1. Przedmiot

Celem niniejszego dokumentu jest opracowanie polityki bezpieczeństwa informacji oraz określenie podstawowych zasad dopuszczalnego wykorzystania informacji i pozostałych zasobów związanych z ich przetwarzaniem.

2. Zakres

Niniejszy dokument ma zastosowanie do następujących zasobów:

- 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 wyżej wymienionych informacji (oprogramowanie, sprzęt komputerowy, sieci komunikacyjne, nośniki informacji, wyposażenie pomocnicze i instalacje).

Przetwarzanie informacji powinno odbywać się z zachowaniem wszystkich środków bezpieczeństwa gwarantujących:

- Poufność: jest to właściwość zapobiegania ujawnianiu informacji osobom lub procesom nieuprawnionym. Poufność oznacza dostęp do informacji wyłącznie przez osoby lub procesy posiadające odpowiednie upoważnienie.
- Integralność: jest to właściwość mająca na celu ochronę danych przed nieuprawnionymi modyfikacjami. Integralność polega na zachowaniu dokładności informacji w takiej postaci, w jakiej zostały one wygenerowane, bez manipulacji lub zmian dokonywanych przez osoby lub procesy nieuprawnione.
- Dostępność: jest to właściwość polegająca na udostępnianiu danych osobom, które powinny mieć do nich dostęp, niezależnie od tego, czy są to osoby, procesy czy aplikacje. Dostępność to dostęp do informacji i systemów przez upoważnione osoby lub procesy w momencie, gdy jest to wymagane.

3. Szczegółowe przepisy

3.1. Właściwe wykorzystanie aktywów

Informacje i pozostałe aktywa z nimi związane powinny być wykorzystywane wyłącznie do celów i zadań, dla których zostały udostępnione użytkownikom.

Wyraźnie zabrania się:

- Wykorzystywanie aktywów dostarczonych przez Grupo Azpiaran do działań niezwiązanych z ich przeznaczeniem.
- Podłączanie do sieci Grupo Azpiaran niehomologowanych urządzeń komputerowych.
- Wprowadzanie do systemów informatycznych lub sieci korporacyjnej Grupo Azpiaran treści obscenicznych, zawierających groźby, niemoralnych lub obraźliwych.

- Celowe wprowadzanie do sieci korporacyjnej Grupo Azpiaran wszelkiego rodzaju złośliwego oprogramowania (wirusów, robaków, trojanów, programów szpiegujących, oprogramowania ransomware itp.), urządzeń logicznych, urządzeń fizycznych lub wszelkiego rodzaju sekwencji poleceń, które powodują lub mogą powodować jakiekolwiek zakłócenia lub uszkodzenia zasobów informatycznych.
- Uzyskiwanie innych praw lub dostępu niż te, które zostały przypisane przez Grupo Azpiaran.
- Uzyskiwanie dostępu do obszarów o ograniczonym dostępie Grupo Azpiaran bez odpowiedniego upoważnienia.
- Rozszyfrowywać hasła, systemy lub algorytmy szyfrujące oraz wszelkie inne elementy zabezpieczeń wykorzystywane w procesach telematycznych Grupo Azpiaran.
- Zniekształcanie lub fałszowanie rejestrów (logów) systemów informatycznych Grupo Azpiaran.
- Posiadanie, opracowywanie lub uruchamianie programów, które mogą zakłócać pracę innych użytkowników, uszkadzać lub zmieniać zasoby informatyczne Grupo Azpiaran
- Niszczenie, zmienianie, unieruchamianie lub inne formy uszkadzania danych, programów lub dokumentów elektronicznych zawierających informacje chronione.
- Przechowywanie chronionych informacji na lokalnych dyskach komputerów użytkowników, z wyjątkiem tymczasowego przechowywania oprogramowania projektu, nad którym pracuje dana osoba.

3.2. Poufność

Użytkownik mający dostęp do informacji Grupo Azpiaran powinien traktować te informacje jako domyślnie chronione. Za informacje niechronione można uznać wyłącznie te informacje, do których użytkownik uzyskał dostęp 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.

