WYDANIE
01

PROCEDURA
P/01

POLITYKA BEZPIECZEŃSTWA INFORMACJI

OBOWIĄZUJE OD 08.01.2018

Opracował

Administrator systemów
DNIA _____

Zatwierdził

ZSK" Sp. z o.o.
Prezes
dr inż. Andrzej Poślednik
Prezes Zarządu Dyrektor Generalny
DNIA _____

KARTA ZMIAN

Lp.	Wprowadzono	Anulowano	Data zmiany	Wprowadzający zmianę
1	08.01.2018 r.			

ROZDZIELNIK

LP	Wersja/Otrzymujący procedurę	NR EGZ.	DATA OTRZYMANIA
1	Pełnomocnik ds. ZSZ	1	
2	Wersja elektroniczna		

Spis treści

1. Struktura zarządzania bezpieczeństwem i podział odpowiedzialności

1.1 Administrator Danych odpowiada za:

- Całość bezpieczeństwa informacji;
- Nadzór nad realizacją Polityki Bezpieczeństwa Informacji oraz innych dokumentów wewnętrznych związanych z ochroną informacji;
- Decydowanie o współpracy w zakresie bezpieczeństwa z innymi podmiotami;
- Wyrażanie zgody na udostępnienie stronom trzecim informacji stanowiących tajemnicę firmy; Nadawanie i odbieranie uprawnień do korzystania z danych w systemach.

1.2 Koordynacja działań w zakresie Bezpieczeństwa Informacji

Administrator Danych, Koordynator ds. Bezpieczeństwa Informacji oraz Właściciele Aktywów koordynują działania w zakresie bezpieczeństwa poprzez:

- Wskazywanie kierunków działań w zakresie bezpieczeństwa;
- Wykonywanie przeglądów Polityki Bezpieczeństwa Informacji;
- Monitorowanie istotnych zmian narażenia aktywów informacyjnych na podstawowe zagrożenia;
- Wykonywanie przeglądu i monitorowanie naruszeń bezpieczeństwa informacji;
- Spotkania na przeglądach zarządzania oraz doraźne w sytuacjach mogących mieć istotny wpływ na bezpieczeństwo informacji;
- Analizowanie istotnych zmian narażenia aktywów informacyjnych na zagrożenia; □ Dokonywanie analizy naruszeń bezpieczeństwa informacji.

1.3 Odpowiedzialność w zakresie Bezpieczeństwa informacji

Koordynator ds. Bezpieczeństwa Informacji jest odpowiedzialny za:

- Nadzór nad przestrzeganiem obowiązujących w firmie zasad ochrony informacji;
- Koordynację zapewnienia bezpieczeństwa informacji oraz związanych z nim polityk i procedur;
- Podejmowanie odpowiednich działań w przypadku wykrycia naruszeń bezpieczeństwa informacji lub prób takich naruszeń;
- Zapewnienie przetwarzania danych osobowych zgodnie z Ustawą o ochronie danych osobowych oraz innymi przepisami powszechnie obowiązującego prawa;
- Monitorowanie zmian w przepisach prawnych dotyczących sposobu zabezpieczenia danych oraz dostosowanie systemu do wymagań prawnych;
- Decydowanie o współpracy w zakresie bezpieczeństwa z innymi podmiotami;
- Przeprowadzenie w imieniu Administratora Danych szkoleń dla osób upoważnionych do korzystania z informacji objętych ochroną;
- Rozstrzyganie problemów dotyczących wątpliwości w stosowaniu dokumentacji systemu;

1.4 Odpowiedzialność w zakresie aktywów

Właściciele aktywów odpowiadają za:

- Bezpieczeństwo informacji w zakresie, nad którym sprawują nadzór;
- Przeciwdziałanie dostępowi do informacji chronionych osób niepowołanych;
- Decydowanie o współpracy w zakresie bezpieczeństwa z innymi podmiotami, w zakresie, nad którym sprawują nadzór;
- Wyrażanie zgody na udostępnienie stronom trzecim informacji chronionych należących do aktywu, którego są właścicielami;
- Podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie;
- Zapewnienie przetwarzania danych osobowych zgodnie z Ustawą o ochronie danych osobowych;
- Bieżące nadzorowanie oraz zarządzanie aktywem, jako właściciele aktywów;
- Nadzór nad poprawnością pracy systemów informatycznych oraz mechanizmów zabezpieczających dane w tych systemach;
- Nadzór nad zabezpieczeniem danych poprzez tworzenie i właściwe zabezpieczanie kopii zapasowych;
- Analizę pracy systemu informatycznego w celu wykrycia potencjalnych zagrożeń;
- Nadzór nad przeprowadzaniem w bezpieczny sposób napraw oraz konserwacji sprzętu i oprogramowania służącego do przetwarzania lub będącego nośnikiem danych;
- Utrzymywanie ochrony aktywów i zasobów, którymi dysponują;
- Wprowadzanie zabezpieczeń;
- Utrzymanie aktualnych wersji oprogramowania oraz dokumentacji eksploatacyjnej;
- Wnioskowanie o nadanie lub odebranie uprawnień oraz prowadzenie ewidencji nadanych uprawnień do dostępu do informacji chronionych;
- Prowadzenie dokumentacji systemu;
- Organizowanie szkoleń z zakresu bezpieczeństwa informacji dla osób upoważnionych do korzystania z informacji objętych ochroną;
- Przegląd i weryfikację efektywności ustanowionego systemu i informowanie podczas przeglądu o jej wynikach;
- Autoryzacja zakupów sprzętu i oprogramowania pod kątem zgodności z zasadami systemu bezpieczeństwa informacji;
- Współpracę z Koordynatorem ds. Bezpieczeństwa Informacji oraz innymi Właścicielami Aktywów w zakresie realizacji zadań dotyczących bezpieczeństwa informacji;
- Propagowanie zasad Systemu Zarządzania Bezpieczeństwem Informacji wśród pracowników w podległych im obszarach;
- Nadzorowanie realizacji założeń Polityki Bezpieczeństwa Informacji i innych dokumentów systemu bezpieczeństwa informacji w podległych obszarach.

