TYTUŁ: Bezpieczeństwo systemów informatycznych

OPRACOWAŁ	*SPRAWDZIŁ*	*ZATWIERDZIŁ*
Imię nazwisko	*Imię nazwisko*	*Imię nazwisko*
Adrian Gnus	*Krystyna Kowalczyk*	*Aleksander Słota*
Podpis	*Podpis*	*Podpis*
Data 10.03.2020	*Data 10.03.2020*	*Data 10.03.2020*

ZAWARTOŚĆ PROCEDURY

Wersja nienadzorowana

1. CEL

Celem procedury jest zapewnienie prawidłowej realizacja zadań wynikających z zakresu administrowania sprzętem komputerowym i gromadzenia danych w formie elektronicznej.

2. ZAKRES STOSOWANIA

Procedura obowiązuje wszystkich pracowników firmy w okresie ich zatrudnienia oraz podwykonawców działających na zlecenie firmy w przedmiotowej sferze.

3. SKRÓTY I DEFINICJE

Administrator systemów – osoba działająca na podstawie umowy bądź zlecenia na wykonywanie obsługi informatycznej firmy

4. ODPOWIEDZIALNOŚĆ I UPRAWNIENIA

Prezes Zarządu:

Nakreśla i nadzoruje wszelkie działania związane z funkcjonowaniem systemu informatycznego w firmie.

Dyrektor Agencji Celnej :

Nadzoruje przestrzeganie zasad bezpieczeństwa systemów informatycznych związanych z funkcjonowaniem Oddziału Sławków, Oddziału Małaszewicze, Oddziału Hrubieszów, Oddziału Chorzów, Oddziału Medyka, Oddziału Gdynia, Oddziału Świnoujście.

Kierownicy wszystkich komórek organizacyjnych:

Nadzorują przestrzeganie zasad bezpieczeństwa systemów informatycznych w podległych komórkach organizacyjnych.

Administratorzy systemów:

Przeprowadzają wszelkie czynności związane z funkcjonowaniem systemu informatycznego oraz bezpieczeństwem informacji.

5. OPIS POSTĘPOWANIA

Czynność	Osoba odpowiedzialna	Tryb postępowania
Zawieranie umów o zakup oprogramowania bądź sprzętu informatycznego	Prezes firmy	Wybór na rynku najlepszej oferty, Zatwierdzanie zamówień nadsyłanych przez kierownika agencji, administratora systemów, Zmiany w umowach
Zawieranie umów o świadczenie usług informatycznych	Prezes firmy	Wybór na rynku najlepszej dla firmy oferty, Zmiany w umowach
Tworzenie, rozbudowa systemów komputerowych	Administrator systemów	TSL Silesia Sp. z o.o. zatrudnia informatyka oraz korzysta z zewnętrznych dostawców usług informatycznych.
Nadzór nad systemem wymiany informacji	Administrator systemów, Kierownik jednostki organizacyjnej	W zakresie poczty elektronicznej nadzór nad przepływem informacji sprawuje Dyrektor Oddziału. Nadzór nad serwerem poczty elektronicznej sprawuje firma DOMENY PL. Maksymalna przepustowość skrzynek wynosi 20MB. Oprogramowanie pocztowe jest zabezpieczone filtrem antyspamowym.
Nadzór nad zainstalowanym oprogramowaniem	Administrator systemów	W zakresie bezpieczeństwa danych: Instalowanie oprogramowania antywirusowego, zaimplementowanie mechanizmów ochrony sieci komputerowej, monitoring sieci komputerowych.

