POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH PRZETWARZANYCH W

Przedsiębiorstwo Handlowo-Usługowe SUPON Silesia Sp. z o.o.

1. WSTĘP

§ 1.

1. Celem dokumentu „Polityka bezpieczeństwa danych osobowych”, zwanego dalej „Polityką”, jest wyznaczenie kierunku działań mających na celu zapewnienie bezpieczeństwa informacji w PHU SUPON SILESIA Sp. z o.o., zwanym dalej „Spółką” oraz wyrażenie poparcia kierownictwa Spółki dla tych działań.
2. Na treść dokumentu składają się podstawowe zasady i wytyczne dotyczące bezpieczeństwa danych osobowych w Spółce.
3. Podstawę formalno-prawną do opracowania dokumentacji „Systemu ochrona danych osobowych”, zwanego dalej „Polityką bezpieczeństwa danych osobowych”, stanowią:
   3.1. ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.), zwana dalej „ustawą” – do dnia 25 maja 2018 roku.;
   3.2. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) – po dniu 25 maja 2018 roku.

§ 2.

Polityka jest dokumentem nadrzędnym dla wszystkich dokumentów dotyczących ochrony danych osobowych w Spółce.

§ 3.

1. Z treścią Polityki powinni zapoznać się wszyscy pracownicy Spółki i członkowie Zarządu.

W uzasadnionych przypadkach z treścią dokumentu mogą zapoznać się podmioty spoza Spółki.

§ 4.

W treści polityki oraz załączników do niej mogą pojawić się pojęcia, które oznaczają:

1. aktywa – wszystko, co ma wartość dla organizacji;
2. akceptowanie ryzyka – decyzja, aby zaakceptować ryzyko;
3. analiza ryzyka – systematyczne korzystanie z informacji w celu zidentyfikowania źródeł i oceny ryzyka;
4. bezpieczeństwo informacji – zachowanie poufności, integralności i dostępności informacji; dodatkowo, mogą być brane pod uwagę inne własności, takie jak: autentyczność, rozliczalność, niezaprzeczalność i niezawodność;
5. dostępność – właściwość bycia dostępnym i użytecznym na żądanie upoważnionego podmiotu;
6. identyfikowanie ryzyka – proces znajdowania, zestawiania i charakteryzowania elementów ryzyka;
7. incydent związany z bezpieczeństwem informacji – pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które

stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji;

8. integralność – właściwość polegającą na zapewnieniu dokładności i kompletności aktywów;
9. kryptografia z kluczem publicznym – kryptografia, w której wykorzystuje się klucz publiczny i odpowiadający mu klucz prywatny, w określonej kolejności, w celu szyfrowania i deszyfrowania;
10. następstwa – rezultat niepożądanego incydentu;
11. niezaprzeczalność – brak możliwości wyparcia się swego uczestnictwa w całości lub części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie;
12. obszar bezpieczny – budynek lub część budynku otoczone ciągłą, wewnętrzną barierą bezpieczeństwa zapewniającą, że tylko osoby uprawnione mają dostęp do obszaru bezpiecznego; wewnątrz obszaru bezpiecznego mogą funkcjonować strefy ograniczonego dostępu, do których mogą wchodzić osoby, którym nadano uprawnienia dostępu do tych stref;
13. obszar chroniony – obszar, na którym rozmieszczone są aktywa Spółki, a w szczególności urządzenia i maszyny, środki transportu oraz budynki wraz z ich wyposażeniem i zgromadzonymi w nich zasobami informacyjnymi i środkami przetwarzania informacji;
14. obszar publicznie dostępny, dostaw i załadunku – teren wokół budynku (budynków) oraz wydzielone w budynkach obszary dostępne dla wszystkich osób, z których istnieją wejścia do obszarów bezpiecznych, przeznaczone do przyjmowania interesantów i gości oraz osób realizujących dostawy i załadunek lub dla innych celów; w obrębie obszaru publicznie dostępnego, dostaw i załadunku realizuje się kontrolowanie osób i pojazdów;
15. ocena ryzyka – proces porównywania oszacowanego ryzyka z określonymi kryteriami w celu określenia znaczenia ryzyka;
16. podatność – słabość aktywu, lub grupy aktywów, która może być wykorzystana przez co najmniej jedno zagrożenie;
17. podpis elektroniczny – przekształcenie kryptograficzne danych, umożliwiające odbiorcy danych sprawdzenie ich pochodzenia i integralności oraz zapewniające nadawcy ochronę przed sfałszowaniem danych przez odbiorcę;
18. polityka – wyrażona przez kierownictwo ogólna intencja i kierunki działań;
19. pomieszczenie wymagające szczególnej ochrony – pomieszczenie umiejscowione w obszarze bezpiecznym lub strefie ograniczonego dostępu, do którego dostęp posiadają wyłącznie osoby posiadające specjalne uprawnienia dostępu;
20. poufność – właściwość polegająca na tym, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom, podmiotom lub procesom;
21. postępowanie z ryzykiem – proces wyboru i wdrażania środków modyfikujących ryzyko;
22. punkt dostępu – drzwi, bramka wejściowa na kartę lub obszar publicznie dostępny (taki jak np. obszar dostaw i załadunku lub obszar wydawania przepustek), przez które można wejść do obszaru bezpiecznego, strefy ograniczonego dostępu lub pomieszczenia wymagającego szczególnej ochrony;

23. rozliczalność – właściwość zapewniająca, że działania podmiotu mogą być śledzone w sposób charakterystyczny tylko dla tego podmiotu;
24. ryzyko – kombinacja prawdopodobieństwa zdarzenia i jego konsekwencji;
25. ryzyko związane z bezpieczeństwem informacji – potencjalna sytuacja, w której określone zagrożenie wykorzysta podatność aktywów lub grupy aktywów powodując w ten sposób szkodę w organizacji;
26. skutek – negatywna zmiana w odniesieniu do osiąganego poziomu celów biznesowych;
27. strefa ograniczonego dostępu – wydzielona w obszarze bezpiecznym strefa, do której dostęp posiadają wyłącznie osoby posiadające uprawnienia dostępu do strefy; mogą to być pojedyncze pomieszczenia lub grupy pomieszczeń wraz z ciągami komunikacyjnymi;
28. system informatyczny (teleinformatyczny) – zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych poprzez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego
29. szacowanie ryzyka – całościowy proces analizy i oceny ryzyka;
30. uwierzytelniać – ustalać ważność deklarowanej tożsamości;
31. właściciel aktywu – osoba lub wyznaczona struktura organizacyjna Spółki, która ma zatwierdzoną kierowniczą odpowiedzialność za zaprojektowanie, wdrożenie, rozwój, utrzymanie, wykorzystywanie oraz bezpieczeństwo aktywu;
32. zabezpieczenie – środki służące zarządzaniu ryzykiem, łącznie z politykami, procedurami, zaleceniami, praktyką lub strukturami organizacyjnymi, które mogą mieć naturę administracyjną, techniczną, zarządczą lub prawną;
33. zagrożenie – potencjalna przyczyna niepożądanego incydentu, który może wywołać szkodę w systemie lub organizacji;
34. zarządzanie ryzykiem – skoordynowane działanie kierowania i zarządzania organizacją z uwzględnieniem ryzyka;
35. zdarzenie związane z bezpieczeństwem informacji – określony stan systemu, usługi lub sieci, który wskazuje na możliwe naruszenie polityki bezpieczeństwa, błąd zabezpieczenia lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem.