Należy zminimalizować liczbę raportów w formie papierowej zawierających informacje chronione i przechowywać je w bezpiecznym miejscu, niedostępnym dla osób nieuprawnionych (np. pod kluczem).

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

Wszystkie te obowiązki pozostają w mocy po zakończeniu współpracy z Grupo Azpiaran.
Niewypełnienie tych obowiązków może stanowić przestępstwo ujawnienia tajemnic.
Oprócz wyżej wymienionych kwestii, w celu zapewnienia bezpieczeństwa danych osobowych użytkownik powinien przestrzegać następujących zasad postępowania:

- Pliki mogą być tworzone wyłącznie wtedy, gdy jest to konieczne do wykonywania pracy. Pliki tymczasowe nie mogą być nigdy zapisywane na lokalnych dyskach komputerów użytkownika i muszą zostać zniszczone, gdy przestaną być przydatne do celów, dla których zostały utworzone. Tymczasowo można zapisywać wyłącznie programowanie projektu rozwojowego, nad którym pracuje dana osoba.
- Dane osobowe nie mogą być przechowywane na lokalnych dyskach komputerów użytkownika.
- Wyprowadzanie nośników i dokumentów poza pomieszczenia, w których znajdują się te informacje, może być zatwierdzone wyłącznie przez osobę odpowiedzialną za bezpieczeństwo (kierownika ds. systemów) zgodnie z środkami bezpieczeństwa zawartymi w niniejszym dokumencie.
- Nośniki i dokumenty muszą umożliwiać identyfikację rodzaju zawartych w nich informacji, być zinwentaryzowane i przechowywane w miejscu o ograniczonym dostępie dla osób nieupoważnionych.
- Przesyłanie informacji chronionych za pośrednictwem sieci telekomunikacyjnych (np. poczty elektronicznej) nie może odbywać się w postaci niezaszyfrowanej. Informacje chronione należy udostępniać osobom trzecim za pośrednictwem SharePoint, szyfrując te dane lub stosując inne mechanizmy gwarantujące, że informacje nie będą zrozumiałe ani nie będą mogły być manipulowane przez osoby trzecie.

3.3. Postępowanie dyscyplinarne

Użytkownik, który nie przestrzega niniejszych przepisów, naraża się na wszczęcie postępowania dyscyplinarnego i, w stosownych przypadkach, sankcji.
Grupa Azpiaran może wprowadzić kontrole w celu sprawdzenia przestrzegania niniejszych zasad, bez uszczerbku dla przestrzegania obowiązujących przepisów dotyczących ochrony danych osobowych i prawa do prywatności.

3.4. Zwrot aktywów

Użytkownik jest zobowiązany do zwrotu wszystkich informacji i aktywów związanych z przetwarzaniem danych, które znajdują się w jego posiadaniu, po zakończeniu współpracy z Grupo Azpiaran.
Dostęp wszystkich użytkowników do informacji i aktywów związanych z ich przetwarzaniem musi zostać anulowany po zakończeniu współpracy z Grupo Azpiaran lub dostosowany do zmian funkcji, które nastąpiły.

3.5. Bezpieczeństwo fizyczne

Dostęp do dokumentacji będzie ograniczony wyłącznie do osób upoważnionych.

Archiwizacja nośników lub dokumentów będzie odbywać się zgodnie z kryteriami przewidzianymi w odpowiednich przepisach prawnych oraz zgodnie z wymaganiami organizacji klientów. Kryteria te muszą gwarantować prawidłowe przechowywanie dokumentów, lokalizację i dostęp do informacji.

Urządzenia służące do przechowywania dokumentów zawierających dane osobowe muszą być wyposażone w mechanizmy uniemożliwiające ich otwarcie. Jeżeli cechy fizyczne tych urządzeń nie pozwalają na zastosowanie tego środka, należy podjąć działania uniemożliwiające dostęp osób nieuprawnionych.

W przypadku gdy nośniki lub dokumenty nie są przechowywane w urządzeniach do przechowywania określonych w poprzednim punkcie, ponieważ są w trakcie przeglądu lub przetwarzania, przed lub po ich archiwizacji, osoba odpowiedzialna za nie powinna je przechowywać i uniemożliwiać w każdym momencie dostęp do nich osobom nieuprawnionym.

