

Polityka bezpieczeństwa sieci

Firma, nazwa i stanowisko:

Data:

Podpis:

Proszę również o wpisanie „przeczytane i zatwierdzone”

Wersja	Właściciel (Dział lub funkcja)	Grupa Docelowa	Zatwierdzone Przez	Data zatwierdzenia	Częstotliwość przeglądu	Przejrzane tematy
1	ICT	Pracownicy i dostawcy	ICT	07/2023	Co najmniej co 3 lata	/

I. Wstęp

Niniejsza polityka opiera się na międzynarodowo uznanych normach **ISO 27001 dotyczących bezpieczeństwa informacji i 27002** dotyczących technologii informatycznych i ma zastosowanie do firm outsourcingowych IT lub innych zewnętrznych dostawców (zwanym dalej łącznie „Użytkownikiem”), którym udziela się dostępu do sieci komputerowej lub komunikacji elektronicznej VPK Packaging Group NV lub jednej lub więcej jej spółek zależnych lub stowarzyszonych (zwanym dalej łącznie „VPK”).

W zamian za udzielenie takiego Dostępu przez VPK, Użytkownik zgadza się na warunki niniejszej polityki.

Polityka ta składa się z **3 części**:

1. Kontrola dostępu: obowiązki, które Użytkownik musi spełnić, i procedury, które Użytkownik musi przestrzegać, aby ograniczyć (nieautoryzowany) dostęp do sieci VPK.

2. Podczas dostępu: obowiązki, które Użytkownik musi spełnić, i procedury, których Użytkownik musi przestrzegać podczas dostępu do sieci VPK.

3. Różne: inne postanowienia dotyczące bezpieczeństwa informacji i technologii informatycznych, w tym procedura powiadamiania w przypadku zagrożenia bezpieczeństwa sieci lub incydentu.

Obowiązki wynikające z niniejszej polityki obejmują upoważnionych pracowników, kontrahentów i innych przedstawicieli Użytkownika. Użytkownik musi poinformować wszystkich upoważnionych użytkowników, którzy będą korzystać z VPK Networks, o swoich obowiązkach wynikających z niniejszej polityki, ale Użytkownik pozostaje w pełni odpowiedzialny za naruszenia wobec VPK.

Jeśli którykolwiek Użytkownik nie będzie przestrzegał niniejszej polityki, wówczas taki Użytkownik może, oprócz wszystkich innych środków zaradczych, według wyłącznego uznania VPK, od tego momentu nie być uprawniony do świadczenia usług dla VPK i/lub zostać pozbawiony dostępu do VPK Networks.

Słowa pisane wielkimi literami mają znaczenie opisane w tytule 2.

II. Definicje

- ✓ „Dostępny” oznacza wszelkie uprawnienia lub uprawnienia, jakie Użytkownik może posiadać w celu przeglądania, pobierania, tworzenia lub modyfikowania informacji w sieci VPK, infrastrukturze VPK lub dowolnej innej aplikacji VPK.
- ✓ „Sesja zdalna” oznacza dowolny dostęp do sieci VPK nawiązany poprzez połączenie dial-up lub połączenie ciągłe.
- ✓ „Informacje poufne VPK” należy zdefiniować jako informacje odnoszące się do przeszłych, obecnych i przyszłych badań, rozwoju, działalności biznesowej, produktów, usług i wiedzy technicznej VPK. Informacje poufne VPK obejmują, ale nie ograniczają się do, informacji technicznych i biznesowych odnoszących się do wynalazków lub produktów VPK, badań i rozwoju, produkcji, wytwarzania i procesów

inżynieryjnych, informacje o kosztach, zyskach lub marżach, umiejętnościach i wynagrodzeniach pracowników, finansach, klientach, marketingu, produkcji, przyszłych planach biznesowych oraz wszelkie zastrzeżone lub poufne informacje stron trzecich, do których Użytkownik może mieć dostęp

- ✓ Termin „Sieć(i) VPK” odnosi się do dowolnego komputera VPK lub zasobu lub sieci komunikacji elektronicznej, które przetwarzają, przechowują lub przesyłają dane lub informacje VPK, w tym Poufne Informacje VPK.

III. Czego (nie) robić

1. KONTROLA DOSTĘPU

1.1 Wprowadzenie

Użytkownik może uzyskać dostęp i korzystać z VPK Networks tylko w zakresie niezbędnym do rozwijania relacji biznesowych lub usługowych z VPK. Użytkownik zgadza się, że nie będzie w inny sposób korzystać ani uzyskiwać dostępu do VPK Networks, do własnego użytku lub w jakimkolwiek innym celu.