2. OPIS SPOSOBU PRZETWARZANIA DANYCH OSOBOWYCH

2.1 Ogólny opis zakresu i sposobu przetwarzania danych osobowych

§ 5.

Spółka przetwarza dane osobowe w zakresie niezbędnym do realizacji prawnie uzasadnionego interesu Spółki.

§ 6.

1. Spółka przetwarza dane osobowe dotyczące:
   1.1. klientów zainteresowanych ofertą spółki;
   1.2. klientów obsługiwanych po zawarciu umowy – dla celów realizacji umowy;
   1.3. klientów spółki, którzy wyrazili zgodę na otrzymywanie treści marketingowych
   1.4. osób, które przekazały (osobiście, pocztą tradycyjną, pocztą elektroniczną, telefonicznie lub za pośrednictwem strony internetowej) konkretne sprawy do realizacji;
   1.5. osób, których dane osobowe zostały powierzone Spółce na podstawie podpisanych umów powierzenia.
   1.6. pracowników Spółki i członków ich rodzin;
   1.7. kandydatów do pracy, na staż lub na praktyki;
   1.8. osób odbywających w Spółce praktykę lub staż;
   1.9. osób, które świadczą lub świadczyły usługi na rzecz Spółki na podstawie umów cywilnoprawnych;
   1.10. osób, których dane osobowe zostały zarejestrowane w związku z wydawaniem dokumentu uprawniającego do wejścia do obszaru bezpiecznego.
2. Dane osobowe przetwarza się w następujących lokalizacjach należących do Spółki:
   - ul. Wiosny Ludów 91 40-373 Katowice

§ 7.

Zakres przetwarzania danych osobowych przez poszczególnych pracowników Spółki wynika z zapisów w „Kartach zakresów obowiązków i odpowiedzialności oraz uprawnień pracowników" i indywidualnych upoważnień.

§ 8.

Dane osobowe są przetwarzane w Spółce:

1. z wykorzystaniem systemów informatycznych;
2. przy pomocy metod i środków innych niż określone w pkt 1.

§ 9.

Z uwagi na zakres i sposób realizacji zadań w Spółce, dokonywana jest wymiana danych osobowych pomiędzy Spółką oraz następującymi osobami i podmiotami:

1. osobami, o których mowa w § 6 ust. 1;
2. urzędami podatkowymi,
3. Zakładem ubezpieczeń Społecznych;

2.2 Obszar przetwarzania danych osobowych

§ 10.

1. Wykaz budynków, pomieszczeń i części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe w Spółce, prowadzi się według ustalonego wzoru zgodnie z procedurą „Prowadzenie wykazu budynków, pomieszczeń i części pomieszczeń tworzących obszar przetwarzania danych osobowych".

§ 11.

2. W przypadku powierzenia przez Spółkę podmiotowi zewnętrznemu, w drodze pisemnej umowy, zadań związanych z przetwarzaniem danych osobowych, przetwarzanie danych może odbywać się, w zależności od warunków umowy, w budynkach Spółki lub w budynkach należących do tego podmiotu.

2.3 Opis struktury zbiorów danych osobowych

§ 12.

1. Strukturę zbioru danych osobowych przetwarzanych w Spółce tworzą:
   1.1. dokumenty papierowe dotyczące poszczególnych spraw, gromadzone w aktach spraw i teczkach spraw;
   1.2. wykazy i rejestry papierowe – tworzone tymczasowo dla potrzeb świadczenia usług;
   1.3. sformalizowane dokumenty papierowe stanowiące dokumenty niezbędne dla świadczenia usług;

1.4. dokumenty elektroniczne tworzone przez pracowników Spółki dla potrzeb realizacji powierzonych zadań;

1.5. bazy danych zawierające dane osobowe przetwarzane w systemach informatycznych.

2.4 Proces zarządzania bezpieczeństwem danych osobowych

§ 13.

1. W Spółce realizowane są następujące zadania składające się na proces zarządzania bezpieczeństwem danych osobowych:

1.1. prowadzenie rejestru czynności przetwarzania;

1.2. prowadzenie rejestru kategorii przetwarzania;

1.3. prowadzenie rejestru zbiorów danych;

1.4. prowadzenie rejestru upoważnień do przetwarzania danych osobowych;

1.5. prowadzenie rejestru uprawnień nadanych dla osób zatrudnionych lub wykonujących pracę na podstawie umów cywilno-prawnych;

1.6. planowanie i koordynowanie przebiegu procesów zarządzania ryzykiem w spółce (jeśli konieczne);

1.7. formułowanie i doskonalenie Polityki bezpieczeństwa danych osobowych, w szczególności: zasad dotyczących obowiązków i odpowiedzialności osób zatrudnionych w Spółce, oraz zakresu wykonanych przez nich zadań mających na celu zapewnienie odpowiedniego poziomu bezpieczeństwa przetwarzanych danych osobowych;

1.8. nadzorowanie przez Inspektora Ochrony Danych Osobowych (jeśli zachodzi konieczność powołania) stosowania w Spółce środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych

1.9. monitorowanie bezpieczeństwa danych osobowych przetwarzanych w sieci teleinformatycznej Spółki;

1.10. opracowywanie i wdrażanie programów szkoleń w zakresie ochrony danych osobowych;

1.11. nadzorowanie postępowań wyjaśniających naruszenia ochrony danych osobowych;

3. DEFINICJA BEZPIECZEŃSTWA DANYCH OSOBOWYCH, JEGO CELE ORAZ ZAKRES I ZNACZENIE

§ 14.

Realizacja podstawowych zadań Spółki polega na przetwarzaniu informacji, czyli dokonywaniu operacji na danych, w szczególności takich jak: zbieranie, przekazywanie lub przesyłanie, utrwalanie, zmienianie, przekształcanie i udostępnianie, a także przechowywanie i usuwanie danych osobowych.

§ 15.

1. W trakcie realizowania celów statutowych Spółka jest zobowiązana do przestrzegania przepisów prawa, w tym w szczególności przepisów zobowiązujących Spółkę do ochrony danych osobowych.
2. Biorąc pod uwagę brzmienie definicji: poufności, integralności i dostępności, bezpieczeństwo danych osobowych w Spółce oznacza przede wszystkim:
   2.1. zapewnienie odpowiedniej jakości procesów przetwarzania informacji, a w szczególności jakości środków przetwarzania informacji, odpowiednich warunków ich użytkowania oraz sprawności i efektywności ich wykorzystywania;
   2.2. dysponowanie pracownikami o odpowiedniej wiedzy, umiejętnościach i doświadczeniu, zaangażowanymi w wykonywanie powierzonych im zadań;
   2.3. zorganizowanie odpowiedniej ochrony aktywów Spółki przed dostępem fizycznym osób nieupoważnionych, w celu zabezpieczenia tych aktywów przed kradzieżą, uszkodzeniem lub zniszczeniem;
   2.4. zabezpieczenie informacji przetwarzanej w Spółce przed jej ujawnieniem osobom lub podmiotom nieuprawnionym;
   2.5. zabezpieczenie systemów teleinformatycznych eksploatowanych w Spółce przed zagrożeniami pochodzącymi z sieci publicznych oraz ze strony osób użytkujących te systemy z upoważnienia Spółki;
   2.6. zabezpieczenie aktywów Spółki przed ich uszkodzeniem lub zniszczeniem w wyniku pożaru, zalania, lub zjawisk naturalnych;
   2.7. zapewnienie ciągłości działania krytycznych procesów przetwarzania informacji w Spółce.