Szafy, segregatory lub inne elementy, w których przechowywane są nośniki lub dokumenty, muszą znajdować się w obszarach, do których dostęp jest chroniony drzwiami wyposażonymi w systemy otwierania za pomocą klucza lub innego równoważnego urządzenia. Obszary te muszą pozostawać zamknięte, gdy dostęp do nośników lub dokumentów nie jest konieczny.

Wykonywanie kopii lub reprodukcji dokumentów zawierających dane osobowe podlegające szczególnej ochronie (np. dotyczące zdrowia) może odbywać się wyłącznie pod kontrolą osób upoważnionych przez administratora systemów.

Należy zniszczyć kopie lub reprodukcje w taki sposób, aby uniemożliwić dostęp do zawartych w nich informacji lub ich późniejsze odzyskanie.

W przypadku fizycznego przenoszenia dokumentacji zawartej w pliku należy podjąć środki mające na celu uniemożliwienie dostępu do przenoszonych informacji lub manipulowania nimi.

3.6. Dokumenty, nośniki i urządzenia przenośne

Nośniki, urządzenia przenośne i dokumenty zawierające informacje chronione muszą umożliwiać identyfikację ich zawartości, być zinwentaryzowane i dostępne wyłącznie dla osób upoważnionych przez osobę odpowiedzialną za bezpieczeństwo.

Wynoszenie nośników i dokumentów, w tym tych zawartych w wiadomościach e-mail lub do nich załączonych, poza pomieszczenia kontrolowane przez Grupo Azpiaran musi odbywać się za pośrednictwem korporacyjnego serwisu SharePoint, upoważniając indywidualne, nieudostępniane adresy e-mail. Po zakończeniu konieczności udostępniania dostęp zostanie cofnięty.

Podczas przenoszenia dokumentacji należy podjąć środki mające na celu zapobieżenie kradzieży, utracie lub nieuprawnionemu dostępowi do informacji podczas transportu.

W przypadku wyrzucania jakiegokolwiek dokumentu lub nośnika zawierającego informacje chronione należy przystąpić do jego zniszczenia lub usunięcia, podejmując środki mające na celu zapobieżenie dostępowi do zawartych w nim informacji lub ich późniejszemu odzyskaniu.

Identyfikacja nośników zawierających informacje chronione powinna odbywać się przy użyciu zrozumiałych i znaczących systemów etykietowania, które umożliwiają użytkownikom posiadającym upoważniony dostęp do wspomnianych nośników i dokumentów identyfikację ich zawartości, a utrudniają identyfikację pozostałym osobom.
Ponadto nośniki i urządzenia przenośne powinny być szyfrowane, zwłaszcza gdy znajdują się poza siedzibą organizacji.

3.7. Ochrona przed złośliwym oprogramowaniem

Systemy informatyczne będą aktualizowane zgodnie z najnowszymi dostępnymi aktualizacjami zabezpieczeń.
W mikrokomputerach Apple, Windows i Android będzie dostępne oprogramowanie antywirusowe.
Oprogramowanie antywirusowe powinno być zawsze włączone i aktualizowane.

3.8. Wymiana informacji

Żaden użytkownik nie może w żadnym wypadku ukrywać swojej tożsamości ani nią manipulować.
Dystrybucja informacji w formie elektronicznej lub fizycznej będzie odbywać się za pomocą środków określonych w umowie o świadczenie usług w tym zakresie i wyłącznie w celu ułatwienia wykonywania funkcji związanych z tą umową.
W odniesieniu do wymiany informacji 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.

3.9. Korzystanie z poczty elektronicznej

Zasób ten będzie wykorzystywany do celów zawodowych. Wszelkie inne wykorzystanie jest zabronione.
Wyraźnie zabrania się przechwytywania i/lub nieuprawnionego wykorzystywania wiadomości lub adresów e-mail innych użytkowników.
Użytkownik powinien odrzucać wszelkie wiadomości e-mail pochodzące z niewiarygodnych źródeł, ponieważ mogą one zawierać wirusy lub złośliwe kody, spam itp.