Ponadto:

- a. Użytkownik ma dostęp wyłącznie do sieci VPK i informacji VPK, w tym poufnych informacji VPK, do których użytkownik uzyskał specjalne prawa dostępu od VPK.
- b. Użytkownik nie będzie podejmował prób nieautoryzowanego dostępu do sieci VPK ani nie będzie zezwalał nieautoryzowanym osobom na dostęp do sieci, danych lub informacji VPK.
- c. Użytkownik nie będzie uzyskiwał dostępu ani podejmował prób uzyskania dostępu do żadnych sieci lub systemów stron trzecich za pośrednictwem sieci VPK, chyba że uzyska pisemne upoważnienie od VPK.
- d. Identyfikator użytkownika VPK może być używany wyłącznie do logowania się do sieci VPK i nie jest przeznaczony do użytku w żadnej innej sieci.
- e. Użytkownik nie będzie replikował ani przechowywał informacji VPK w sposób, który niepotrzebnie ujawnia informacje.



- f. Użytkownik wdroży zabezpieczenia poufności podsumowane w sekcji 2.5.

Użytkownikowi nie wolno wprowadzać, dodawać, usuwać ani w żaden inny sposób modyfikować Sieci VPK ani danych dostępnych za pośrednictwem Sieci VPK, z wyjątkiem przypadków, w których Użytkownik został do tego upoważniony przez VPK na piśmie.

1.2 Bezpieczeństwo fizyczne i środowiskowe

Sprzęt użytkownika, taki jak komputery PC, stacje robocze i inny sprzęt ICT, który uzyskuje dostęp do sieci VPK:

- a. Będzie fizycznie dostępny wyłącznie dla upoważnionych pracowników, kontrahentów i innych przedstawicieli użytkownika.
- b. Musi wykorzystywać kontrole, które ograniczają dostęp do sieci VPK wyłącznie dla upoważnionych pracowników, kontrahentów i innych przedstawicieli użytkownika.
- c. Nie będzie zawierać żadnego oprogramowania ani połączenia ze zdalnym węzłem, które umożliwia routing TCP/IP, chyba że taka możliwość routingu jest wyłączona.
- d. Nie będzie wykorzystywać funkcji automatyzującej hasła w procesie logowania, takiej jak przechowywanie hasła w makrze, skrypcie logowania lub klawiszu funkcyjnym lub zaznaczenie pola „zapisz hasło”.
- e. Użytkownik musi się wylogować przed opuszczeniem zasobów komputerowych.

1.2 Uwierzytelnianie użytkownika

Administracja identyfikatorami użytkowników VPK. VPK może administrować przydziałem indywidualnych identyfikatorów użytkowników Użytkownikowi, w takim przypadku Użytkownik musi dostarczyć VPK:

- a. Jeśli to możliwe, pełne imię i nazwisko każdej osoby, która będzie miała dostęp do sieci VPK.
- b. Niezwłoczne powiadomienie, na piśmie, o zakończeniu stosunku pracy lub przydzieleniu osób z dostępem do sieci VPK, aby indywidualne identyfikatory logowania



użytkowników mogły zostać zmienione, a VPK mogło podjąć inne środki w celu zapobiegania nieautoryzowanemu dostępowi.

Administracja identyfikatorem użytkownika. Użytkownikowi może zostać przydzielony blok identyfikatorów użytkownika, w takim przypadku Użytkownik jest odpowiedzialny za zarządzanie i administrowanie identyfikatorami użytkownika w ramach swoich operacji.

a. Użytkownik musi rejestrować przydział identyfikatorów użytkownika w rejestrze, aby zapewnić spójność, uniknąć duplikacji i pociągnąć poszczególnych użytkowników do odpowiedzialności za ich uprawnienia dostępu do sieci VPK. Na żądanie VPK Użytkownik musi dostarczyć VPK kopię swojego bieżącego i historycznego rejestru identyfikatorów użytkownika VPK.

b. W miarę możliwości Użytkownik podejmie środki, aby zapewnić, że pojedynczy identyfikator użytkownika nie zostanie przypisany wielu użytkownikom.

c. Po zakończeniu stosunku pracy lub przydzieleniu osobom identyfikatora użytkownika, Użytkownik niezwłocznie unieważni identyfikator użytkownika dla takiego użytkownika.

Poświadczenia uwierzytelniające. VPK może ustanowić mechanizm silnych poświadczeń uwierzytelniających, takich jak, ale nie wyłącznie, certyfikaty cyfrowe, tokeny, karty inteligentne i dane biometryczne, aby zapewnić dostęp, rozliczalność i unieważnienie. Po ustanowieniu takiego mechanizmu VPK przekaże Użytkownikowi uzasadnione powiadomienie o tym.