4. DEKLARACJA ZAANGAŻOWANIA KIEROWNICTWA

§ 16.

1. Kierownictwo Spółki popiera i czynnie wspiera prowadzone w Spółce działania mające na celu ustanowienie, wdrożenie i doskonalenie Systemu Ochrony Danych Osobowych (zwanego dalej SODO). Osiągnięcie celów bezpieczeństwa informacji stanowi gwarancję odpowiedniej jakości usług świadczonych przez Spółkę, a w rezultacie dostarczania na odpowiednim poziomie satysfakcji klientom Spółki.
2. Kierunki prowadzonych w Spółce działań w zakresie bezpieczeństwa informacji wynikają z założeń, o których mowa w § 14 - § 15.

§ 17.

1. Poziom bezpieczeństwa informacji w Spółce jest odpowiedni wówczas, gdy:
   1.1. wdrożone są zabezpieczenia wymagane na podstawie przepisów prawa;
   1.2. ryzyko związane z bezpieczeństwem informacji, przy funkcjonujących zabezpieczeniach, jest akceptowalne.

§ 18.

1. Projektowanie i wybór zabezpieczeń, których wdrożenie jest konieczne z uwagi na przepisy prawa, łączy się z projektowaniem i wyborem zabezpieczeń, które mają zapewnić osiągnięcie i utrzymanie poziomu bezpieczeństwa informacji.
2. W polityce stosuje się następujące zasady ogólne:
   2.1. zasada rozdziału kompetencji – funkcje i zadania w obszarze przetwarzania informacji realizują inne zespoły ludzkie niż w obszarze bezpieczeństwa informacji (jeśli to możliwe);
   2.2. zasada wiedzy koniecznej – pracownicy posiadają dostęp tylko do tych informacji, które są konieczne do realizacji powierzonych im zadań;
   2.3. zasada pracy zbiorowej – wszyscy pracownicy powinni być świadomi konieczności przestrzegania określonych procedur bezpieczeństwa zapewniających ochronę i efektywność wykorzystywania aktywów, ponieważ te same aktywa są udostępnione równocześnie wielu użytkownikom;
   2.4. zasada indywidualnej odpowiedzialności – za utrzymanie odpowiedniego poziomu bezpieczeństwa poszczególnych aktywów odpowiadają konkretne osoby, które mają świadomość tego, za co są odpowiedzialne i jakie konsekwencje poniosą, jeżeli zaniedbają swoje obowiązki;
   2.5. zasada uzasadnionej obecności – prawo przebywania w określonych pomieszczeniach mają wyłącznie osoby, które są do tego upoważnione lub posiadają tymczasową zgodę wydaną przez władze Spółki;
   2.6. zasada zdrowego rozsądku – nie ma systemów przetwarzania informacji absolutnie bezpiecznych, dlatego zabezpieczenia należy wdrażać w sposób racjonalny, zwracając uwagę na to, aby w wyniku tych wdrożeń nie sparaliżować funkcjonowania organizacji spółki;

2.7. zasada przywilejów koniecznych – każdy użytkownik systemu przetwarzania informacji posiada prawa ograniczone wyłącznie do tych usług, które są konieczne do wykonywania powierzonych mu zadań;

2.8. zasada asekuracji zabezpieczeń – ochrona aktywów systemu przetwarzania informacji nie może opierać się wyłącznie na jednym zabezpieczeniu, nawet, gdy zastosowana technologia jest uznawana za wysoce zaawansowaną i niezawodną;

2.9. zasada najsłabszego ogniwa – w pracach nad doskonaleniem zabezpieczeń trzeba mieć świadomość, że jakość systemu zabezpieczeń wyznacza najsłabszy jego element;

2.10. zasada ochrony niezbędnej – minimalny wymagany poziom bezpieczeństwa informacji wynika z obowiązujących przepisów prawa;

2.11. zasada naturalnego styku z użytkownikiem – procedury bezpieczeństwa informacji, niezależnie od ich natury, nie mogą znacząco zmieniać dotychczasowego sposobu pracy, a także nie mogą w szczególności prowadzić do drastycznego utrudnienia tej pracy;

2.12. zasada „wszystko jest zabronione, dopóki nie jest wyraźnie dozwolone” – zabezpieczenia należy wdrażać w sposób racjonalny, zwracając uwagę, by w wyniku tych wdrożeń nie sparaliżować funkcjonowania organizacji (nie ma absolutnie bezpiecznych systemów przetwarzania informacji).

5. ORGANIZACJA BEZPIECZEŃSTWA INFORMACJI

§ 19.

1. Właściwe zarządzanie bezpieczeństwem informacji w Spółce zapewnia wewnętrzna struktura organizacyjna, w której skład wchodzą w szczególności:
   1.1. Prezes Spółki;
   1.2. Zarząd Spółki;
   1.3. właściciele aktywów.
2. Odpowiedzialność za bezpieczeństwo informacji w Spółce ponoszą:
   2.1. wszyscy pracownicy Spółki – w zakresie odpowiednim do nałożonych na nich obowiązków oraz posiadanych przez nich uprawnień;
   2.2. osoby zatrudnione w Spółce w ramach praktyki lub stażu – w zakresie określonym w umowie o odbywaniu praktyki lub stażu albo w programie praktyki lub stażu;
   2.3. osoby świadczące na rzecz Spółki, w związku z realizacją umowy, usługi, które mogą wpływać na poufność lub integralność informacji i dostępność aktywów wykorzystywanych w Spółce przez procesy przetwarzania informacji – w zakresie określonym w umowie.

§ 20.

1. W związku z posiadanymi kompetencjami i obowiązkami wynikającymi z przepisów prawa, Prezes Spółki odpowiada w szczególności za:
   1.1. utworzenie w Spółce odpowiedniej struktury organizacyjnej, zapewniającej właściwe zarządzanie bezpieczeństwem informacji;
   1.2. powołanie zespołu odpowiedzialnego za zapewnienie warunków organizacyjnych dla realizacji polityki bezpieczeństwa informacji w Spółce oraz nadzór nad jej realizacją;
   1.3. określenie dla komórek organizacyjnych zadań mających na celu zapewnienie bezpieczeństwa informacji;
2. Odpowiedzialność Zarządu Spółki za bezpieczeństwo informacji wynika z **Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)**.
3. Zarząd Spółki odpowiada za ustanowienie i doskonalenie zasad polityki, koordynację działań w zakresie bezpieczeństwa informacji oraz nadzór nad SODO, a w szczególności dokonywanie przeglądów polityki bezpieczeństwa informacji i podejmowanie działań doskonalących.
4. Dobrą praktyką w ramach zarządzania bezpieczeństwem informacji jest przeprowadzenie, nie rzadziej niż raz w roku, audytu wewnętrznego w zakresie bezpieczeństwa informacji oraz ocenę efektywności, skuteczności i adekwatności zarządzania ryzykiem w bezpieczeństwie informacji.

