Załącznik nr 3 do OPZ

ZARZĄDZENIE
Prezesa Zarządu Górnośląskiego Towarzystwa Lotniczego S.A. w Katowicach

Nr 88 z dnia 1 października 2009 roku

w sprawie wprowadzenia Polityki Bezpieczeństwa Systemu Kontroli Dostępu w Międzynarodowym Porcie Lotniczym Katowice w Pyrzowicach

Na podstawie Uchwały Zarządu Górnośląskiego Towarzystwa Lotniczego S.A. w Katowicach Nr 3/X/2009 z dnia 1 października 2009 r., zarządzam co następuje:

§ 1

Wprowadza się *Politykę Bezpieczeństwa Systemu Kontroli Dostępu w Międzynarodowym Porcie Lotniczym Katowice w Pyrzowicach,* stanowiącą **załącznik nr 1** do niniejszego Zarządzenia.

§ 2

Nadzór nad wykonaniem Zarządzenia powierza się Dyrektorowi MPL Katowice oraz Kierownikowi Pionu Bezpieczeństwa.

§ 3

Zarządzenie wchodzi w życie z dniem 2 listopada 2009 r.

Prezes Zarządu

Artur Tomasik

Polityka Bezpieczeństwa Systemu Kontroli Dostępu w Międzynarodowym Porcie Lotniczym Katowice w Pyrzowicach

Sporządziła: Justyna Kycia

Rozdział 1

POSTANOWIENIA OGÓLNE

Dane osobowe w przetwarzane są w celu:

1. Realizacji statutowych ilości wydanych identyfikatorów osobowych dla pracowników zatrudnionych w Międzynarodowym Porcie Lotniczym.
2. W celu weryfikacji osób posiadających identyfikatory osobiste.
3. Dla realizacji innych usprawiedliwionych celów i zadań wynikających z Zarządzenia nr 61 Prezesa Zarządu Górnośląskiego Towarzystwa Lotniczego S.A. w Katowicach z dnia 3 kwietnia 2008 roku ,, W sprawie określenia trybu wydawania przepustek w MPL Katowice w Pyrzowicach."
4. Biuro Przepustek stosuje odpowiednie środki organizacyjne w celu zabezpieczenia danych osobowych oraz zabezpieczeniem Systemu Kontroli Dostępu przed ich udostępnianiem osobom nieupoważnionym, zabraniem oraz skopiowaniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy o ochronie danych osobowych, nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem.
5. Niniejszy dokument opisuje reguły dotyczące zapewnienia bezpieczeństwa Systemu Kontroli Dostępu.
6. **Administratorem Systemu Kontroli Dostępu jest Specjalista ds. Zabezpieczenia Technicznego . Zastępcą Administratora Systemu Kontroli Dostępu jest Specjalista ds. Szkoleń i Kontroli Dostępu.**

Którzy:

1) Nadają uprawnienia do Systemu Kontroli Dostępu, stanowiące załącznik nr 1:
   - Użytkownika
   - Operatora
   - Główne Hasło tzw. ,,SUA Alarmowe"
2) Obowiązkiem osób posiadających dostęp do Systemu Kontroli Dostępu jest przestrzeganie postanowień niniejszej Polityki Bezpieczeństwa.
3) Prowadzą rejestr osób upoważnionych, które posiadają dostęp do Systemu Kontroli Dostępu, wzór rejestru stanowi załącznik nr 2.
4) Nadzorują przeglądy, konserwacje Systemu Kontroli Dostępu.
5) Podejmują stosowne działania zgodnie z niniejszą Polityką Bezpieczeństwa w przypadku otrzymania informacji o naruszeniu zabezpieczeń Systemu Kontroli Dostępu.
6) Dokonują przeglądu niniejszej Polityki Bezpieczeństwa pod kątem aktualności i stosowalności nie rzadziej niż raz na pół roku.
7) W przypadku otrzymania powiadomienia o naruszeniu oplombowanej metalowej skrzynki w której znajduję się Główne Hasło tzw. alarmowe, dokonują zmiany Głównego Hasła Systemu Kontroli Dostępu.
8) W przypadku otrzymania powiadomienia naruszeniu ochrony Systemu Kontroli Dostępu , przeprowadzają postępowanie, stanowiące załącznik nr 3.