Użytkownik powinien unikać niepotrzebnego ujawniania adresu e-mail, przede wszystkim nie uczestnicząc w łańcuchach wiadomości, nawet jeśli ich cel wydaje się altruistyczny.

3.10. Łączność z Internetem

Zasób ten będzie wykorzystywany do celów zawodowych. Wszelkie inne wykorzystanie jest zabronione.

W żadnym wypadku nie wolno uzyskiwać dostępu do stron internetowych zawierających gry, treści seksualne lub treści obraźliwe lub naruszające godność ludzką lub prawa podstawowe.

3.11. Bezpieczeństwo logiczne

Użytkownicy będą mieli dostęp wyłącznie do tych zasobów, które są niezbędne do wykonywania ich obowiązków.

Wprowadzone zostaną mechanizmy uniemożliwiające użytkownikom dostęp do zasobów, do których nie mają uprawnień.

Osoba odpowiedzialna za systemy będzie odpowiedzialna za aktualizację listy użytkowników i profili oraz uprawnień dostępu dla każdego z nich.

Wyłącznie osoby upoważnione (administratorzy) przez osobę odpowiedzialną za systemy mogą przyznawać, zmieniać lub cofać uprawnienia dostępu do zasobów, zgodnie z kryteriami ustalonymi przez Grupo Azpiaran i organizację klienta.

W przypadku użytkowników spoza organizacji muszą oni podlegać tym samym warunkom i obowiązkom bezpieczeństwa, co osoby wewnętrzne.

Należy ustanowić mechanizm umożliwiający jednoznaczną i spersonalizowaną identyfikację każdego użytkownika próbującego uzyskać dostęp do systemów informatycznych oraz weryfikację, czy jest on uprawniony.

Procedura przypisywania, dystrybucji i przechowywania haseł zapewni ich poufność i integralność.

Po interwencji administratora użytkowników systemy informatyczne automatycznie wymuszą zmianę hasła.

Systemy informatyczne będą automatycznie wymuszały zmianę hasła co najmniej raz na 90 dni, o ile system na to pozwala i nie ma możliwości aktywacji MFA.

Aktualne hasła będą przechowywane w formie nieczytelnej.

Minimalna długość hasła powinna wynosić 8 znaków, na przemian cyfry, znaki alfanumeryczne (wielkie i małe litery) oraz znaki specjalne.

Tymczasowe uprawnienia dostępu będą konfigurowane na krótki okres czasu, a po jego upływie zostaną automatycznie wyłączone.

Systemy informatyczne ograniczają możliwość wielokrotnych prób nieautoryzowanego dostępu do maksymalnie 5 prób.

3.12. Obowiązki użytkownika

3.12.1. Korzystanie z haseł

Użytkownik nie powinien w żadnym wypadku ujawniać swojego identyfikatora i/lub hasła innemu użytkownikowi ani przechowywać go w formie pisemnej w miejscu widocznym lub dostępnym dla osób trzecich.

W przypadku, gdy system informatyczny nie zażąda tego automatycznie, użytkownik powinien zmienić tymczasowe hasło przypisane przy pierwszym prawidłowym logowaniu do systemu lub interwencji administratora.

W przypadku, gdy system nie zażąda tego automatycznie, użytkownik powinien zmienić swoje hasło co najmniej raz na 90 dni, o ile system na to pozwala i nie ma możliwości aktywacji MFA.

Minimalna długość hasła powinna wynosić 8 znaków.

Hasła powinny składać się z kombinacji znaków numerycznych, alfanumerycznych (wielkich i małych liter) oraz specjalnych. Zaleca się stosowanie następujących zasad przy wyborze haseł:

- Nie należy używać słów odnoszących się do rozpoznawalnych pojęć, przedmiotów lub idei (np. ważne daty, dni tygodnia, miesiące roku, imiona użytkowników, osoby, numery telefonów itp.).
- Hasło powinno być praktycznie niemożliwe do odgadnięcia, ale jednocześnie powinno być łatwe do zapamiętania przez użytkownika (np. użycie akronimu jakiegoś wyrażenia lub frazy itp.).