6. BEZPIECZEŃSTWO ZASOBÓW LUDZKICH

§ 21.

Celem zarządzania bezpieczeństwem zasobów ludzkich jest zapewnienie na odpowiednim poziomie bezpieczeństwa informacji w Spółce poprzez ograniczenie ryzyk, które są następstwem błędu ludzkiego, kradzieży, nadużycia lub niewłaściwego użytkowania zasobów informacyjnych i środków przetwarzania informacji.

§ 22.

1. Bezpieczeństwo zasobów ludzkich osiąga się poprzez zapewnienie kompetentnych, uczciwych i świadomych w zakresie bezpieczeństwa informacji osób wykonujących prace na rzecz Spółki. Realizuje się to:

   1.1. przed zatrudnieniem – zapewniając, że osoby wykonujące pracę na rzecz Spółki spełniają formalne wymagania ustalone dla danego stanowiska pracy w zakresie doświadczenia zawodowego i kwalifikacji;

   1.2. podczas zatrudnienia – zapewniając, że osoby wykonujące pracę na rzecz Spółki są świadome zagrożeń, swoich obowiązków i odpowiedzialności prawnej oraz są szkolone w zakresie procedur bezpieczeństwa i poprawnego korzystania ze środków przetwarzania informacji;

   1.3. po ustaniu zatrudnienia lub zmianie stanowiska – zapewniając, że:

      1.3.1. osoby kończące pracę w Spółce mają określoną odpowiedzialność w zakresie bezpieczeństwa informacji w związku z zakończeniem pracy,

      1.3.2. osoby kończące pracę w Spółce lub zmieniające stanowisko dokonują w sposób określony w wewnętrznych aktach prawnych zwrotu posiadanych aktywów,

      1.3.3. osobom kończącym pracę w Spółce są odbierane prawa dostępu do informacji i środków przetwarzania informacji,

      1.3.4. osobom zmieniającym stanowisko są odpowiednio modyfikowane prawa dostępu do informacji i środków przetwarzania informacji.

2. Cel zarządzania bezpieczeństwem zasobów ludzkich osiąga się m. in. dzięki ustanowionym zasadom i procedurom normującym: weryfikację kandydatów do pracy podczas naboru i zatrudniania pracowników, upoważnianie do dostępu do zasobów, postępowanie w przypadku naruszenia bezpieczeństwa informacji oraz rozwiązywanie umów o pracę.

§ 23.

1. Odpowiedzialność za kształtowanie i realizację polityki personalnej, w aspekcie bezpieczeństwa zasobów ludzkich, ponosi Zarząd Spółki.
2. Uszczegółowienie Polityki bezpieczeństwa w obszarze bezpieczeństwa zasobów ludzkich zawiera załącznik Nr 4.

7. BEZPIECZEŃSTWO FIZYCZNE I ŚRODOWISKOWE

§ 24.

1. Celem zarządzania bezpieczeństwem fizycznym i środowiskowym jest zapewnienie na odpowiednim poziomie bezpieczeństwa informacji w budynkach użytkowanych przez Spółkę, poprzez zabezpieczenie danych, w szczególności przed nieautoryzowanym dostępem fizycznym, uszkodzeniami lub awariami systemów wspomagających oraz innymi zagrożeniami fizycznymi i środowiskowymi.
2. Bezpieczeństwo fizyczne i środowiskowe osiąga się wdrażając odpowiednie zabezpieczenia, które w szczególności polegają na zapewnieniu ochrony aktywów przed nieautoryzowanym dostępem fizycznym oraz uszkodzeniami lub zakłóceniami sieci zasilania elektrycznego lub innych systemów wspomagających, funkcjonujących w budynkach i pomieszczeniach użytkowanych przez jednostki organizacyjne Spółki.

§ 25.

1. Zarządzanie bezpieczeństwem fizycznym i środowiskowym w Spółce oparte jest na następujących zasadach ogólnych:
   1.1. ochronie fizycznej i środowiskowej podlegają wszystkie budynki użytkowane przez Spółkę wraz z instalacjami, w jakie są one wyposażone oraz wszystkie aktywa rozmieszczone w tych budynkach;
   1.2. elementy systemów i sieci teleinformatycznych powinny być rozmieszczone i chronione w taki sposób, aby ograniczyć ryzyko płynące z zagrożeń i niebezpiecznych czynników środowiskowych oraz możliwości nieuprawnionego dostępu;
   1.3. aktywa krytyczne powinny być zlokalizowane w strefach ograniczonego dostępu, a wejścia do tych stref powinny być kontrolowane;
   1.4. systemy wspomagające powinny być regularnie sprawdzane pod kątem poprawności funkcjonowania;
   1.5. sprzęt informatyczny i nośniki informacji wynoszone poza siedzibę Spółki powinny być zabezpieczone przed nieuprawnionym dostępem lub zniszczeniem;
   1.6. z wycofywanych z użycia urządzeń i nośników informacji powinny być, w sposób nieodwracalny, usuwane informacje;

§ 26.

1. Odpowiedzialność za bezpieczeństwo fizyczne aktywów Spółki ponosi Zarząd Spółki lub osoba przez zarząd wyznaczona. Zaleca się opracowanie i wdrożenie w Spółce zasad ochrony osób i mienia.
2. Uszczegółowienie Polityki bezpieczeństwa w obszarze bezpieczeństwa fizycznego i środowiskowego zawiera załącznik Nr 5.

8. ZARZĄDZANIE SYSTEMAMI I SIECIAMI

8.1. Procedury eksploatacyjne i zakresy odpowiedzialności

§ 27.

1. W zakresie dokumentowania procedur eksploatacyjnych:
   1.1. w celu zapewnienia prawidłowej i bezpiecznej eksploatacji środków przetwarzania informacji Spółki, zaleca się wdrożyć procedury eksploatacyjne, a także przypisać odpowiedzialność w zakresie zarządzania i eksploatacji wszystkich środków przetwarzania informacji;
   1.2. procedury eksploatacyjne powinny być utrzymywane i dostępne dla wszystkich użytkowników, którym są one niezbędne;
   1.3. realizacja procedur eksploatacyjnych powinna być dokumentowana;
   1.4. procedury eksploatacyjne powinny uwzględniać podział obowiązków pomiędzy administratorami i użytkownikami systemu teleinformatycznego Spółki;
   1.5. procedury eksploatacyjne powinny obejmować w szczególności:
      1.5.1. tworzenie kopii zapasowych,
      1.5.2. odtwarzanie systemu po awarii,
      1.5.3. konserwację sprzętu.
2. Dokumentacja powykonawcza infrastruktury oraz dokumentacja techniczna, administratora i użytkownika podlega ochronie. Dokumentacja ta udostępniana jest zgodnie z zasadą wiedzy koniecznej.