1.5 Zakres uprawnień i odpowiedzialności Administratora

Administrator:

- Uczestniczy w opracowaniu szczególnych wymagań bezpieczeństwa i procedur bezpieczeństwa;
- Nadzoruje i kontroluje konfigurację systemu w zakresie dostępu do sieci teleinformatycznej;
- Kontroluje znajomość procedur bezpieczeństwa przez wszystkich użytkowników systemu w zakresie bezpieczeństwa teleinformatycznego;
- Prowadzi szkolenia z zakresu bezpieczeństwa teleinformatycznego;

- Prowadzi bieżącą kontrolę zabezpieczeń oraz zgodność funkcjonowania systemu ze szczególnymi wymaganiami bezpieczeństwa;
- Wdraża procedury ochrony antywirusowej, przed złośliwym oprogramowaniem oraz nieuprawnionym dostępem do zasobów systemów za pośrednictwem sieci teleinformatycznych;
- Sprawdza poprawność działania systemu oraz jego zabezpieczeń w zakresie ochrony antywirusowej, przed złośliwym oprogramowaniem oraz innymi zagrożeniami mogącymi pochodzić z sieci teleinformatycznych;
- Proponuje zmiany mające na celu zwiększenie bezpieczeństwa systemu lub sieci teleinformatycznej;
- Nadzoruje proces sporządzania kopii zapasowych danych znajdujących się w systemach teleinformatycznych.

1.6 Odpowiedzialność właścicieli procesów

Właściciele procesów odpowiadają za:

- Przestrzeganie zasad ochrony informacji przez nich samych jak i przez podległych im pracowników,
- Identyfikowanie i dokumentowanie zagrożeń zachowania bezpieczeństwa informacji,
- Definiowanie oraz realizacji działań zapobiegających zagrożeniom,
- Zapoznanie pracowników z obowiązkami związanymi z ochroną informacji na stanowiskach pracy;
- Przeprowadzenie szkoleń pracowników w zakresie przepisów prawa oraz wewnętrznych zasad dotyczących ochrony informacji;

1.7 Odpowiedzialność pracowników

Odpowiedzialność za bezpieczeństwo informacji w firmie ponoszą wszyscy pracownicy zgodnie z posiadanymi zakresami obowiązków. Każdy pracownik zobowiązany jest dbać o bezpieczeństwo powierzonych mu do przetwarzania, archiwizowania lub przechowywania informacji zgodnie z obowiązującymi przepisami wewnętrznymi, w tym m. in. stosować zasady opisane w Polityce oraz innych dokumentach wewnętrznych;

Ponadto pracownik jest zobowiązany:

- Chronić informacje podlegające ochronie przed dostępem do nich osób nieuprawnionych;
- Chronić dane przed przypadkowym lub umyślnym zniszczeniem, utratą lub modyfikacją;
- Chronić sprzęt, nośniki magnetyczne i wydruki komputerowe zawierające dane chronione;
- Utrzymywać w tajemnicy powierzone hasła, częstotliwością ich zmiany oraz szczegóły technologiczne systemów także po ustaniu zatrudnienia w firmie;
- Stosować się do szczegółowych zaleceń w zakresie ochrony antywirusowej, a także do innych zaleceń wynikających z Systemu Zarządzania Bezpieczeństwem Informacji;

- Powiadomić Pełnomocnika ds. ZSZ, Właściciela Aktywu lub bezpośredniego przełożonego o ujawnieniu lub możliwości ujawnienia informacji chronionych osobom nieupoważnionym, o nieautoryzowanej zmianie informacji chronionych lub możliwości wprowadzenia nieautoryzowanych zmian, o zniszczeniu lub możliwości zniszczenia informacji chronionych; o zablokowaniu lub możliwości zablokowania pracy systemu informatycznego przetwarzającego informacje

1.8 Bezpieczeństwo informacji w zarządzaniu projektami

Projekty realizowane w ZSK dzielą się na projekty np. inwestycyjne i projekty Unijne.
Zasady bezpieczeństwa informacji w projektach uregulowane są w instrukcjach, umowach i wytycznych do tych projektów. Ryzyko w BI oszacowano na wczesnym etapie projektu w celu identyfikacji niezbędnych zabezpieczeń. Zdefiniowano i przypisano obowiązki w zakresie BI do właściwych ról określonych w dokumentach zarządzania projektami.

Zabrania się pod rygorem odpowiedzialności służbowej i karnej: Ujawniania informacji chronionych (w tym dane osobowe), kopiowania bazy danych lub ich części poza kopiami przewidzianymi w dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji, jak np. kopie bezpieczeństwa, uszkadzania lub niszczenia sprzętu lub informacji za wyjątkiem sytuacji wycofywania z użycia sprzętu lub nośników zgodnie z odpowiednimi procedurami, zabrania się przetwarzania informacji chronionych w sposób mogący narażać na utratę bezpieczeństwa tych danych przez naruszenie poufności, integralności lub dostępności, instalowania oprogramowania niezwiązanego z wykonywaniem obowiązków służbowych na wszelkich urządzeniach powierzonych pracownikowi, dokonywania zmian ustawień, konfiguracji systemów, komputerów, telefonów komórkowych przez użytkowników.

2. Współpraca

2.1 Zasady współpracy z osobami trzecimi

Goście oraz inne osoby przebywające na terenie Spółki niebędące pracownikami są zobowiązane do przestrzegania następujących zasad:

- Reguł bhp;
- Reguł bezpieczeństwa przeciwpożarowego; □ Wpisania się w księdze gości w sekretariacie.

Każda osoba niebędąca pracownikiem Spółki, która wykonuje prace zlecone, z którymi wiąże się dostęp do informacji chronionych przez Spółkę zobligowana jest do podpisania oświadczenia o zachowaniu poufności.

Osoby niezatrudnione w Spółce mogą otrzymać od Koordynatora ds. Bezpieczeństwa Informacji lub Właściciela Aktywu prawo dostępu fizycznego i/lub logicznego do informacji, jeżeli:

- Jest to niezbędne do realizacji obowiązków Spółki wobec Klientów lub do bieżącego funkcjonowania Spółki;
- Dają one gwarancję zachowania poufności;
- Podpisały ze Spółką oświadczenie o zachowaniu tajemnicy przedsiębiorstwa lub umowę określającą odpowiedzialność za naruszenie poufności.