Wykonywanie kopii zapasowych	Administrator systemów	Agencja Celna - tworzenie przyrostowej kopii bezpieczeństwa raz dziennie przez program Shadow Protect Server firmy StoregeCraft na zewnętrznych dyskach twardych pracujących w RAID5 oraz replikowanie na drugi zestaw zewnętrznych dysków twardych pracujących w RAID5 znajdujący się w innej lokalizacji. Centrala - Tworzenie kopii plików serwera raz dziennie na dysku zewnętrznym. Sprawdzanie poprawności wykonywania kopii serwera „sławkowskiego" odbywa się automatycznie przez program tworzący kopię bezpieczeństwa. Ponadto minimum raz w tygodniu sprawdzany jest dziennik kopii. Minimum raz w miesiącu odbywa się testowe odzyskiwanie informacji z kopii zapasowych.
Bieżący nadzór nad prawidłowością funkcjonowania systemów komputerowych	Kierownik Oddziału	W zakresie stwierdzonych nieprawidłowości, Wypracowanie systemów HELP DESK Z usługobiorcą usług informatycznych oraz z usługodawcami oprogramowania.
Stosowane zabezpieczenia pomieszczeń serwerowych, pomieszczeń komputerowych	Prezes Firmy, Dyrektor Agencji Celnej	Stosowane zabezpieczenia: 1. Mechaniczne: wydzielone osobne pomieszczenie z ograniczonym dostępem (zamykane na klucz, do dyspozycji tylko wyznaczonych osób). 2. Alarm oraz monitoring na terenie budynku oraz pomieszczeń. 3. Klimatyzacja w pomieszczeniu serwerowym. 4. Dostępny odpowiedni sprzęt gaśniczy. 5. Awaryjne zasilanie (zastosowanie zasilania awaryjnego UPS w przypadku krótkotrwałych zaników prądu oraz możliwość podpięcia agregatu prądotwórczego w przypadku dłuższych przerw w dostawie prądu).
Stosowane zabezpieczenia serwerów	Administrator systemów	- aktualizacja systemów operacyjnych, - włączona zapora sieciowa, - zainstalowane oprogramowanie antywirusowe z automatyczną aktualizacją bazy wirusów, - zasady haseł dotyczące serwera „sławkowskiego" (minimum 8 znaków, minimalny okres ważności hasła 1 dzień, maksymalny 90 dni, blokada konta na 30 minut po maksymalnie 10 nieudanych próbach), - konfiguracja RAID dysków.
Stosowane zabezpieczenia stanowisk komputerowych	Administrator systemów	- aktualizacja systemów operacyjnych, - aktualizacja zainstalowanego oprogramowania, - włączona zapora sieciowa, - zainstalowane oprogramowanie antywirusowe z automatyczną ochroną systemu plików w czasie rzeczywistym, skanowaniem nośników wymiennych, sprawdzaniem plików przy włączeniu komputera, automatyczną aktualizacją bazy wirusów, - blokada sesji po 15 minutach i wymuszenie konieczności ponownego zalogowania, - dla użytkownika: zakaz odchodzenia od komputera z niezablokowaną sesją.

Stosowany system zabezpieczeń dla oprogramowania: polecenie zakładania haseł dostępu i nadawania uprawnień	Prezes firmy, Dyrektor Agencji Celnej, Agent celny, Kierownik Biura Zarządu	W zakresie poczty elektronicznej oraz innego oprogramowania dotyczącego działalności firmy - Prezes firmy lub Dyrektor Agencji Celnej. W zakresie kont na serwerze „sławkowskim" i oprogramowania celnego - Dyrektor Agencji Celnej. W zakresie indywidualnych stanowisk komputerowych – pracownik/agent celny. W zakresie plików z poufnymi danymi (np. dane osobowe) – Kierownik Biura Zarządu. W centrali firmy przyjęto system okresowych zmian haseł do systemów operacyjnych: hasła zmieniane są co trzy miesiące (co najmniej 8 znaków w tym cyfra), W przypadku aplikacji celnych okresowa zmiana haseł co 1 miesiąc. Zakaz przechowywania haseł w niechronionej formie.
Odbieranie uprawnień i zmiana haseł dostępu	Prezes firmy, Dyrektor Agencji Celnej	W przypadku zwolnienia, ograniczenia uprawnień lub innych okoliczności następuje zmiana haseł oraz kodów dostępu znanych pracownikowi.
Stosowane zabezpieczenia sieci LAN i WLAN	Administrator systemów	Stosowanie odpowiednich zabezpieczeń sieci, tj: - zapora sieciowa na styku LAN-sieć publiczna, - aktualne oprogramowania routerów, - kluczowe urządzenia sieciowe zabezpieczone silnym, nietypowym hasłem, - WLAN szyfrowane (zastosowanie standardu WPA2), - wydzielenie odrębnej (również szyfrowanej) sieci bezprzewodowej dla gości. Monitorowanie trendów i rozbudowa zabezpieczeń w przypadku zmiany standardów.
Korzystanie z HELP DESKU	Kierownik Oddziału	Bezpośredni dostęp do systemów helpdesk posiada kierownik agencji. W przypadku wystąpienia jakiejkolwiek nieprawidłowości - agent celny jest zobowiązany powiadomić kierownika o wystąpieniu awarii.
Reagowanie na nieprzewidziane zdarzenia związane z zakłóceniem działania systemu lub jego awarią	Administrator systemów	Podjęcie odpowiednich działań naprawczych w celu wyeliminowania zaobserwowanych samodzielnie lub zgłoszonych przez pracownika awarii z czasem reakcji określonym w umowie. W razie konieczności przywrócenie danych z kopii bezpieczeństwa.
Podjęcie działań w przypadku zdarzeń losowych	Prezes zarządu, Administrator systemów	Należy mieć na uwadze, że ze względu na różnorodność możliwych zdarzeń losowych podejmowane działania powinny być jak najlepiej dostosowane do sytuacji. Poniższe kroki są ogólnymi wskazówkami. - wyłączenie (jeśli to możliwe) uszkodzonego sprzętu komputerowego, - odłączenie od zasilania i sieci oraz odseparowanie uszkodzonego sprzętu od innych urządzeń, - przeniesienie sprawnych urządzeń w bezpieczne miejsce. W celu zabezpieczenia danych tworzone są kopie bezpieczeństwa. - Jeżeli uszkodzeniu ulegnie serwer „sławkowski" należy stworzyć nową maszynę wirtualną na serwerze „bytomskim" i na niej przywrócić system z backupu. Następnie przekonfigurować wszystkie routery na połączenie z nową podsiecią. - Jeżeli uszkodzeniu ulegnie serwer „bytomski" należy tymczasowo wykorzystać dowolny dostępny komputer jako serwer wymiany plików oraz źródło bazy danych. Następnie bez zbędnej zwłoki zakupić nowy sprzęt, zainstalować system serwerowy i odtworzyć sytuację sprzed