Rozdział 2

EWIDENCJA ZASOBÓW

1. Wyjaśnienie używanych pojęć:
   1) Dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
   2) Baza danych osobowych – każdy posiadający strukturę zbiór danych o charakterze osobowym, dostępnych według określonych kryteriów.
   3) Przetwarzanie danych – jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.
   4) Usuwanie danych – zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.
   5) System zarządzania bazą danych – system oprogramowania zawierający mechanizmy zapewniające spójność i bezpieczeństwo danych, sprawny dostęp do danych, środki programistyczne służące do przetwarzania danych, jednoczesny dostęp do danych dla wielu użytkowników, środki pozwalające na regulację dostępu do danych, środki pozwalające na odtworzenie zawartości bazy danych po awarii.
   6) System Informatyczny – zbiór powiązanych ze sobą elementów: serwerów z systemami operacyjnymi, systemu zarządzania bazą danych, baz danych, oprogramowania (programów użytkowych), urządzeń końcowych (komputerów, terminali, drukarek) oraz urządzeń służących do komunikacji między sprzętowymi elementami systemu.
   7) Administrator Systemu – osoba nadająca uprawnienia użytkownikom do poszczególnych funkcji programu.
   8) Uwierzytelnienie – weryfikacja tożsamości użytkownika rejestrującego się w danym systemie; w Systemie Informatycznym Biura Przepustek weryfikacja odbywa się w oparciu o identyfikator i hasło użytkownika.
   9) Autoryzacja – sprawdzenie uprawnień użytkownika w stosunku do określonych zasobów. Systemu Informatycznego oraz operacji jakich może wykonywać.

2. Stacje do zarządzania Systemem Kontroli Dostępu znajdują się:

   - Biuro Przepustek (piętro nr1, stacja nr 2)
   - Centrum Monitoringu (piętro nr 2, stacja nr 1).

Rozdział 3

OPIS ZDARZEŃ NARUSZAJĄCYCH SYSTEM KONTROLI DOSTĘPU

Podział zagrożeń:

1) Zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu); ich wystąpienie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu; ciągłość systemu zostaje zakłócona, nie dochodzi do naruszenia poufności danych,
2) Zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, awarie sprzętowe, błędy oprogramowania), może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych zawartych w Systemie Kontroli Dostępu.
3) Zagrożenia zamierzone (świadome i celowe naruszenia poufności danych w Systemie Kontroli Dostępu); zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy, zagrożenia te możemy podzielić na: nieuprawniony dostęp do systemu kontroli dostępu z zewnątrz (włamanie do systemu), nieuprawniony dostęp do systemu z jego wnętrza, nieuprawniony przekaz danych, pogorszenie jakości sprzętu i oprogramowania, bezpośrednie zagrożenie materialnych składników systemu.

Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia Systemu Kontroli Dostępu:

1) Awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia systemu kontroli dostępu, a także niewłaściwe działanie serwisanta.
2) Pojawienie się odpowiedniego komunikatu alarmowego od części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu.
3) Jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie.
4) Naruszenie lub próba naruszenia integralności systemu.
5) Modyfikacja danych w Systemu Kontroli Dostępu lub zmiana w strukturze danych bez odpowiedniego upoważnienia.
6) Niedopuszczalna manipulacja danymi w Systemie Kontroli Dostępu.
7) Ujawnienie osobom nieuprawnionym danych osobowych albo innych strzeżonych elementów systemu Kontroli Dostępu.
8) Praca w Systemie Kontroli Dostępu, wykazująca nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony danych osobowych (np. praca przy komputerze osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu).
9) Ujawnienie istnienia nieautoryzowanych kont dostępu do danych lub tzw. "bocznej furtki", itp.
10) Rażące naruszenie dyscypliny pracy w zakresie przestrzegania polityki bezpieczeństwa (nie wylogowanie się przed opuszczeniem stanowiska pracy, nie zamknięcie pomieszczenia z komputerem , prace na danymi Systemu Kontroli Dostępu w celach prywatnych, itp.).

Rozdział 4

ZESTAWIENIE ŚRODKÓW ORGANIZACYJNYCH I TECHNICZNYCH ZAPEWNIAJĄCYCH OCHRONĘ SYSTEMU KONTROLI DOSTĘPU

Zabezpieczenia Biura Przepustek oraz Centrum Monitoringu, w którym znajduje się System Kontroli Dostępu:

1) Biuro Przepustek w którym znajduje się stacja do zarządzania Systemem Kontroli Dostępu, stacja nr 2, zamykane jest na klucz oraz w przypadku opuszczenia pomieszczenia przez ostatniego użytkownika, także w godzinach pracy.
2) Po zakończeniu pracy, Biuro Przepustek jest zamykane na klucz, oplombowywane oraz uruchamiany jest alarm.
3) Centrum Monitoringu w którym znajduje się System Kontroli Dostępu – stacja nr 1, jest całodobowo strzeżone przez wartowników WSO SOL oraz poprzez rejestr CCTV.
4) Wejście do Centrum Monitoringu następuje poprzez uwierzytelnienie biometryczne (linie papilarne oraz karta biometryczna).
5) Główne Hasło Systemu Kontroli Dostępu tzw. alarmowe, znajduje się w oplombowanej oraz zamykanej na klucz metalowej skrzynce, która znajduję się w Centrum Monitoringu.