Osobom tym powinno zostać odebrane prawo dostępu po wygaśnięciu przyczyny udzielenia w/w dostępu, np. po wykonaniu zleconej pracy.

2.2 Zasady współpracy z innymi podmiotami

Współpraca Spółki z innymi podmiotami oparta jest na umowach. Zawierając te umowy Spółka ma na względzie, aby obejmowały one deklarację o zachowaniu bezpieczeństwa informacji i przestrzegania zasad systemu bezpieczeństwa informacji przyjętych w Spółce.

2.3 Zakończenie zatrudnienia

Wraz z zakończeniem zatrudnienia pracownik rozlicza się z posiadanych aktywów. Administrator/właściciel aktywów jest odpowiedzialny za aktualizację uprawnień dostępu i aktywów dla danego pracownika, a bezpośredni przełożony odpowiada za kontrolę rozliczenia pracownika z posiadanych aktywów.

3. Polityka kontroli dostępu

3.1 Kontrola dostępu do pomieszczeń biurowych

Kontrola dostępu do pomieszczeń pracowników jest realizowana przy pomocy kart dostępu lub kluczy wydawanych przez pracowników sekretariatu.

Każdy pracownik odpowiada za swoją kartę dostępu. W przypadku zagubienia karty dostępu należy niezwłocznie poinformować o tym fakcie przełożonego i Administratora (zgłoszenie zagubienia traktowane będzie, jako incydent). System kart dostępu jest zarządzany przez Administratora. Dla pomieszczeń wyposażonych w system kart dostępu zabrania się korzystania z kluczy, które powinny być przechowywane w sekretariacie i mogą być użyte, po zgłoszeniu awarii systemu dostępu lub innych sytuacji uniemożliwiających uzyskanie dostępu do pomieszczeń przy pomocy karty.

3.2 Kontrola dostępu do pomieszczeń wrażliwych

Na terenie firmy znajdują się obszary wydzielone z uwagi na pomieszczenia chronione w szczególny sposób. Dostęp ten jest kontrolowany przez kartę dostępu oraz klucz. Dostęp osób nieupoważnionych w tym obszarze odbywa się tylko w obecności upoważnionych pracowników.

3.3 Zasady nadawania uprawnień użytkowników

Udzielanie, zmiana i odbiór uprawnień użytkowników jest wykonywane przez Administratora na wniosek Prezesa. W przypadku rejestrowania konta nowego użytkownika w systemie, identyfikator i hasło początkowe musi mu być przekazane w sposób uniemożliwiający użycie tych informacji przez osoby nieuprawnione. Nowy użytkownik jest zobowiązany do zmiany hasła już przy pierwszym zalogowaniu do systemu.

3.4 Zasada korzystania z usług sieciowych

Do systemu produkcyjnego sieci naszej firmy mają dostęp wyłącznie komputery podłączone do usługi katalogowej na podstawie identyfikatorów sprzętowych oraz posiadające certyfikat nadany przez wewnętrzne centrum certyfikatów. Urządzenia niespełniające tych warunków mogą jedynie korzystać z odseparowanej sieci przeznaczonej dla gości.

3.5 Kontrola dostępu do systemów i aplikacji

Dostęp do systemów i aplikacji odbywa się w oparciu o unikatowy identyfikator i hasło użytkownika. Odpowiednia polityka bezpieczeństwa wymusza wysoki poziom złożoności haseł użytkowników i ich okresową zmianę. Użytkownicy przydzielani są do odpowiednich grup bezpieczeństwa regulujących uprawnienia do poszczególnych zasobów. Aplikacje i systemy o znaczeniu krytycznym posiadają dodatkowe unikatowe identyfikatory i hasła. System monitoruje zdarzenia dostępu do zasobów i rejestruje je w odpowiednich dziennikach.
W systemie regularnie dokonuje się przeglądu uprawnień i ograniczania praw użytkowników do poziomu niezbędnego do realizacji zadań wynikających z powierzonych obowiązków.

Użycie uprzywilejowanych programów narzędziowych zostało ograniczony wyłącznie do stosowania przez Administratorów.
Utworzone jest repozytorium aplikacji dopuszczonych do pracy przez pracowników ZSK. Za aktualizację tego repozytorium odpowiada Administrator.

4. Zasady wymiany informacji

Zobowiązuje się pracowników do niedziałania na szkodę organizacji. Zabrania się pozostawiania krytycznych lub wrażliwych informacji przy urządzeniach drukujących np. kopiarkach, drukarkach, do których ma dostęp nieautoryzowany personel. Należy pamiętać o szczególnych środkach ostrożności podczas rozmów telefonicznych unikając podsłuchania lub przechwycenia informacji przez: osoby znajdujące się w bezpośrednim sąsiedztwie, użycie podsłuchu, osób znajdujących się po stronie odbiorcy.

5. Zarządzanie dostępem użytkowników

5.1 Rejestrowanie i wyrejestrowywanie użytkowników

Na wniosek prezesa zarządu firmy administrator dokonuje rejestracji lub wyrejestrowania użytkownika w systemie teleinformatycznym. Nowemu użytkownikowi nadawany jest unikatowy identyfikator w oparciu o imię i nazwisko oraz jednorazowe hasło zgodne z polityką haseł. System wymusza na użytkowniku po pierwszym zalogowaniu zmianę hasła.
W przypadku wyrejestrowywania użytkownika z systemu, administrator dokonuje blokady konta użytkownika. Następnie przeprowadza analizę danych indywidualnych użytkownika i w uzasadnionych przypadkach wykonuje ich kopię bezpieczeństwa. Po formalnym rozwiązaniu umowy i rozliczeniu użytkownika jest on usuwany z systemu usługi katalogowej wraz ze skrzynką pocztową. Następnie użytkownik zostaje usunięty z systemów krytycznych posiadających dodatkowe własne identyfikatory i hasła. Certyfikat użytkownika zostaje odwołany.