3. Za aktualność i kompletność dokumentacji odpowiada właściciel aktywu, którego dotyczy dokumentacja.

8.2. Ochrona przed kodem złośliwym

§ 28.

1. Za ochronę przed kodem złośliwym odpowiada Zarząd Spółki lub osoba przez zarząd wyznaczona.
2. Zezwala się na wykorzystywanie w sieci teleinformatycznej Spółki wyłącznie oprogramowania dopuszczonego do eksploatacji w Spółce.

§ 29.

1. Ochrona zasobów informatycznych Spółki przed kodem złośliwym powinna być oparta na oprogramowaniu wykrywającym i naprawczym, na świadomości w zakresie bezpieczeństwa oraz mechanizmach kontroli dostępu i zarządzania zmianami. W tym celu wymaga się:
   1.1. wdrożenia zabezpieczeń zapobiegających, wykrywających i usuwających kod złośliwy na każdej stacji roboczej oraz serwerach (jeśli takie serwerowe zabezpieczenia istnieją;

1.2. używania oprogramowania wykrywającego i naprawczego, korzystającego z automatycznego uaktualniania wzorców i mechanizmów skanujących (aktualizacja sygnatur szkodliwego oprogramowania powinna być prowadzona automatycznie); jeżeli automatyczna dystrybucja nowych sygnatur szkodliwego oprogramowania nie jest możliwa, powinna być prowadzona manualnie, co najmniej raz na tydzień;

1.3. sprawdzania wszystkich plików na informatycznych nośnikach danych oraz plików otrzymywanych poprzez sieć pod kątem obecności kodu złośliwego;

1.4. przeprowadzania raz na tydzień (po godzinach pracy) sprawdzeń wszystkich plików na stacjach roboczych pod kątem obecności kodu złośliwego;

1.5. traktowania jako incydentu związanego z bezpieczeństwem informacji każdego przypadku stwierdzenia obecności niezatwierdzonych plików lub nieautoryzowanych poprawek;

1.6. sprawdzania załączników poczty elektronicznej oraz ściąganych danych pod kątem obecności kodu złośliwego; sprawdzanie powinno odbywać się w różnych miejscach, np. na serwerach poczty elektronicznej, stacjach roboczych oraz podczas logowania ze stacji zewnętrznych do sieci Spółki;

1.7. sprawdzania stron internetowych pod kątem obecności kodu złośliwego;

1.8. wprowadzenia zabezpieczeń przed wprowadzeniem kodu złośliwego w trakcie konserwacji lub wykonywania procedur awaryjnych, kiedy możliwe jest obejście mechanizmów ochrony przed kodem złośliwym.

8.3. Kopie zapasowe

§ 30.

1. Kopie zapasowe systemów, aplikacji i baz danych eksploatowanych w Spółce wykonuje się w celu zapewnienia możliwości odtworzenia w przypadku utraty aktualnie użytkowanych danych, konfiguracji systemów i aplikacji.
2. Kopie zapasowe powinny być tworzone i testowane w sposób regularny w odniesieniu do baz danych, a w odniesieniu do oprogramowania i ustawień systemowych – przed i po dokonaniu zmiany konfiguracyjnej.

§ 31.

1. Za tworzenie kopii zapasowych odpowiedzialna jest osoba wyznaczona przez Zarząd Spółki.
2. Wymaga się stworzenia i zatwierdza zasad i procedur tworzenia kopii zapasowych. Zasady te powinny określać w szczególności: częstotliwość tworzenia, rodzaj kopii, ilość kopii oraz miejsce, okres i sposób ich przechowywania.
3. Szczegółowe zasady wykonywania kopii zapasowych aktywów krytycznych określa załącznik Nr 6.

8.4. Zarządzanie bezpieczeństwem sieci

§ 32.

Za bezpieczne zarządzanie siecią teleinformatyczną Spółki odpowiada Zarząd Spółki lub osoba przez Zarząd wyznaczona.

§ 33.

Bezpieczne zarządzanie siecią teleinformatyczną Spółki ma na celu ochronę sieci przed zagrożeniami wewnętrznymi i zewnętrznymi oraz utrzymanie bezpieczeństwa systemów i aplikacji sieciowych, a w szczególności przesyłanych informacji. W tym celu należy:

1. stosować techniki kryptograficzne do przesyłania danych poprzez infrastrukturę sieciową niezarządzaną przez pracowników Spółki;
2. wdrożyć zabezpieczenia mające na celu ochronę integralności i poufności danych przesyłanych przez sieci publiczne lub bezprzewodowe oraz ochronę przyłączonych systemów i aplikacji;
3. wdrożyć mechanizmy monitorowania i tworzenia dzienników zdarzeń w celu umożliwienia rejestracji działań związanych z bezpieczeństwem;
4. stosować techniki zabezpieczania usług sieciowych, takie jak: uwierzytelnienie, szyfrowanie i zabezpieczenie połączeń;
5. wyłączać zbędne usługi sieciowe;
6. monitorować bezpieczeństwo usług świadczonych przez zewnętrznego dostawcę, zapewniając sobie takie prawo w umowach o świadczenie usług.

§ 34.

1. Zabrania się podłączania stacji roboczych jednocześnie do sieci Spółki i innej sieci teleinformatycznej.
2. Zezwala się na podłączanie urządzeń wielofunkcyjnych (typu drukarka, skaner, fax) jednocześnie do sieci Spółki i sieci telefonicznej.

8.5. Obsługa informatycznych nośników danych

§ 35.

1. Wymienne informatyczne nośniki danych powinny być przechowywane i eksploatowane zgodnie z zaleceniami producenta, w taki sposób, aby uchronić zapisaną na nich informację przed nieautoryzowanym ujawnieniem lub niewłaściwym użyciem.
2. Szczegółowe zasady zarządzania wymiennymi informatycznymi nośnikami danych oraz zasady ich niszczenia określa załącznik Nr 6.

8.6. Wymiana informacji

§ 36.

1. Za bezpieczeństwo wymiany informacji odpowiada właściciel zasobu informacyjnego.

2. Bezpieczna wymiana informacji w sieci teleinformatycznej Spółki polega na zapewnieniu ochrony tej informacji przed przechwyceniem, kopiowaniem, modyfikacją, błędnym przekierowaniem i zniszczeniem.

§ 37.

1. W celu zapewnienia bezpieczeństwa wymiany informacji, w sieci teleinformatycznej Spółki należy przechowywać informacje na centralnych zasobach sieciowych lub w systemach informatycznych, zamiast na lokalnych zasobach, oraz minimalizować użycie informatycznych nośników danych.
2. W przypadku przekazywania plików, których treść wg właściciela zasobu informacyjnego podlega ochronie, wymaga się stosowania metod kryptograficznych lub co najmniej szyfrowania poprzez kompresję pliku z hasłem. Pliki mogą być przekazywane za pośrednictwem informatycznego nośnika danych lub z wykorzystaniem protokołu korzystającego z metod kryptograficznych. Dostęp do serwera, którego usługa opiera się na tym protokole, musi być imienny (login) i zabezpieczony hasłem, przy czym hasło powinno być przekazywane inną metodą lub drogą niż zaszyfrowane dane.
3. Zezwala się na przyłączanie urządzeń przenośnych (np. smartfon, tablet) do sieci Spółki pod warunkiem, że będą one komunikować się wyłącznie z określonymi serwerami (np. serwerem pocztowym).
4. Szczegółowe zasady bezpiecznego korzystania z urządzeń przenośnych określa załącznik Nr 6.

