnych i technicznych, Grupo Azpiaran będzie przeprowadzać kontrole, zarówno okresowe, jak i wtedy, gdy będzie to konieczne ze względów bezpieczeństwa lub świadczenia usług.