5.2 Przydzielanie dostępu użytkownikom

Na wniosek Prezesa zarządu Administrator przypisuje lub usuwa użytkownika do/z określonych grup zabezpieczeń nadając lub odbierając mu uprawnienia dostępu do dodatkowych zasobów. Nadanie lub odebranie praw do systemów krytycznych wymaga od administratora utworzenia lub usunięcia unikatowego identyfikatora i hasła w tychże systemach.

5.3 Zarządzanie prawami uprzywilejowanego dostępu

Prawa uprzywilejowanego dostępu posiada:

- administrator systemu
- specjalna grupa zabezpieczeń obejmująca pracowników wsparcia technicznego (administrator i jego zastępca).
- konta konieczne do działania uprzywilejowanych usług systemu teleinformatycznego
- unikatowe konta użytkowników i hasła w obrębie urządzeń tworzących infrastrukturę sieciową

Konta te są wyraźnie oznaczone w systemie teleinformatycznym. Ich identyfikatory i hasła utrzymywane są na bieżąco w dokumentacji dostępnej pracownikom wsparcia technicznego.

5.4 Zarządzanie poufnymi informacjami uwierzytelniającymi użytkowników

System automatycznie blokuje konta w przypadku nieudanych prób logowania lub wygaśnięcia hasła. System wymusza blokadę stacji roboczej w przypadku braku aktywności użytkownika w przeciągu 15 minut. Administrator nie zna haseł zwykłych użytkowników systemu, może jedynie dokonać resetowania hasła w przypadku jego utraty/zapomnienia przez użytkownika.

6. Zasady korzystania z systemów informatycznych

Przed przystąpieniem do pracy w systemie informatycznym użytkownik zobowiązany jest sprawdzić urządzenie komputerowe i stanowisko pracy ze zwróceniem uwagi, czy nie zaszły okoliczności wskazujące na naruszenie bezpieczeństwa informacji. W przypadku naruszenia bezpieczeństwa informacji użytkownik postępuje zgodnie z polityką zarządzania incydentami.

Użytkownik rozpoczyna pracę w systemie informatycznym od uwierzytelnienia się za pomocą swojego unikatowego identyfikatora i hasła. Niedopuszczalne jest uwierzytelnianie się na hasło i identyfikator innego użytkownika lub praca w systemie informatycznym na koncie innego użytkownika. Zakończenie pracy użytkownika w systemie następuje po wylogowaniu się z systemu. Po zakończeniu pracy użytkownik zabezpiecza swoje stanowisko pracy, w szczególności nośniki wymienne, dokumenty i wydruki zawierające ważne dane, przed dostępem osób nieupoważnionych zgodnie z polityką czystego biurka i ekranu.

6.1 Oprogramowanie

Oprogramowanie instalowane jest na komputerach użytkowników przez Administratora lub w wyjątkowych sytuacjach przez użytkowników każdorazowo po uzyskaniu zgody Administratora. Oprogramowanie może być wykorzystywane wyłącznie do użytku służbowego. Administrator przeprowadza wyrywkowo niezapowiedziane kontrole oprogramowania zainstalowanego na stacjach roboczych. Zakłada się przeprowadzenie kontroli każdej stacji roboczej przynajmniej raz w roku.

6.2 Poczta elektroniczna

Użytkownik korzystający z konta pocztowego może je wykorzystywać wyłącznie do użytku służbowego. Wszelka wpływająca korespondencja prywatna musi zostać natychmiast usunięta.

6.3 Internet

Wszyscy użytkownicy komputerów, telefonów komórkowych mają możliwość korzystania z internetu. Należy jednak pamiętać, że powinno się korzystać z internetu tylko i wyłącznie do użytku służbowego. Możliwe jest blokowanie treści zawartych w internecie, niezwiązanych z wykonywaną pracą lub obniżającą wydajność dostępu do internetu. Zapora centralna sieci produkcyjnej rejestruje dostęp do zasobów internetu i blokuje dostęp do informacji potencjalnie niebezpiecznych lub uznanych za zawierające treści niepożądane.

7. Polityka stosowania urządzeń mobilnych i telepraca

Użytkownik wyposażony w komputer przenośny ma możliwość pracy zdalnej i korzystania z zasobów firmowych pod warunkiem nadania odpowiednich uprawnień w systemie. Praca zdalna na zasobach firmowych jest możliwa tylko za pośrednictwem szyfrowanego tunelu VPN.

Dodatkowo każdy użytkownik pod warunkiem nadania odpowiednich uprawnień w systemie ma możliwość zdalnego korzystania z firmowej poczty elektronicznej za pośrednictwem swojego komputera przenośnego lub dowolnego innego urządzenia przy użyciu przeglądarki internetowej.

Blokada dostępu zdalnego musi być zgłoszona przez Dyrektora Działu pisemnie lub przy użyciu poczty elektronicznej. Praca na odległość stron zewnętrznych wymagająca zdalnego dostępu do aktywów firmy uregulowana jest odpowiednimi umowami i instrukcjami eksploatacyjnymi systemów pracujących w trybie zdalnego dostępu z zastosowaniem stosownych zabezpieczeń.

8. Okresowa kontrola praw dostępu

Administrator systemu nie rzadziej niż raz w miesiącu przeprowadza kontrolę aktualności i poprawności listy zarejestrowanych w systemie użytkowników i przypisanych im praw dostępu. Przegląd odbywa się poprzez porównanie faktycznie istniejących kont z zatwierdzonym wykazem użytkowników.

9. Bezpieczeństwo komunikacji

9.1 Zarządzanie bezpieczeństwem sieci

Sieć teleinformatyczna firmy została podzielona na logiczne segmenty ze względu na ich przeznaczenie. Przepływ informacji pomiędzy segmentami sieciami ograniczony jest do minimum niezbędnego do funkcjonowania urządzeń i systemów i odbywa się w centralnej zaporze. Zapora rejestruje ruch sieciowy i zgłasza na bieżąco próby nieautoryzowanego dostępu.
Sieć podzielona została na następujące segmenty:
- sieć zarządzająca
- sieć backend systemów serwerowych i pamięci masowych
- sieć produkcyjna
- sieć dla firmy zewnętrznej dla której ZSK świadczy usługi informatyczne.
- sieć laboratoryjna wraz z siecią dla gości

9.2 Przesyłanie informacji

Użytkownik podczas pracy w systemie informatycznym sprawdza na bieżąco poprawność działania systemu i informuje o wszelkich nieprawidłowościach. W przypadku naruszenia bezpieczeństwa informacji użytkownik postępuje zgodnie z polityką zarządzania incydentami.