6) Zabezpieczenia przed nieautoryzowanym dostępem do stacji zarządzającej Systemem Kontroli Dostępu znajdującego się w Biurze Przepustek:

1) Podłączenie urządzenia końcowego (komputera, terminala, drukarki) do sieci
2) komputerowej Administracji dokonywane jest przez Administratora Sieci.
3) Udostępnianie użytkownikowi dostępu do Systemu Kontroli Dostępu odbywa się poprzez wydanie upoważnienia przez Administratora Systemu Kontroli Dostępu oraz Zastępcę Administratora Systemu Kontroli Dostępu.
4) Identyfikacja użytkownika w systemie odbywa się poprzez zastosowanie podwójnego uwierzytelnienia (hasło do danej stacji oraz login użytkownika).
5) Przydzielenie indywidualnego identyfikatora każdemu użytkownikowi Systemu Kontroli Dostępu i rejestrowanie przez System czasu logowania użytkownika i rodzaju wprowadzonych przez niego danych (tzw. Rejestr Zdarzeń).
6) Zabrania się użytkownikowi udostępnianie osobie postronnej stanowiska do zarządzania Systemem Kontroli Dostępu do wykonywania wpisów i zmian w Systemie Kontroli Dostępu.
7) Zabezpieczenie hasłami kont na komputerze w którym znajduje się System Kontroli Dostępu.
8) Architektura biura umożliwia wgląd osobom nieupoważnionym w monitor stacji do zarządzania Systemem Kontroli Dostępu.
9) System Kontroli Dostępu pracuje w wyodrębnionej sieci lokalnej.

5. Zabezpieczenia przed utratą danych osobowych zawartych w Systemie Kontroli Dostępu w wyniku awarii:

1) Zasilanie gwarantowane.
2) Ochrona serwera przed zanikiem zasilania poprzez stosowanie zasilaczy zapasowych UPS.
3) Ochrona przed utratą zgromadzonych danych poprzez cykliczne wykonywanie kopii zapasowych, w przypadku awarii odtwarzane są dane i system operacyjny.
4) Zastosowanie ochrony przeciwpożarowej poprzez umieszczenie w pomieszczeniu gaśnicy, okresowa kontrolowanych przez specjalistę.

Rozdział 5

INSTRUKCJA ZARZĄDZANIA SYSTEMEM KONTROLI DOSTĘPU

1. Niniejsza instrukcja określa szczegółowe zasady zarządzania Systemem Kontroli Dostępu .

1) Hasło do Konta użytkownika/operatora alarmowego w Systemie Kontroli Dostępu modyfikuje Administrator Systemu Kontroli Dostępu lub Zastępca Systemu Kontroli Dostępu, na podstawie upoważnienia.
2) Ustanie stosunku pracy lub przejście użytkownika do innej jednostki organizacyjnej GTL S.A., skutkuje usunięciem jego konta z Systemu Kontroli Dostępu .
3) Administrator Systemu Kontroli Dostępu oraz Zastępca Administratora Sytemu Kontroli Dostępu jest operatorem uprzywilejowanym, posiadającym uprawnienia do zmiany Głównego Hasła tzw. alarmowego w Systemie Kontroli Dostępu.
4) Główne Hasło Systemu Kontroli Dostępu jest używane tylko w uzasadnionych przypadkach.
5) Główne Hasło tzw. Awaryjne, Systemu Kontroli Dostępu jest deponowane w Centrum Monitoringu w oplombowanej referentką o numerze: PLK 38 K-ce lub PLK 70 K-ce, metalowej skrzynce.
6) Tylko operator mający uprawnienia do Głównego Hasła tzw. awaryjnego ma prawo uruchomić stacje nr 1, która znajduje się w Centrum Monitoringu.
7) Dokonanie otwarcia tzw. metalowej skrzynki i uzyskanie Głównego Hasła tzw. awaryjnego przez operatora, który posiada uprawnienia, jest odnotowywane przez niego w rejestrze wykonanych obowiązków służbowych – karta stanowiska pracy na stacji nr 1 stanowi załącznik nr 6
8) Osoba upoważniona, która użyła Głównego Hasła, o zaistniałym fakcie powiadamia drogą telefoniczną Administratora Sytemu Kontroli Dostępu lub Zastępcy Administratora Systemu Kontroli Dostępu. Następnie dokonuje adnotacji w rejestrze użycia Głównego Hasła (karta stanowiskowa pracy). Załącznik nr 5
9) Po każdorazowej zmianie użycia głównego hasła, Administrator dokonuje zmiany Głównego Hasła.
10) Administrator Systemu Kontroli Dostępu lub Zastępca Administratora Systemu Kontroli Dostępu nadaje uprawnienia użytkownikom do poszczególnych funkcji programu zgodnie z zakresem upoważnień.