		wystąpienia awarii. Awaryjnie do wykorzystania są dwa stare serwery: dawny serwer „sławkowski" (obecnie służy jako serwer repliki kopii zapasowych serwera „sławkowskiego". W sytuacji zagrożenia ciągłości działania firmy obecne zdanie traci priorytet) oraz dawny serwer „bytomski" (nieużywany). Obydwa serwery znajdują się w różnych lokalizacjach, innych niż obecnie używane. W momencie zdarzenia losowego wyłączającego z użytku jednocześnie obydwa obecnie działające serwery jest możliwość awaryjnego działania firmy na dawnych serwerach do czasu naprawy/zakupu nowego sprzętu.
Postępowanie w przypadku incydentu związanego z bezpieczeństwem informacji	Wszystkie osoby	1. Każda osoba, która uzyskała informacje o możliwości wystąpienia lub wystąpieniu incydentu bezpieczeństwa informacji zobowiązana jest niezwłocznie powiadomić przełożonego oraz Administratora systemu. 2. Osoba powiadamiająca powinna podjąć działanie zabezpieczające lub naprawcze na własną rękę tylko i wyłącznie w sytuacji gdy podjęcie natychmiastowego działania jest bezpieczne i niezbędne, a osoba posiada odpowiednie kompetencje. 3. Osoba zgłaszająca w miarę możliwości powinna zabezpieczyć materiał dowodowy. 4. Przełożony oraz Administrator systemu zapoznają się z relacją osoby zgłaszającej oraz zaistniałą sytuacją. 5. Przełożony oraz Administrator systemu wybierają metodę dalszego postępowania oraz jeśli to możliwe podejmują stosowne działania. 6. W przypadku poważnych incydentów bezpieczeństwa informacji i/lub niemożliwości podjęcia szybkich działań naprawczych niezwłocznie informowany zostaje Prezes Zarządu. 7. Wszelkie incydenty bezpieczeństwa informacji odnotowywane są w rejestrze zdarzeń zagrażających bezpieczeństwu.
Praca na odległość	Administrator systemu,	Zapewnienie bezpiecznego tunelowego połączenia określonych komputerów z serwerem (wg. dyspozycji wydanych przez Dyrektora Agencji Celnej/Prezesa Zarządu). Monitorowanie i nadzór nad bezpiecznym korzystaniem z sieci.
Usuwanie danych (w przypadku przekazania na zewnątrz lub utylizacji sprzętu komputerowego)	osoba przekazująca sprzęt	Zadbanie o trwałe usunięcie danych z nośników korzystając ze sprawdzonych i dostępnych metod.

6. UDOKUMENTOWANE INFORMACJE

1. Z1_TSL/BI-4
2. Instrukcja wydawania i przechowywania kluczy – Bytom.
3. Instrukcja wydawania i przechowywania kluczy – Sławków.
4. Instrukcja wydawania i przechowywania kluczy – Małaszewicze
5. Instrukcja wydawania i przechowywania kluczy – Hrubieszów
6. Instrukcja wydawania i przechowywania kluczy – Gdynia
7. Instrukcja wydawania i przechowywania kluczy – Świnoujście
8. Instrukcja wydawania i przechowywania kluczy – Chorzów
9. Instrukcja wydawania i przechowywania kluczy – Medyka

Zestawienie oprogramowania dozwolonego do stosowania:

NAZWA	OBSZAR ZASTOSOWANIA	RODZAJ LICENCJI
Windows 7 i nowsze	system operacyjny	oem
Microsoft Office	biurowy	oem, box
Huzar	celny	płatna
EuroTrans	spedycyjno-biurowy	płatna
StorageCraft	backup	płatna
NitroPro	biurowy	płatna
ESET	antywirus	płatna
ABBYY FineReader	biurowy	płatna
Firebird	baza danych	darmowe
PDFSam	biurowy	darmowe
Trans.eu	spedycja	darmowe
GG	spedycja	darmowe
OpenVPN	połączenia zdalne	darmowe
Skype	spedycja	darmowe
GreenRail	spedycja	darmowe
WinRAR	biurowy	darmowe
PDF Creator, Acrobat Reader, Flash Player, Java	biurowy	darmowe

Lista programów dozwolonych do stosowania jest listą otwartą. Na wniosek pracownika i po zatwierdzeniu Prezesa Zarządu może zostać rozszerzona o niezbędne dla pracownika programy.