Administrator wykonuje okresowe przeglądy zasobów wykorzystywanych przez nadzorowane aplikacje oraz dokonuje aktualizacji oprogramowania lub wysyłają komunikaty o obowiązku przeprowadzenia aktualizacji. W ramach przeglądu sprawdzane są logi systemowe, logi baz danych, wykorzystanie pojemności dysków i innych zasobów sprzętowych. W przypadkach przekroczenia optymalnych parametrów podejmuje działania zwiększające przydział zasobów do aplikacji. Wszystkie urządzenia, istotne dla funkcjonowania infrastruktury są zabezpieczone przed awarią zasilania za pomocą urządzeń UPS, pozwalających na bezpieczne zamknięcie systemów oraz ich ponowne uruchomienie po powrocie zasilania. Ich działanie jest monitorowane zdalnie.

9.3 Konta pocztowe

Konta pocztowe przyznawane są zgodnie z polityką kontroli dostępu do systemów i sieci. W przestrzeni adresowej firmy występują również adresy grupowe. Przynależność użytkownika do adresu grupowego wynika z wykonywania powierzonych obowiązków i struktury organizacyjnej.

9.4 Zasady bezpieczeństwa informacji przy korzystaniu z poczty elektronicznej

Bezpieczeństwo informacji przy korzystaniu z poczty elektronicznej zależy w znacznej mierze od ustawień programu obsługującego pocztę oraz od działania samego użytkownika. Każdy użytkownik, który uzyskał uprawnienia do korzystania z poczty elektronicznej jest zobowiązany przynajmniej jeden raz w ciągu dnia odczytać dostarczoną pocztę. Dotyczy to dni jego obecności w pracy. W przypadku nieobecności w pracy powinien podjąć działania, żeby zminimalizować negatywny wpływ nieobecności na wymianę informacji (poinformowanie ważnych nadawców, odpowiednie ustawienia automatyki programu pocztowego). Należy pamiętać o tym, że informacja przesyłana pocztą elektroniczną jest łatwa do odczytania przez osoby, dla których nie została przeznaczona. W przypadku istnienia potrzeby ochrony przesyłanej informacji przed nieuprawnionym dostępem, należy stosować odpowiednie do sytuacji środki bezpieczeństwa (hasła, szyfrowanie).

Przy przesyłaniu załączników należy uwzględnić fakt, że skrzynki pocztowe mają ograniczoną pojemność i dostosować do niej rozmiary przesyłek (kompresja, podział przesyłki na części) oraz czas przechowywania informacji (czyszczenie skrzynek, archiwizacja).

Ze względów wydajnościowych Administrator ustanawia ograniczenia, co do wielkości skrzynek pocztowych oraz dopuszczalnego rozmiaru przesyłanej poczty

Wysłanie wiadomości pocztą elektroniczną nie gwarantuje, że dotrze ona do adresata i zostanie przez niego przeczytana. W przypadku, gdy dostarczenie jej jest istotne z biznesowego punktu widzenia, należy zastosować wbudowane w system pocztowy mechanizmy potwierdzenia odbioru i przeczytania przesyłki lub zażądać potwierdzenia tego faktu przez adresata.

Ze względu na to, że nadawca poczty może stosunkowo łatwo podszyć się pod kogoś innego (jeżeli poczta nie jest podpisana odpowiednim podpisem elektronicznym), należy przy przesyłkach budzących wątpliwości a istotnych biznesowo potwierdzić inną drogą tożsamość nadawcy.

Przy kierowaniu wiadomości do kilku odbiorców należy się upewnić, czy życzą oni sobie, by ich adresy e-mail były wzajemnie udostępniane, i na tej podstawie wybrać odpowiedni sposób adresowania: do (do), do wiadomości – (dw), ukryta kopia do (udw). Stosując ostatni wariant unikamy ujawniania adresów e-mail poszczególnym adresatom jednej wiadomości.

9.5 Ochrona systemowa poczty przychodzącej

Poczta przychodząca jest kontrolowana na serwerze komercyjnymi środkami antywirusowymi i antyspamowymi.

9.6 Archiwizowanie poczty

Skrzynki pocztowe użytkowników przechowywane są na serwerze i objęte ogólną polityką backupów w firmie. Za zabezpieczenie skrzynek przechowywanych lokalnie oraz archiwum poczty zapisanego lokalnie odpowiadają użytkownicy.

9.7 Instalacja oprogramowania w systemach produkcyjnych

Za aktualizację oprogramowania układowego, aplikacji i systemów operacyjnych serwerów oraz urządzeń infrastruktury odpowiada administrator. Każdorazowo wykonywana jest odpowiednia kopia zapasowa umożliwiająca przywrócenie stanu systemu/aplikacji z przed operacji aktualizacji w przypadku wystąpienia niepożądanych efektów. Systemy operacyjne, aplikacje oraz szczepionki antywirusowe stacji roboczych o ile to możliwe są realizowane w sposób automatyczny za pośrednictwem odpowiednich usług.
Do systemów produkcyjnych dopuszcza się tylko produkty będące przetestowanymi wersjami finalnymi posiadającymi udokumentowane pochodzenie oraz odpowiednią dokumentację z określonymi wymaganiami technicznymi.

10. Zarządzanie wymiennymi nośnikami

Wymienne nośniki informacji muszą być opisane w sposób umożliwiający identyfikację zawartości nośnika, jeżeli posiadają informacje chronione, nie mogą one być wynoszone poza siedzibą firmy bez zgody przełożonego. Zaleca się wymazanie poprzedniej zawartości wszelkich nośników wielokrotnego użytku, które mają być wyniesione z firmy, o ile zawartość ta nie będzie już potrzebna.