Jeśli użytkownik podejrzewa, że jego identyfikator i hasło są używane przez inną osobę, powinien natychmiast zmienić hasło i zgłosić ten incydent na adres ITteam@azpiaran.com.

3.12.2. Sprzęt

Użytkownik powinien upewnić się, że jego komputer spełnia następujące normy:

- W przypadku braku aktywności komputer blokuje się automatycznie w ciągu maksymalnie 10 minut.
- Nie posiada:
  - Narzędzi, które mogą naruszać środki bezpieczeństwa.
  - Nielegalnych kopii programów.
  - Programy nieposiadające certyfikatu zgodności.
- Posiada aktualne i aktywowane oprogramowanie antywirusowe na komputerach Apple, Windows i Android.
- Na bieżąco aktualizowany o najnowsze dostępne aktualizacje zabezpieczeń.

3.12.3. Stanowisko pracy

Użytkownik musi przestrzegać co najmniej następujących zasad dotyczących czystości 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 pod kluczem dokumenty papierowe i nośniki danych, gdy nie są używane, zwłaszcza poza godzinami pracy.
- Blokować sesję lub wyłączać komputer użytkownika, gdy pozostawia się go bez nadzoru.
- Zabezpiecz zarówno punkty odbioru i wysyłania informacji (poczta tradycyjna, skanery i faksy), jak i urządzenia do kopiowania (kserokopiarki, faksy i skanery).
- Bez zbędnej zwłoki usuwać wszelkie chronione informacje po ich wydrukowaniu.

- Niszczenie informacji chronionych, gdy przestaną być potrzebne.

3.13. Praca zdalna

Praca zdalna, rozumiana jako dostęp do sieci firmowej z zewnątrz, będzie regulowana poprzez wprowadzenie następujących zasad:

- Nie zezwala się na korzystanie z infrastruktury (oprogramowania, sprzętu i sieci komunikacyjnych) niekontrolowanej przez Grupo Azpiaran.
- Kryteria zezwalania na telepracę zostaną ustalone w oparciu o potrzeby danego stanowiska pracy.
- Ustanowione zostaną środki niezbędne do bezpiecznego połączenia z siecią korporacyjną.
- Ustanowione zostaną systemy monitorowania i kontroli bezpieczeństwa ustanowionych połączeń.
- Będzie kontrolowane cofanie praw dostępu i zwrot infrastruktury po zakończeniu okresu jej wykorzystywania.

3.14. Oprogramowanie

Oprogramowanie mogą instalować wyłącznie osoby upoważnione (administratorzy) przez osobę odpowiedzialną za administrację.

Użytkownik powinien korzystać wyłącznie z dostarczonych wersji oprogramowania i zgodnie z zasadami ich użytkowania.

Surowo zabrania się:

- Instalowanie nielegalnych kopii jakichkolwiek programów, w tym programów standardowych.
- Korzystanie z oprogramowania nieautoryzowanego przez administratora.
- Odinstalowywanie jakichkolwiek programów zainstalowanych przez Grupo Azpiaran.

3.15. Incydenty

Przez incydent rozumie się każde nieoczekiwane zdarzenie lub serię zdarzeń związanych z bezpieczeństwem informacji, które mogą w znacznym stopniu zagrozić działalności Grupo Azpiaran i naruszyć niniejsze przepisy.

W przypadku wykrycia potencjalnej luki w zabezpieczeniach, zdarzenia lub incydentu, użytkownik powinien niezwłocznie powiadomić o tym fakcie adres ITteam@azpiaran.com.

3.16. Zgodność z przepisami

Zapewniona zostanie zgodność z ograniczeniami prawnymi dotyczącymi wykorzystania materiałów chronionych przepisami dotyczącymi własności intelektualnej.

Użytkownik może korzystać wyłącznie z materiałów autoryzowanych przez Grupo Azpiaran do wykonywania swoich obowiązków.

Surowo zabrania się korzystania z oprogramowania komputerowego bez odpowiedniej licencji użytkowania.

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

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

Zapewnione zostanie przestrzeganie obowiązujących przepisów dotyczących ochrony danych osobowych w zakresie przetwarzania danych osób fizycznych zidentyfikowanych i możliwych do zidentyfikowania.