§ 38.

1. W zakresie korzystania z poczty elektronicznej wymaga się:
   1.1. ochrony wiadomości przed nieupoważnionym dostępem, modyfikacją lub odmową usługi;
   1.2. zapewnienia poprawnej adresacji;
   1.3. zapewnienia niezawodności i dostępności usług;
   1.4. ochrony przed atakami na pocztę elektroniczną;
   1.5. ochrony przed niechcianymi wiadomościami (tzw. spamem);
   1.6. zapewnienia możliwości użycia technik kryptograficznych;
   1.7. zachowywania wiadomości, przez okres 3 lat, na potrzeby prowadzenia postępowań wyjaśniających;
   1.8. aby udostępnianie skrzynki pocztowej pracownika innym osobom miało charakter wyjątkowy, podyktowany istotnymi względami służbowymi, a stały użytkownik poczty elektronicznej został o tym fakcie poinformowany;
   1.9. zapewnienia kontroli udostępniania skrzynek pocztowych innym użytkownikom.
2. Za bezpieczną eksploatację systemu poczty elektronicznej odpowiada Zarząd Spółki lub osoba przez Zarząd wyznaczona
3. Szczegółowe zasady bezpiecznego korzystania z Internetu i poczty elektronicznej określa załącznik Nr 6.

8.7. Monitorowanie

§ 39.

1. Rejestrowane i monitorowane powinny być wszystkie zdarzenia polegające na użyciu urządzeń informatycznych i sieciowych oraz programów narzędziowych i diagnostycznych, zapewniając weryfikację i rozliczalność użytkowników wykonujących zadania, do których zostali uprawnieni.
2. Zaleca się, aby rejestrowaniu podlegały:
   2.1. identyfikator użytkownika;
   2.2. data, czas i szczegóły ważnych zdarzeń, w tym rozpoczęcia i zakończenia pracy w systemie;
   2.3. identyfikator lub lokalizacja stacji roboczej;
   2.4. pomyślne i niepomyślne próby dostępu do systemu, danych i innych zasobów;
   2.5. aktywacje i dezaktywacje systemów ochrony, w szczególności takich jak oprogramowanie antywirusowe i systemy wczesnego wykrywania włamań.

§ 40.

Zarejestrowane dane z monitoringu działań użytkowników oraz zdarzenia związane z bezpieczeństwem informacji, na potrzeby ewentualnych postępowań wyjaśniających oraz monitorowania kontroli dostępu, powinny być przechowywane przez okres 2 lat (jeśli pozwala na to dostępna przestrzeń).

§ 41.

Wymaga się, aby uniemożliwić – o ile to wykonalne – administratorom systemów kasowanie, modyfikację lub dezaktywację dzienników zawierających zapisy o ich własnych działaniach.

§ 42.

Zaleca się prowadzenia rejestrów działań administratorów i operatorów systemów zawierających informacje pozwalające na ustalenie:

1. czasu wystąpienia zdarzenia;
2. efektu zdarzenia (powodzenie, niepowodzenie);
3. zasobów wykorzystanych w zdarzeniu;
4. konta użytego do zainicjowania zdarzenia oraz identyfikację administratora lub operatora;
5. błędu systemowego i podjętych działań naprawczych;
6. informacji o sesjach zewnętrznych połączeń zdalnych;
7. zmiany oprogramowania lub wersji;
8. użytych programów narzędziowych;
9. zmiany konfiguracji sprzętu, systemu operacyjnego i oprogramowania.

§ 43.

1. Odpowiednia dokładność i możliwość korelacji rejestrów zdarzeń, których zapisy mogą służyć jako dowody w postępowaniu w przypadku naruszenia bezpieczeństwa, jest zapewniona przez właściwe ustawienie zegarów urządzeń teleinformatycznych.
2. Wymaga się synchronizacji zegarów wszystkich systemów przetwarzania informacji w organizacji lub domenie z uzgodnionym, dokładnym i redundantnym źródłem czasu.

9. KONTROLA DOSTĘPU

5.0. Wymagania wobec kontroli dostępu

§ 44.

Za organizację systemu kontroli dostępu do informacji oraz środków przetwarzania informacji odpowiada Zarząd Spółki lub osoba przez Zarząd wyznaczona.

§ 45.

1. Nadawanie uprawnień dostępu powinno być realizowane na podstawie formalnych wniosków.
2. Nadane uprawnienia powinny być odbierane niezwłocznie po ustaniu potrzeby ich posiadania.

§ 46.

1. W przypadku konieczności natychmiastowego odebrania lub ograniczenia uprawnień pracownika dopuszcza się możliwość zastosowania uproszczonego trybu polegającego na przekazaniu stosownej informacji pocztą elektroniczną przez jego bezpośredniego przełożonego lub pracownika kierującego komórką ochrony informacji.
2. W wyjątkowych sytuacjach, podyktowanych istotnymi względami służbowymi, dopuszcza się przejęcie wszystkich uprawnień pracownika (np. poprzez wygenerowanie nowego hasła) przez jego przełożonego. Fakt ten musi być udokumentowany w postaci notatki służbowej, z którą należy zapoznać pracownika, kierownika jednostki organizacyjnej i właściwą komórkę ochrony informacji.

5.1. Zarządzanie dostępem użytkowników

§ 47.

1. Użytkownik sieci teleinformatycznej Spółki powinien być jednoznacznie identyfikowany poprzez indywidualny identyfikator, aby można było przypisać poszczególnym użytkownikom określone działania i odpowiedzialność za nie.
2. Wprowadzenie identyfikatorów grupowych powinno być zatwierdzane, a ich użycie udokumentowane w sposób umożliwiający jednoznaczną identyfikację użytkowników z nich korzystających.
3. Raz użyty identyfikator nie może być przydzielony innemu użytkownikowi.

§ 48.

Wymaga się:

1. okresowego, nie rzadziej niż raz w roku, przeglądu nadanych uprawnień;
2. przeglądu i ponownego nadania praw dostępu użytkowników, gdy zmieniają oni miejsce zatrudnienia w Spółce;
3. blokowania kont po 30 dniach nieaktywności (jeśli system pozwala na zablokowanie konta).

5.2.Zarządzanie hasłami

§ 49.