Wymienne nośniki informacji muszą być transportowane i przechowywane w sposób zabezpieczający przed dostępem osób nieuprawnionych oraz utratą nośnika bądź informacji na nim zapisanej. Korzystanie z wymiennych nośników informacji powinno się odbywać z uwzględnieniem ochrony ich zawartości przed złośliwym lub szkodliwym oprogramowaniem. Jako zasadę przyjmuje się trwałe niszczenie nośników zawierających informacje chronione tak, aby nie był możliwy odczyt z nich jakichkolwiek danych, jeżeli używanie ich nie jest już uzasadnione lub zostały one uszkodzone, np.: przez fizyczne zniszczenie nośnika. W przypadku przekazywania innemu pracownikowi komputerów lub dysków zawierających dane chronione, zawarte na przekazywanych nośnikach, są nieodwracalnie usuwane w sposób uniemożliwiający ich ponowne odtworzenie lub odczytanie, np. poprzez wykorzystania specjalistycznego oprogramowania do wielokrotnego nadpisywania danych.

11. Polityka postępowania z informacjami

Informacja (w postaci aktywów informacyjnych) jest sklasyfikowana zgodnie ze stawianymi jej wymaganiami w zakresie ochrony. Szczególnie traktowane są informacje powierzone przez Klientów. Określone zostały zasady postępowania z danymi grupami informacji oraz grupy pracowników posiadające do nich dostęp.

Zasady postępowania dotyczące bezpieczeństwa informacji odnoszą się do informacji chronionych. Informacje chronione to wszystkie aktywa informacyjne wykazane w analizie ryzyka. Osobami upoważnionymi do dostępu do informacji chronionych są pracownicy firmy, dla których dana informacja jest niezbędna do wykonywania obowiązków służbowych oraz osoby spoza firmy, którym interes firmy wymaga udostępnienia danej informacji. Upoważnieni pracownicy posiadają indywidualne konta w systemach informatycznych, ustalony dostęp do poszczególnych pomieszczeń i tym samym dostęp do informacji. Każdy użytkownik informacji chronionej ma obowiązek postępowania z nią zgodnie z poniższymi zasadami:

11.1 Zasada poufności informacji

Nieudostępnianie informacji osobom nieupoważnionym (zarówno pracownikom firmy jak i osobom trzecim), korzystanie z informacji w taki sposób, aby udaremnić dostęp do niej osób nieupoważnionych, odpowiednia ochrona informacji podczas jej przechowywania i przesyłania.

11.2 Zasada integralności informacji

Odpowiednie aktualizowanie informacji, która tego wymaga, przetwarzanie informacji tylko zgodnie z odpowiednimi dla niej politykami i zasadami,

11.3 Zasada dostępności informacji

Przechowywanie i dystrybucja informacji w taki sposób, aby była dostępna dla osób upoważnionych zawsze, gdy jest potrzebna (ustalone miejsca przechowywania, rejestracja wypożyczeń, okresowe wykonywanie, przechowywanie i sprawdzanie kopii zapasowych informacji zgodnie z zasadami tworzenia kopii).

12. Klasyfikacja informacji

12.1 Informacje powszechne

Informacja powszechna – powszechnie mówiona, taka, która może przysporzyć firmie korzyści. Pracownicy mogą o tych informacjach mówić swobodnie. Jeżeli informacja nie zostanie zakwalifikowana, jako powszechna to należy ją traktować, jako informacja zastrzeżoną lub jako tajemnica przedsiębiorstwa.

12.2 Informacje zastrzeżone

Informacje warunkowo dopuszczone do ujawnienia, przekazywane w ograniczonym zakresie, mogą zostać przekazane w sytuacjach specjalnych. Np. informacje ujawnione podczas rozmów z dostawcami.

12.3 Tajemnica przedsiębiorstwa

Przez tajemnicę przedsiębiorstwa rozumie się nieujawnione do wiadomości publicznej, mówione oraz pisane informacje techniczne, technologiczne, handlowe, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, co do których przedsiębiorca podjął niezbędne działania w celu zachowania ich poufności. Poniższa przykładowa klasyfikacja informacji została przeprowadzona na podstawie wykazu aktywów informacyjnych, uwzględnionych w analizie ryzyka. Istotność pozostałych informacji, które nie zostały uwzględnione w poniższym zestawieniu, określa Dyrektor Działu lub Koordynator ds. Bezpieczeństwa Informacji.

W celu zapobiegania nieautoryzowanemu dostępowi oraz naruszeniu bezpieczeństwa lub kradzieży informacji i środków jej przetwarzania wprowadza się politykę czystego biurka i czystego ekranu.

13. Polityka czystego biurka

Ważne dokumenty i nośniki danych nie powinny pozostać niezabezpieczone w czasie nawet chwilowej nieobecności w pokoju. Pokój należy zamknąć. Po zakończeniu pracy ważne dokumenty i komputerowe nośniki z danymi powinny być przechowywane w szafach, a pokoje zamknięte. Wyjątek stanowią specjalnie chronione pomieszczenia technologiczne, w których instrukcja przetwarzania przewiduje inny sposób

postępowania. Szczególną uwagę należy zwrócić na drukarki sieciowe i kserokopiarki dostępne dla większej liczby pracowników. Pracownicy powinni odbierać dokumenty natychmiast po wykonaniu przez urządzenie zleconego zadania. Nie powinny one pozostawać dostępne ani dla obcych osób ani dla pracowników nieposiadających stosownych uprawnień.