2. Metody i środki uwierzytelniania

1) Uwierzytelnienie użytkownika/operatora w Systemie Kontroli Dostępu następuje po podaniu nazwy użytkownika - login oraz hasła.
2) Hasła użytkownika/operatora serwera są szyfrowane.
3) Użytkownik/operator nie może udostępniać swojej nazwy użytkownika i hasła innej osobie.
4) Nazwa użytkownika/operatora składa się z 3 do 8 znaków (liter łacińskich lub/i cyfr).
5) Hasło musi zawierać minimum 6 znaków, w tym mała, duża litera, znak specjalny, cyfra.
6) Hasło nie może być takie samo jak nazwa użytkownika/operatora.
7) Hasło nie może być zapisane w miejscu dostępnym dla osób nieuprawnionych.

Rozdział 6

PROCEDURY ROZPOCZĘCIA, ZAWIESZENIE I ZAKOŃCZENIA PRACY W SYSTEMIE KONTROLI DOSTĘPU

Rozpoczęcie pracy:

1) Włączenie monitora i komputera.
2) Zalogowanie się do Systemu Kontroli Dostępu poprzez wprowadzenie nazwy użytkownika i hasła.
3) Uruchomienie programu Delta Controls.

Zawieszenie pracy w przypadku czasowego opuszczenia stanowiska pracy:

1) Wylogowanie z Systemu Kontroli Dostępu.
2) Zakończenie pracy z Systemem Kontroli Dostępu.
3) Wyłączenie monitora.

Zakończenie pracy:

1) Zakończenie pracy programu zgodnie z instrukcją obsługi.
2) Wylogowanie z Systemu kontroli Dostępu.
3) Zablokowanie komputera i wyłączenie monitora.

ROZDZIAŁ 7

INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA SYSTEMU KONTROLI DOSTĘPU

1. Niniejsza instrukcja określa tryb postępowania w sytuacji naruszenia Systemu Kontroli Dostępu.
2. Każda osoba zatrudniona posiadająca dostęp do Systemu Kontroli Dostępu, która stwierdzi lub podejrzewa naruszenie systemu, zobowiązana jest do niezwłocznego poinformowania Administratora oraz Zastępcę Administratora Systemu Kontroli Dostępu. W przypadku ich nieobecności bezpośredniego przełożonego.
3. Wartownik WSO SOL pełniący służbę w Centrum Monitoringu jest zobowiązany do ochrony zabezpieczonego Głównego Hasła oraz weryfikacji pracownika. na podstawie listy osób upoważnionych do wykonywania pracy w Systemie Kontroli Dostępu.
4. Wartownik WSO SOL przed rozpoczęciem służby w Centrum Monitoringu dokonuje sprawdzenia stanu zabezpieczenia metalowej skrzynki w której znajduje się Główne Hasło. Następnie dokonuje wpisu w książce przebiegu służby.
5. W przypadku stwierdzenia naruszenia zabezpieczenia Głównego Hasła przez nieupoważnioną osobę, Wartownik WSO SOL niezwłocznie powiadamia o zaistniałej sytuacji Dowódcę Zmiany, który informuje o zaistniałym zdarzeniu Administratora Systemu Kontroli Dostępu lub Zastępcę Administratora Systemu Kontroli Dostępu.
6. Administrator lub jego Zastępca dokumentuje zaistniały przypadek naruszenia oraz sporządza raport, który powinien zawierać w szczególności:
   - Wskazanie osoby powiadamiającej o naruszeniu oraz innych osób zaangażowanych lub odpytanych w związku z naruszeniem,
   - Określenie czasu i miejsca naruszenia i powiadomienia,
   - Określenie okoliczności towarzyszących i rodzaju naruszenia,
   - Podjęte działania,
   - Wstępną ocenę przyczyn wystąpienia naruszenia,
   - Ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego.