1. Niedopuszczalne jest występowanie kont niezabezpieczonych hasłami.
2. Należy wymuszać natychmiastową zmianę hasła początkowego przydzielonego użytkownikowi.
3. Hasła nowe, zastępcze lub tymczasowe mogą być przekazywane po uprzedniej weryfikacji tożsamości użytkownika.
4. Zabrania się przekazywania haseł przez osoby trzecie lub za pośrednictwem otwartych wiadomości pocztowych. Dopuszcza się przekazanie hasła za pomocą jednego z poniższych sposobów:
   4.1. odbiór hasła osobiście przez użytkownika;
   4.2. szyfrowanie z użyciem klucza publicznego odbiorcy;
   4.3. zabezpieczenie za pomocą programów „pakujących", przy czym klucz rozpakowujący przekazywany jest inną drogą niż „spakowany" plik z hasłem;
   4.4. dzielenie hasła i przekazywanie go dwiema niezależnymi drogami; zezwala się na przekazywanie haseł tymczasowych lub jednorazowych w całości drogą telefoniczną.
5. Zabrania się pozostawiania bez zmiany haseł domyślnych, dostarczonych przez producenta w trakcie instalacji systemu lub oprogramowania.
6. Hasło dobrej jakości:
   6.1. ma długość co najmniej 8 znaków – dla standardowego konta użytkownika;
   6.2. ma długość co najmniej 10 znaków – dla konta uprzywilejowanego;
   6.3. ma długość co najmniej 12 znaków – jeżeli jest wykorzystywane jako klucz szyfrowania informacji;
   6.4. składa się ze znaków wchodzących w skład co najmniej trzech grup znaków spośród następujących czterech grup: małe litery, duże litery, cyfry, znaki specjalne;
   6.5. nie jest oparte na prostych skojarzeniach, łatwych do odgadnięcia lub wywnioskowania z informacji dotyczącej danej osoby;
   6.6. nie jest podatne na atak słownikowy;
   6.7. nie zawiera ciągu jednakowych znaków ani grup znaków złożonych z samych cyfr lub samych liter.

§ 50.

W zakresie haseł administracyjnych zasobów o najwyższych uprawnieniach dotyczących np. systemów, serwerów, baz danych, aplikacji, urządzeń aktywnych sieci:

1. wymaga się przechowywania duplikatów haseł;
2. duplikaty haseł przechowuje się w bezpiecznych kopertach, które uniemożliwiają otwarcie bez uszkodzenia ich struktury; koperty przechowuje się w miejscu zapewniającym dostęp wyłącznie osobom upoważnionym;

3. na kopercie należy umieścić datę jej złożenia, podpis osoby składającej oraz skróconą nazwę przynależności hasła;
4. zaleca się prowadzenia ewidencji kopert zawierających hasła;
5. za aktualność przechowywanych haseł odpowiada bezpośrednio administrator zarządzający danym hasłem;
6. awaryjne otwarcie koperty z hasłem wymaga akceptacji właściciela zasobu lub osoby przez niego upoważnionej i udokumentowania w ewidencji kopert (jeżeli jest prowadzona); po użyciu generowane jest nowe hasło, którego kopia przechowywana jest na identycznych zasadach;
7. koperty z nieaktualnym hasłami podlegają niszczeniu;
8. zezwala się na stosowanie, zamiast kopert, odpowiedniego systemu elektronicznego (managera haseł).

§ 51.

1. Wymaga się, aby system zarządzania hasłami:
   1.1. wymuszał użycie indywidualnych identyfikatorów użytkownika i haseł zapewniających zachowanie rozliczalności;
   1.2. zezwalał użytkownikom na wybór i zmianę własnych haseł oraz zawierał procedurę potwierdzania zmian haseł dla unikania błędów w ich wprowadzaniu;
   1.3. wymuszał wybór haseł dobrej jakości;
   1.4. wymuszał okresową zmianę haseł, chyba że stosowane są silniejsze metody uwierzytelniania;
   1.5. wymuszał zmianę haseł tymczasowych przy pierwszym logowaniu się do systemu;
   1.6. prowadził, jeżeli to technicznie możliwe, spis co najmniej pięciu poprzednich haseł użytkowników oraz zapobiegał ponownemu ich użyciu;
   1.7. blokował wyświetlanie haseł na ekranie podczas ich wprowadzania;
   1.8. przechowywał i przesyłał hasła w formie zabezpieczonej.
2. Dopuszcza się alternatywne metody silnego uwierzytelniania i weryfikacji tożsamości, takie jak: metody kryptograficzne, karty elektroniczne, tokeny lub metody biometryczne.

5.3. Odpowiedzialność użytkowników

§ 52.

Wszyscy użytkownicy są zobowiązani do:

1. utrzymywania hasła w tajemnicy;
2. unikania zapisywania haseł, chyba że mogą one być przechowywane w bezpieczny sposób, a metoda przechowywania została zatwierdzona przez kierownika komórki organizacyjnej;
3. niezwłocznej zmiany hasła w przypadku, gdyby cokolwiek mogło wskazywać na możliwość naruszenia bezpieczeństwa systemu lub hasła;

4. wybierania hasła dobrej jakości;
5. zmieniania hasła co najmniej raz na 90 dni – zalecanym okresem użytkowania hasła jest 30 dni;
6. unikania powtarzania lub cyklicznego używania starych haseł;
7. zmiany hasła tymczasowego podczas pierwszego logowania się do systemu;
8. niewprowadzania haseł do zautomatyzowanych procesów logowania, np. w makrach lub przeglądarkach internetowych;
9. nieudostępniania swoich haseł innym użytkownikom;
10. niekorzystania z takiego samego hasła w celach służbowych i pozasłużbowych.

§ 53.

Wymaga się, aby użytkownicy sieci teleinformatycznej Spółki:

1. zamykali aktywne sesje po zakończeniu pracy, chyba że są one zabezpieczone przez mechanizm blokujący, np. wygaszacz ekranu chroniony hasłem;
2. wyrejestrowywali się z serwerów i stacji roboczych w chwili zakończenia sesji;
3. zabezpieczali nieużywane w danym momencie komputery osobiste lub terminale przed nieupoważnionym dostępem poprzez blokadę klawiatury lub w inny równoważny sposób, np. dostęp do komputera po podaniu hasła.

5.4.Kontrola dostępu do sieci

§ 54.

Za bezpieczny dostęp do sieci odpowiada Zarząd Spółki lub osoba przez Zarząd wyznaczona.

§ 55.

Przy korzystaniu z usług sieciowych wymaga się aby:

1. zdalny dostęp dla stron trzecich był zatwierdzony przez właściciela zasobu teleinformatycznego, do którego dostęp ma zostać udzielony;
2. autoryzacja uprawnień dostępu do sieci i usług sieciowych odbywała się w sposób formalny;

§ 56.

Zaleca się:

1. zabronić przyłączania do sieci wewnętrznej Spółki urządzeń, które nie są kontrolowane i zarządzane przez pracowników Spółki;
2. zabronić podłączania informatycznych nośników danych zawierających dane prywatne do urządzeń wchodzących w skład infrastruktury teleinformatycznej Spółki.

5.5.Kontrola dostępu do systemów operacyjnych

§ 57.

Za bezpieczny dostęp do systemów operacyjnych odpowiada Zarząd Spółki lub osoba przez Zarząd wyznaczona..

§ 58.