14. Polityka czystego ekranu

Zasada „czystego ekranu" odnosi się do serwerów, stacji roboczych oraz urządzeń przenośnych np. laptopów, telefonów komórkowych. Każdorazowe odejście od stanowiska pracy powinno zostać poprzedzone wylogowaniem się lub zablokowaniem systemu. Po zakończeniu pracy należy zamknąć aktywne aplikacje oraz wylogować się z urządzeń. W związku z użytkowaniem komputerów stacjonarnych, przenośnych, telefonów komórkowych: wprowadza się obowiązek korzystania tylko z przypisanych danemu pracownikowi urządzeń, a jeżeli nie jest to możliwe, korzystanie z innych urządzeń, ale zawsze z własnym identyfikatorem i hasłem, zabrania się korzystania z aplikacji i systemów nie pod swoim loginem i hasłem, opuszczenia stanowiska pracy, bez uprzedniego wylogowania się lub zablokowania systemu. Pracownicy wprowadzający informacje do systemów informatycznych powinni dokonać sprawdzenia poprawności wprowadzanych danych, dane chronione powinny być przechowywane w miejscach do tego przeznaczonych.
Zabrania się przechowywania danych osobowych na nośnikach wymiennych, urządzenia będące własnością firmy są przypisane konkretnemu pracownikowi, osoba przypisana do urządzenia mobilnego odpowiada za jego bezpieczeństwo (kradzież, utrata lub ujawnienie danych), zabrania się pracownikom firmy korzystania ze środków mobilnych, a w szczególności z komputerów przenośnych w celach niezwiązanych stricte z interesem firmy, zaleca się zachowanie szczególnej ostrożności podczas używania urządzeń mobilnych poza siedzibą firmy, a zwłaszcza w miejscach publicznych. Zabrania się podłączania urządzeń do niezabezpieczonych sieci bezprzewodowych. Urządzenia przetwarzające dane nie powinny być pozostawiane w miejscach publicznych oraz w samochodzie bez nadzoru, pracownik odpowiada za nieautoryzowany dostęp osób nieupoważnionych do danych zawartych w swoim urządzeniu mobilnym, w razie zagubienia lub kradzieży komputera przenośnego użytkownik zobowiązany jest do niezwłocznego działania zgodnie z polityką zarządzania incydentami.

15. Relacje z dostawcami

15.1 Bezpieczeństwo informacji w relacjach z dostawcami

Każdorazowa współpraca z dostawcami zewnętrznymi wymaga utworzenia i podpisania przed przystąpieniem do prac umowy: - regulującej zasady współpracy,
- ustanawiającej osoby odpowiedzialne z obu stron za współpracę, biorących udział w realizacji
- określającej sposób i zakres dostępu oraz poziom uprawnień do systemu firmy
- określającej wymagania techniczne i funkcjonalne stawiane usłudze lub produktowi
- określającej wymagania zgodności z przepisami prawa oraz niniejszą polityką
- określającej harmonogramu prac
- określającej metody/sposobu testowania produktu lub usługi w sposób nie powodujący wpływu na istniejące środowisko produkcyjne
- określającej sposób zabezpieczenia systemu, umożliwiający cofnięcie wprowadzonych zmian w przypadku wystąpienia niepożądanych efektów.
- określającej odbiór końcowy produktu lub usługi wraz z dokumentacją

Dostęp odbywa się przy pomocy unikatowego identyfikatora i hasła umożliwiając rejestrowanie i monitorowanie zmian wprowadzanych przez zewnętrznego dostawcę.

15.2 Zarządzanie usługami świadczonymi przez dostawców

Usługi świadczone przez dostawców podlegają bieżącemu monitoringowi. Powstałe incydenty są natychmiast zgłaszane za pośrednictwem osób odpowiedzialnych i dokumentowane minimum w formie elektronicznej (email). Osoba odpowiedzialna ma obowiązek śledzenia incydentu do momentu pozytywnego usunięcia przyczyny i skutku wystąpienia zdarzenia. W przypadkach szczególnych należy udokumentować sytuację w postaci odpowiedniego wpisu na stronie bazy wiedzy technicznej, w celu umożliwienia szybszej reakcji w przypadku ponownego wystąpienia podobnego zdarzenia.

16. Polityka zarządzania incydentami

Zdarzenie – jest to określony stan systemu, który wskazuje na możliwe naruszenie polityki bezpieczeństwa informacji, błąd zabezpieczenia lub nieznana dotychczas sytuacja, która może być związana z bezpieczeństwem.

Incydent – jest to pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji. W firmie przyjmuje się następujące zakresy rejestrowania incydentów: naruszenie polityki bezpieczeństwa informacji w firmie: informacji dotyczących firmy, informacji dotyczących Klientów, naruszenie obowiązujących polityk i zasad, wykryte próby lub faktyczne: włamania, napaści, kradzieże, włamania do systemu IT, interwencje ochrony, sytuacje pożarowe, załączenia systemów alarmowych, awarie: systemów firmy, maszyn niszczących, fakty niedostatecznych umiejętności użytkowników, przekroczenia uprawnień, niedopełnienia obowiązków, zaniedbań, fakty wydostania się nośników informacji lub pochodzących od nich informacji do miejsc niepożądanych. O ile to możliwe, stwierdzający incydent niezwłocznie podejmuje działania mające na celu nie dopuszczenie lub usunięcie skutków naruszenia polityki bezpieczeństwa w firmie.

Incydent krytyczny oznacza zdarzenie powstałe na skutek działania z premedytacją

Incydent ważny oznacza zdarzenie powstałe w skutek nie umyślny.

Stwierdzenie incydentu zgłaszane jest pocztą elektroniczną poprzez pracowników naszej firmy na adres sbsadmins@zsk.pl.

W przypadku braku dostępu do poczty elektronicznej incydent może zostać zgłoszony telefonicznie do Administratora lub Dyrektora/Kierownika Działu. Zgłaszane incydenty rejestrowane są przez Administratora. Rejestr jest należycie chroniony przed dostępem osób niepowołanych. Zarejestrowane incydenty stanowią podstawę do oceny skuteczności zabezpieczeń i omawiane są na przeglądzie systemu.

Odnotowanie incydentu zawiera: Datę i godzinę wystąpienia, miejsce wystąpienia incydentu, opis incydentu, osoby związane z incydentem, opis działań po incydencie.

16.1 Postępowanie w przypadku zaistnienia zdarzenia o określonym poziomie zagrożenia:

Krytyczny – w przypadku wystąpienia incydentu kwalifikującego się do poziomu „Krytyczny" wyciągane są konsekwencje służbowe lub prawne w stosunku do osób związanych z incydentem. Wzywane są odpowiednie służby: policja, straż miejska lub straż pożarna.