Hasła. Hasła muszą być zgodne z następującymi standardami:

a. VPK określi długość hasła lub zgodzi się na nią w przypadku, gdy Użytkownik musi je utworzyć.

b. Hasło musi być nieczytelne i z niczym się nie kojarzące

c. Hasło musi zostać zmienione, gdy istnieje podejrzenie, że zostało udostępnione nieautoryzowanemu użytkownikowi Użytkownika lub innej osobie trzeciej.

d. Hasło musi zostać zmienione na proste żądanie VPK.



Poufność identyfikatorów użytkownika i haseł. Użytkownik potwierdza, że każdy identyfikator użytkownika lub hasło przyznane Użytkownikowi przez VPK będzie uważane za Poufne Informacje VPK i jest przeznaczone wyłącznie do użytku Użytkownika w związku z jego relacją biznesową lub usługową z VPK. Użytkownik musi zaszyfrować wszystkie identyfikatory użytkownika i hasła. Użytkownik nie będzie udostępniał, ujawniał ani wykorzystywał w żaden nieautoryzowany sposób identyfikatorów użytkownika i haseł przyznanych przez VPK. Użytkownik ponosi odpowiedzialność za działania osób korzystających z identyfikatorów użytkownika i haseł w celu uzyskania dostępu do sieci VPK. Użytkownik będzie chronić, bronić i zwalniać VPK z odpowiedzialności za wszelkie żądania, roszczenia, działania lub przyczyny działań, straty, szkody, koszty, wydatki, wyroki, nagrody, grzywny, kwoty zapłacone w ramach ugody i inne zobowiązania wynikające z zaniedbania przez Użytkownika zachowania bezpieczeństwa i poufności identyfikatorów użytkownika i/lub haseł używanych do uzyskania dostępu do sieci VPK.

Odwołanie przez VPK. VPK może odwołać identyfikatory i hasła w dowolnym momencie, według wyłącznego uznania VPK, w takim przypadku identyfikator użytkownika lub hasło zostaną usunięte.

2. Podczas dostępu

2.1 Informacje ogólne

Uzyskując dostęp do Sieci VPK, Użytkownik zobowiązany jest upewnić się, że jego własne systemy i sieci są odpowiednio chronione przed jakąkolwiek niekorzystną interakcją z Siecią VPK i upewnić się, że Sieć VPK nie jest narażona na żadne zagrożenia bezpieczeństwa w wyniku Dostępu Użytkownika do Sieci VPK.

2.2 Zmiany użytkownika w systemach VPK

W przypadku wszelkich zmian wprowadzanych przez Użytkownika w systemach produkcyjnych VPK, w tym, ale nie wyłącznie, w programach, konfiguracji lub środowisku, Użytkownik:

- a. Przed wdrożeniem, w pełni zweryfikuje takie zmiany w systemie testowym, który replikuje system produkcyjny VPK,



- b. Uzyska wcześniejszą zgodę VPK, a następnie zaplanuje zmianę, z wyjątkiem sytuacji wyjątkowych, w którym to przypadku Użytkownik powiadomi VPK w ciągu dwudziestu czterech (24) godzin od zmiany.
- c. Dostarczy zaktualizowaną dokumentację i procedury wycofania, jeśli są stosowne, do VPK w momencie zmiany.
- d. Utworzy, będzie prowadzić i administrować pisemnym dziennikiem zmian, obejmującym datę/godzinę, nazwisko personelu autoryzującego VPK i zmianę funkcjonalną, który będzie dostępny przez jeden rok na żądanie VPK, w ciągu dwudziestu czterech (24) godzin od takiego żądania.

UWAGA: jeśli Użytkownik ma zainstalowany router VPK w swojej siedzibie, poniższy paragraf nie ma zastosowania.

Użytkownik musi utworzyć pisemny dziennik wszystkich dostępów do sieci VPK i przechowywać informacje z dziennika przez okres jednego roku.

- a. Dziennik musi zawierać następujące informacje dla każdej sesji zdalnej: datę/godzinę, identyfikator użytkownika, imię i nazwisko użytkownika, początek połączenia, koniec połączenia, cel, wykonane testy lub ukończone działania.
- b. Takie informacje z dziennika muszą być dostępne na żądanie VPK w ciągu 24 godzin od takiego żądania.