Rozdział 8

POSTANOWIENIA KOŃCOWE

1. Przypadki nieuzasadnionego zaniechania obowiązku wynikających z niniejszego dokumentu, w szczególności przez osobę, która wobec naruszenia ochrony Systemu Kontroli Dostępu oraz uzasadnionego domniemania takiego naruszenia, nie podjęła działań określonych w niniejszym dokumencie, mogą być potraktowane jako ciężkie naruszenie obowiązków służbowych.
2. Wobec osoby uchylającej się od powiadomienia Administratora Systemu Kontroli Dostępu Bezpieczeństwa oraz Zastępcę Administratora Systemu kontroli Dostępu o wystąpieniu naruszenia lub zagrożenia bezpieczeństwa Systemu Kontroli Dostępu stosuje się karę dyscyplinarną.
3. Niniejsza „Polityka Bezpieczeństwa Systemu Kontroli Dostępu w Międzynarodowym Porcie Lotniczym wchodzi w życie z dniem Zarządzenia Prezesa Zarządu Górnośląskiego Towarzystwa Lotniczego S.A. w Katowicach.

Załączniki:

1) Wzór upoważnienia do Systemu kontroli Dostępu
2) Rejestr osób upoważnionych
3) Wzór raportu z naruszenia bezpieczeństwa Systemu KONTROLI DOSTĘPU
4) Adresy e-mail Administratora Systemu Kontroli Dostępu oraz Zastępcy Administratora Kontroli Dostępu.
5) Karta pracy na stanowisku: ,,Kontrola Dostępu"

Załącznik nr 1

Wzór upoważnienia do Systemu Kontroli Dostępu, nadawanego przez Administratora Systemu Kontroli Dostępu oraz Zastępcę Systemu Kontroli Dostępu.

Upoważnienie do dostępu Systemu Kontroli Dostępu

Data nadania upoważnienia: .....

Upoważniam Panią/Pana .....
(imię i nazwisko upoważnianego)

zatrudnioną/-ego na stanowisku .....
w .....
(oznaczenie jednostki organizacyjnej)

Do Systemu Kontroli Dostępu
.....
.....
(zakres upoważnienia)

Okres trwania upoważnienia:
.....

.....
(podpis i pieczęć Administratora Systemu kontroli Dostępu)

.....
(podpis i pieczęć Zastępcy Administratora Systemu kontroli Dostępu)

Osoba upoważniona do Systemu Kontroli Dostępu jest zobowiązana do:

- Zapoznania się z Instrukcją Działania Systemu Kontroli Dostępu
- Zachowania w tajemnicy danych oraz informacji o zabezpieczeniu Systemu , również po ustaniu zatrudnienia.
- Zapewnienia bezpieczeństwa przetwarzania danych osobowych w Systemie Kontroli Dostępu poprzez ich ochronę przed niepowołanym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem.

....

(podpis osoby upoważnionej) (pieczęć i podpis kierownika jednostki)

Załącznik nr 2

REJESTR OSÓB UPOWAŻNIONYCH
SYSTEM KONTROLI DOSTĘPU

REJESTR UPRAWNIEŃ -KONTROLA DOSTĘPU										
Imię	Nazwisko	Firma	Nr przepustki	Stanowisko	Okres zatrudnienia	Zakres uprawnień	Podpisał	Data dodania uprawnienia	Ważność uprawnienie	Data anulowania uprawnień

Załącznik nr 3

WZÓR RAPORTU Z NARUSZENIA BEZPIECZEŃSTWA SYSTEMU KONTROLI DOSTĘPU

Data: ..... Godzina: .....

Osoba powiadamiająca o zaistniałym zdarzeniu:

.....

(imię, nazwisko, stanowisko służbowe, identyfikator użytkownika (jeśli występuje)

Lokalizacja zdarzenia:

.....

(np. nr pokoju, nazwa pomieszczenia)

Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:

.....

Podjęte działania:

.....

.....

.....

.....

.....

6. Przyczyny wystąpienia zdarzenia:

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Postępowanie wyjaśniające:

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Podpis osoby powiadamiającej o zdarzeniu

.....

(Podpis i pieczęć Administratora Systemu kontroli Dostępu)

.....

(Podpis i pieczęć Zastępcy Administratora Systemu Kontroli Dostępu)

Załącznik nr 4

Administrator Systemu Kontroli Dostępu:
(032)3927470

Zastępca Administratora Systemu Kontroli Dostępu:
Tel kom: 660418598

Załącznik 5

KARTA PRACY NA STANOWISKU

STANOWISKO : ..... *KONTROLA DOSTĘPU*.....

DATA	CZAS PRACY		IMIĘ i NAZWISKO	WYKONYWANE CZYNNOŚCI SŁUŻBOWE	PODPIS