W celu zapewnienia bezpiecznego systemu logowania należy:

1. ograniczyć liczbę nieudanych prób logowania się do systemu do pięciu prób i blokowanie konta po osiągnięciu tej liczby;
2. rejestrować udane i nieudane próby logowania (jeśli to możliwe);
3. blokować wyświetlanie hasła w trakcie wprowadzania lub ukrywać wprowadzane znaki pod symbolami;
4. blokować przesyłanie haseł przez sieć jawnym tekstem;
5. nie dopuszczać, aby rutynowe działania użytkownika były wykonywane z kont uprzywilejowanych;
6. jeśli to możliwe zamykać nieaktywne sesje po przekroczeniu zdefiniowanego okresu braku aktywności, za wyjątkiem określonych sytuacji wynikających z technologii przetwarzania danych.

5.6. Zdalny dostęp do sieci teleinformatycznej Spółki za pośrednictwem sieci publicznej

§ 59.

Za zdalny dostęp do sieci teleinformatycznej Spółki za pośrednictwem sieci publicznej odpowiada Zarząd Spółki lub osoba przez Zarząd wyznaczona.

§ 60.

Wymaga się:

1. aby zdalny dostęp był możliwy wyłącznie po pomyślnej identyfikacji i uwierzytelnieniu oraz jeśli to możliwe, zastosowaniu odpowiednich do zagrożeń mechanizmów kryptograficznych kontroli dostępu, w szczególności:
   1.1. stosowania metody dwuskładnikowego uwierzytelniania,
   1.2. uwierzytelniania zdalnych użytkowników poprzez stosowanie certyfikatów i silnych haseł (co najmniej 10 znaków);
   1.3. aby dostęp do aktywów krytycznych lub dostęp z kont uprzywilejowanych:
   1.4. nie był stały, lecz na żądanie, po uprzednim kontakcie telefonicznym lub mailowym,
   1.5. szyfrowania ruchu;
   1.6. aby komputery, z których nawiązywany jest zdalny dostęp, były zarządzane, konfigurowane i administrowane wyłącznie przez administratorów Spółki (jeśli to możliwe);
   1.7. aby zdalny dostęp dla firm zewnętrznych był możliwy pod warunkiem, że zasady współpracy pomiędzy Spółką a firmą zewnętrzną w zakresie zdalnego dostępu będą wynikać z zawartej umowy.

10. ZARZĄDZANIE INCYDENTAMI ZWIĄZANYMI Z BEZPIECZEŃSTWEM INFORMACJI

§ 61.

1. Zaleca się aby w Spółce wdrożyć wewnętrzne akty prawne określające zasady postępowania i działania prowadzone w przypadku wystąpienia incydentów związanych z bezpieczeństwem informacji. Uregulowania te powinny obejmować: identyfikację incydentów, ich zgłaszanie i rejestrację, analizę, nadawanie poziomu ważności, wyszukiwanie powiązań, podejmowanie działań naprawczych i usuwanie przyczyn.
2. Wyróżnia się następujące kategorie incydentów związanych z bezpieczeństwem informacji:
   2.1. incydenty, w następstwie których może wystąpić utrata dostępności lub użyteczności budynków, ich części lub pojedynczych pomieszczeń;
   2.2. incydenty polegające na uzyskaniu przez osoby nieuprawnione fizycznego dostępu do środków przetwarzania informacji, w następstwie których może nastąpić utrata lub uszkodzenie tych środków;
   2.3. incydenty, które prowadzą do braku pracowników niezbędnych do realizowania procesów przetwarzania informacji;
   2.4. incydenty, w następstwie których może wystąpić nieprawidłowa realizacja usług IT lub utrata dostępu do tych usług;
   2.5. incydenty stanowiące naruszenie ochrony informacji prawnie chronionych, w szczególności: danych osobowych lub przepisów o ochronie informacji niejawnych.

§ 62.

1. Zarządzanie incydentami, w następstwie których może wystąpić utrata dostępności lub użyteczności budynków, ich części lub pojedynczych pomieszczeń, jest realizowane zgodnie z decyzjami podjętymi przez Zarząd Spółki.
2. Zarządzanie incydentami polegającymi na uzyskaniu przez osoby nieuprawnione fizycznego dostępu do środków przetwarzania informacji, w następstwie których może nastąpić utrata lub uszkodzenie tych środków, jest realizowane zgodnie z decyzjami podjętymi przez Zarząd Spółki.
3. Zarządzanie incydentami, które prowadzą do braku pracowników niezbędnych do realizowania procesów przetwarzania informacji, jest realizowane zgodnie z decyzjami podjętymi przez Zarząd Spółki.
4. Zarządzanie incydentami, w następstwie których może wystąpić nieprawidłowa realizacja usług IT lub utrata dostępu do tych usług, jest realizowane zgodnie z decyzjami podjętymi przez Zarząd Spółki.
5. Zarządzanie incydentami związanymi z bezpieczeństwem informacji, stanowiącymi naruszenie ochrony informacji prawnie chronionych, jest realizowane zgodnie z decyzjami podjętymi przez Zarząd Spółki.

11. ZGODNOŚĆ

§ 63.

Systemy informacyjne użytkowane w przedsiębiorstwie i funkcjonujące zabezpieczenia, których celem jest zapewnienie bezpieczeństwa informacji na odpowiednim poziomie, muszą spełniać wymagania określone w przepisach prawa, w szczególności w przepisach o ochronie danych osobowych.

§ 64.

1. Na polecenia najwyższego kierownictwa systematycznie identyfikuje się, dokumentuje oraz monitoruje zgodność funkcjonowania technologii informatycznej i bezpieczeństwa środowiska teleinformatycznego z wymaganiami prawnymi, wewnętrznymi aktami prawnymi, zawartymi umowami i przyjętymi w Spółce standardami.
2. Na polecenie najwyższego kierownictwa wyznaczeni pracownicy lub Inspektor Ochrony Danych Osobowych (jeśli został powołany) prowadzą działania mające na celu spełnienie wymagań bezpieczeństwa określonych w przepisach o ochronie danych osobowych oraz zgodnie z uregulowaniami odrębnych aktów prawnych.

12. ZAŁĄCZNIKI DO POLITYKI BEZPIECZEŃSTWA

załącznik Nr 1. Rejestr czynności przetwarzania danych osobowych

załącznik Nr 2. Polityka bezpieczeństwa informacji w obszarze organizacji bezpieczeństwa

załącznik Nr 3. Polityka bezpieczeństwa informacji w obszarze zarządzania aktywami

załącznik Nr 4. Polityka bezpieczeństwa informacji w obszarze bezpieczeństwa zasobów ludzkich

załącznik Nr 5. Polityka bezpieczeństwa informacji w obszarze bezpieczeństwa fizycznego i środowiskowego

załącznik Nr 6. Polityka bezpieczeństwa informacji w obszarze zarządzania systemami i sieciami

załącznik Nr 7. Procedura prowadzenia wykazu budynków

załącznik Nr 8. Procedura zgłaszania i obsługi naruszeń

załącznik Nr 9. Procedura realizacji obowiązku informacyjnego

załącznik Nr 10. Procedura realizacji praw osób których dane dotyczą

załącznik Nr 11. Procedura monitoringu wizyjnego.

załącznik Nr 12. Procedura nadawania upoważnień.