2.3 Przekazywanie informacji do VPK

Szyfrowanie. VPK może zapewnić Użytkownikowi zatwierdzony mechanizm szyfrowania do wykorzystania we wszystkich elektronicznych transakcjach biznesowych z VPK i w każdym elektronicznym udostępnianiu informacji z VPK. Użytkownik, po udostępnieniu takiego mechanizmu, będzie używał zatwierdzonej przez VPK metodologii szyfrowania do wszelkiego udostępniania informacji z VPK.

Wirusy komputerowe. Użytkownik podejmie wszelkie środki ostrożności, aby zapobiec przeniesieniu wirusa komputerowego do sieci VPK i będzie utrzymywał aktualne i aktywne narzędzia antywirusowe na wszystkich komputerach, które będą bezpośrednio współpracować z siecią VPK. Ponadto:

- a. Użytkownik będzie używał oprogramowania antywirusowego do sprawdzania i usuwania wirusów ze wszystkich plików elektronicznych przesyłanych do lub z VPK.
- b. Użytkownik natychmiast powiadomi VPK, jeśli w pliku wysłanym lub odebranym z VPK zostanie wykryty wirus.



Przekazywanie oprogramowania. Użytkownik może korzystać wyłącznie z programów do komunikacji w sieci zatwierdzonych przez VPK w celu interakcji z sieciami VPK.

2.4 Oprogramowanie

Ochrona. Użytkownik może używać i mieć dostęp do: (a) oprogramowania stron trzecich licencjonowanego dla VPK i/lub (b) zastrzeżonego oprogramowania VPK (zwanym łącznie „Oprogramowaniem”). VPK może udostępnić Użytkownikowi takie Oprogramowanie na (i) żądanie Użytkownika, (ii) ustalenie przez VPK, że korzystanie z takiego Oprogramowania będzie służyć potrzebom biznesowym VPK oraz (iii) zatwierdzenie przez VPK i licencjodawcę oprogramowania strony trzeciej. Jeśli VPK udostępni takie Oprogramowanie, Użytkownik będzie:

- a. Używał oprogramowania stron trzecich w ścisłej zgodności ze wszystkimi warunkami narzuconymi przez licencjodawcę oprogramowania.
- b. Używał Oprogramowania wyłącznie w celu rozwijania relacji biznesowej lub usługowej z VPK.
- c. Nie kopiował Oprogramowania, z wyjątkiem autoryzowanych kopii zapasowych VPK.
- d. Traktował Oprogramowanie jako Poufne Informacje VPK.
- e. Po zakończeniu usług na podstawie niniejszej Umowy, zwrócił Oprogramowanie do VPK, jeśli ma to zastosowanie, lub zniszczył wszystkie kopie Oprogramowania będące w jego posiadaniu.

Umowy z osobami trzecimi. Korzystanie przez Użytkownika z oprogramowania stron trzecich może wymagać podpisania przez Użytkownika umowy o zachowaniu poufności i/lub umowy licencyjnej oprogramowania dla takiego oprogramowania (łącznie „Umowy stron trzecich”). Użytkownik podpisze i wykona takie Umowy stron trzecich na uzasadnione żądanie VPK, a strony wzajemnie uzgodnią, która strona jest odpowiedzialna za zapłatę opłat licencyjnych oraz za oprogramowanie stron trzecich, jeśli ma to zastosowanie.

2.5 VPK Informacje poufne

Użytkownik przyjmuje do wiadomości, że informacje ujawnione mu przez VPK lub do których Użytkownik będzie miał dostęp za pośrednictwem Sieci VPK, mogą obejmować Informacje Poufne VPK. Użytkownik zgadza się, że wykorzysta takie informacje tylko w

zakresie niezbędnym do rozwijania relacji biznesowej lub usługowej z VPK i że nie będzie w żaden inny sposób przywłaszczał sobie takich informacji do własnego użytku lub użytku osób trzecich.

Użytkownik zgadza się chronić tajność Informacji Poufnych VPK w taki sam sposób, w jaki chroni własne dane. W stosownych przypadkach Użytkownik powinien zastosować następujące środki ostrożności:

- Oznaczyć wszystkie wydruki lub materiały namacalne zawierające Informacje Poufne VPK klasyfikacją „Poufne VPK”.
- Traktować Informacje Poufne VPK jako tajne i chronić je przed nieautoryzowanym użyciem lub ujawnieniem.
- Ograniczyć ujawnianie Informacji Poufnych VPK wyłącznie do swoich pracowników i kontrahentów, którzy muszą je znać ze względu na relacje biznesowe lub usługowe Użytkownika z VPK. - Poinformuj każdego pracownika i kontrahenta Użytkownika o istnieniu tego obowiązku zachowania poufności.
- Zabezpiecz fizycznie obszary robocze i materiały zawierające Poufne Informacje VPK.
- Wyrzucić kopie papierowe lub materiały namacalne zawierające Poufne Informacje VPK do niszcarki lub poufnego kosza na śmieci.
- Wyczyścić wszystkie nośniki magnetyczne lub elektroniczne przed wyrzuceniem lub ponownym wydaniem, aby uniemożliwić odzyskanie Poufnych Informacji VPK.
- Traktuj wszystkie informacje na adresach sieciowych VPK jako Poufne Informacje VPK, co obejmuje, ale nie ogranicza się do, niepublikowania informacji w żadnych sieciach zewnętrznych.