Ważny – w przypadku wystąpienia incydentu kwalifikującego się do poziomu „Ważny" Pełnomocnik ds. ZSZ w stosunku do osób odpowiedzialnych za incydent dokonuje pouczenia lub organizuje spotkanie w celu wyjaśnienia przyczyn zajścia incydentu.

17. Analiza incydentu i raportowanie

Obsługa incydentu kwalifikującego się, jako „Krytyczny" powinna zakończyć się zainicjowaniem działań zawierających następujące informacje:

- Przyczyna i okoliczności zaistnienia incydentu,
- Osoby odpowiedzialne za obsługę incydentu,
- Przebieg zdarzenia i podjęte działania,
- Efekt przeprowadzonych działań,
- Wpływ na bezpieczeństwo przetwarzanych informacji, □ Sprawcy zdarzenia i sankcje.

Obsługa zdarzenia kwalifikującego się do poziomu „Ważny" powinna zakończyć się:

- Analizą przyczyn oraz okoliczności zaistnienia incydentu oraz częstotliwości jego występowania,
- Jeżeli częstotliwość występowania jest duża, wówczas należy postępować jak z incydentem zaklasyfikowanym, jako „Krytyczny".

18 . Rejestrowanie zdarzeń i monitorowanie

Na serwerach oraz stacjach roboczych dostępny jest dziennik systemu Windows (aplikacje, zabezpieczania, ustawienia, system), dziennik aplikacji i usług. Lub inne oprogramowanie, które monitoruje prace komputerów, użytkowników, które zbiera informację o zdarzeniach.

Dostęp do informacji w zakresie logów systemowych, aplikacji ograniczony jest do Administratorów.

Na serwerach dostępny jest dziennik systemu Windows (aplikacje, zabezpieczania, ustawienia, system) . lub inne oprogramowanie.

Wszystkie zegary w komputerach podłączonych do sieci lokalnej (domeny) w ZSK pobierają informację o czasie z serwera.

19. Zgodność

Dla zapewnienia zgodnego z prawem działania firmy realizowane są następujące przedsięwzięcia:

a) opracowany został rejestr wymagań prawnych dotyczących funkcjonowania firmy,
b) informacje o aktualnym stanie prawnym w dziedzinach dotyczących działania firmy są na bieżąco przeglądane i aktualizowany jest rejestr
c) zgodność z prawem działań i wyrobów firmy jest sprawdzana:
   □ przez Klientów – odbiory wyrobów,

- przez audytorów wewnętrznych – audyty wewnętrzne, przez jednostki niezależne – coroczne badania sprawozdania finansowego, wewnętrzne i zewnętrzne audyty systemów zarządzania.

20. Polityka bezpieczeństwa w procesach rozwoju i wsparcia

20.1 Polityka bezpieczeństwa prac rozwojowych

- Za bezpieczeństwo prac rozwojowych w danym projekcie odpowiada jego właściciel, zgodnie z zapisami w CRM

- Całość dokumentacji danego projektu przechowywana jest w dedykowanym folderze w aplikacji CRM

20.2 Procedury kontroli zmian w systemach

- Właściciel projektu odpowiada za kontrolę zmian dokonywanych w plikach projektu i nadzór nad nimi.

- Nadzór nad zmianami w projekcie prowadzi również Dyrektor działu, do którego przypisany jest właściciel projektu.

20.3 Przegląd techniczny aplikacji po zmianach w platformie produkcyjnej

- Harmonogram realizacji projektu określa fazy projektu w tym przeglądy techniczne po wprowadzeniu zmian.

20.4 Zasady projektowania bezpiecznych systemów

- Wszystkie projektowane systemy powinny spełniać wymagania obowiązujących ustaw, norm i dostępnej wiedzy technicznej.

- Bezpieczeństwo projektów powinno być weryfikowane wielostopniowo – zarówno automatycznie za pomocą dedykowanego oprogramowania jak i poprzez wyznaczone osoby.

20.5 Bezpieczne środowisko rozwojowe

- Za bezpieczeństwo środowiska rozwojowego odpowiada Administrator Systemów.

20.6 Prace rozwojowe zlecane podmiotom zewnętrznym

- Prace rozwojowe zlecane podmiotom zewnętrznym realizowane są na podstawie indywidualnych umów pomiędzy przedsiębiorstwem a podmiotami zewnętrznymi.

- Za poprawną realizację powyższych prac odpowiada właściciel projektu.

- Nadzór nad pracami rozwojowymi zlecanymi na zewnątrz sprawuje dyrektor działu zamawiającego.

20.7 Testowanie bezpieczeństwa systemów

- Środowisko testowe do wdrażania zmian w bezpieczeństwach systemów zapewnia Administrator Danych

- Algorytm do testowania bezpieczeństwa systemów opracowuje właściciel projektu a nadzoruje dyrektor danego działu.

20.8 Testy akceptacyjne systemów

- Za prowadzenie testów akceptacyjnych systemów odpowiada właściciel danego projektu. Przeprowadzane są w oparciu o obowiązujące normy, własną wiedzę i doświadczenie oraz wytyczne zamawiającego.

- Nadzór nad testami akceptacyjnymi systemów sprawuje Dyrektor danego działu.

20.9 Ochrona danych testowych

- Dane testowe przechowywane są w dedykowanym elektronicznym folderze.

- Nadzór nad integralnością gromadzonych danych prowadzi właściciel danego projektu.

- Nadzór nad bezpieczeństwem danych prowadzi Administrator Danych.

21. Metodyka szacowania ryzyka

Opis metodyki szacowania ryzyka jest zawarty w „Metodzie szacowania ryzyka". Jako kryterium wyznaczania poziomu akceptacji ryzyka jest dążenie do wyrównania ryzyk szczątkowych aktywów w firmie. Wartości ryzyka akceptowalnego jest każdorazowo ustalana na przeglądach zarządzania.

22. Dokumenty związane:

1) Deklaracja stosowania bezpieczeństwa informacji,
2) Metoda szacowania ryzyka

KONIEC