Informacje nie będą uważane za Poufne Informacje VPK, jeśli (1) zostały opublikowane lub są w inny sposób łatwo dostępne dla opinii publicznej, z wyjątkiem naruszenia niniejszej Umowy; (2) zostały prawidłowo otrzymane przez odbiorcę od osoby trzeciej bez ograniczeń poufności; (3) zostały niezależnie opracowane dla odbiorcy przez personel lub agentów niemających Dostępu do Poufnych Informacji VPK; lub (4) były znane odbiorcy przed ich pierwszym otrzymaniem od osoby ujawniającej. W przypadku gdy odbiorca otrzyma wezwanie sądowe lub inny prawidłowo wydany proces administracyjny lub sądowy żądający poufnych informacji VPK („Wezwanie sądowe”), musi on niezwłocznie powiadomić VPK o takim otrzymaniu. Strona otrzymująca



wezwanie sądowe będzie następnie uprawniona do zastosowania się do takiego wezwania sądowego lub innego procesu w zakresie dozwolonym przez prawo, ale musi podjąć uzasadnione wysiłki w celu zachowania poufności poufnych informacji VPK ujawnionych na mocy wezwania sądowego, w zakresie dozwolonym przez prawo.

3. RÓŻNE

3.1 Audyt i monitoring

Użytkownik, uzyskując dostęp do sieci VPK, może mieć możliwość monitorowania i rejestrowania korzystania z takiej sieci przez VPK lub dostawcę usług VPK. Użytkownik wyraźnie wyraża zgodę na takie monitorowanie i rejestrowanie.

VPK może, po uprzednim powiadomieniu, kontrolować zgodność Użytkownika z wymogami poufności i bezpieczeństwa określonymi w niniejszej polityce. Po powiadomieniu Użytkownika, VPK będzie mieć prawo odwiedzić witrynę Użytkownika w zwykłych godzinach pracy, aby zapoznać się ze środkami bezpieczeństwa i kontrolami Użytkownika.

3.2 Zagrożenia i incydenty związane z bezpieczeństwem sieci

Użytkownik musi natychmiast powiadomić VPK o każdym ryzyku lub naruszeniu bezpieczeństwa dotyczącym Sieci VPK lub o jakimkolwiek ryzyku lub naruszeniu bezpieczeństwa dotyczącym jego własnej sieci, które może niekorzystnie wpłynąć na Sieć VPK. Na przykład, jeśli Użytkownik odkryje, że jego sieć została zainfekowana wirusem, musi natychmiast powiadomić VPK. Ponadto, jeśli Użytkownik dowie się o naruszeniu Poufnych Informacji VPK, musi natychmiast powiadomić VPK. W przypadku ryzyka lub naruszenia bezpieczeństwa sieci, Użytkownik zgadza się zakończyć Dostęp do Sieci VPK, dopóki VPK nie udzieli Użytkownikowi ponownej autoryzacji do Dostępu do takich Sieci VPK. Ponadto, Użytkownik musi w pełni współpracować z VPK w celu ochrony Sieci(y) VPK i informacji oraz zgłaszać VPK wszelkie podejrzenia dotyczące braków w bezpieczeństwie komunikacji fizycznej lub elektronicznej.

3.3 Własność intelektualna

Użytkownikowi nie wolno używać ani zmieniać nazwy, znaków towarowych ani innej własności intelektualnej należącej do VPK lub osoby trzeciej, ale dostępnej za





pośrednictwem Sieci VPK, z wyjątkiem przypadków wyraźnie upoważnionych na piśmie przez VPK.

3.4 Zwrot informacji

Użytkownik zgadza się, że na żądanie VPK i według wyłącznego uznania VPK, albo (i) zwróci VPK, albo (ii) zniszczy wszystkie materiały zawierające informacje VPK, w tym poufne informacje VPK. VPK może ponadto wymagać od Użytkownika pisemnego potwierdzenia, że wypełnił swoje zobowiązania wynikające z niniejszego postanowienia.

