POLITYKA BEZPIECZEŃSTWA INFORMACJI WYDAWNICTWA SINE QUA NON

Zarząd SQN świadomy wagi zasobów informatycznych oraz konieczności ochrony informacji stanowiących podstawę świadczonych na rzecz klientów usług, w tym danych osobowych podlegających ochronie na podstawie 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) dalej zwane „RODO", zdecydował się na wdrożenie i uaktualnianie Polityki Bezpieczeństwa Informacji.

I. Opis spółki

SQN jest to więcej niż wydawnictwo. Wydawnictwo to nie tylko instytucja, budynek, miejsce. Wydawnictwo to ludzie. SQN tworzy grupa osób o odmiennych zainteresowaniach i specjalizujących się w różnych dziedzinach. Znajdziecie wśród nas zapalonych kibiców piłkarskich, muzycznych geeków, znawców świata popkultury oraz fanów fantastyki w każdym kształcie i rozmiarze. Połączyło nas zamiłowanie do książek i marzenie o dzieleniu się z innymi prawdziwie wybitnymi tytułami. Każdy z nas dzierży swoją własną cegiełkę – budujemy zwartą i niezaprzeczalnie mocną konstrukcję, jaką jest wydawnictwo SQN. Wszyscy działamy z pasją i zaangażowaniem, ponieważ uważamy literaturę za warunek ciągłego istnienia kultury – warunek sine qua non.

II. Model biznesowy i strategia firmy

Wydawnictwo SQN sprzedaje swoje publikacje w kanale B2B ora B2C dokładając wszelkich możliwych starań, aby publikacje te były jak najlepszej jakości. Koncentrujemy się na obsłudze klienta hurtowego, detalicznego, sklepów internetowych, ale także na rozwoju swojego kanały sprzedaży B2C.

Dążymy do tego aby być liderem na rynku książek sportowych oraz muzycznych a także w TOP5 w kategorii fantastyka.

III. Definicje

Bezpieczeństwo informacji – zachowanie poufności, integralności i dostępności informacji, w tym ochrona przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych, co oznacza, że informacja nie jest ujawniana osobom nieupoważnionym, jest ona dokładna i kompletna oraz dostępna i użyteczna na żądanie upoważnionego personelu, oraz osób, których informacje dotyczą.

Dane osobowe – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie

identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej. Ilekroć w niniejszej polityce mowa o bezpieczeństwie informacji, odnosi się to także do danych osobowych.

Przetwarzanie - oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

Pseudonimizacja - oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;

Administrator - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania;

Podmiot przetwarzający - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;

Odbiorca - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;

Strona trzecia - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe;

Zgoda osoby, której dane dotyczą - oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub

wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;

Naruszenie ochrony danych osobowych - oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;

Ryzyko – prawdopodobieństwo wystąpienia zagrożenia, które, wykorzystując podatność(ci) aktywu, może doprowadzić do jego uszkodzenia lub zniszczenia, w tym do naruszenia danych osobowych.

Szacowanie ryzyka – całościowy proces analizy i oceny prawdopodobieństwa i powagi ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, określane poprzez odniesienia się do charakteru, zakresu, kontekstu i celów przetwarzania danych. Ryzyko szacowane jest przez SQN na podstawie bieżącej i okresowej obiektywnej oceny, w ramach której stwierdza się, czy z operacjami przetwarzania danych wiąże się ryzyko lub wysokie ryzyko.

Poufność i **Integralność** – zapewnienie dostępu do informacji tylko osobom upoważnionym.

Dostępność – zapewnienie, że osoby upoważnione będą miały dostęp do informacji tylko wtedy gdy jest to uzasadnione.

Zarządzanie ryzykiem – proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych, przy zachowaniu akceptowalnego poziomu kosztów.

Incydent związany z bezpieczeństwem informacji – incydent związany z bezpieczeństwem informacji 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.

IV. Zakres obowiązywania Polityki Bezpieczeństwa Informacji

Polityka Bezpieczeństwa Informacji stanowi element strategii opartej na podejściu wynikającym z ryzyka biznesowego, odnoszącej się do ustanawiania, wdrażania, eksploatowania, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji.

V. Deklaracja Zarządu

Zarząd SQN świadomy wagi zasobów informatycznych oraz konieczności ochrony informacji stanowiących podstawę świadczonych na rzecz klientów usług, zdecydował się na wdrożenie Polityki Bezpieczeństwa Informacji.

Zapewnienie bezpieczeństwa informacji oraz systemów, w których są one przetwarzane jest jednym z kluczowych elementów polityki firmy oraz warunkiem ciągłego rozwoju. Gwarancją sprawnej i skutecznej ochrony przetwarzanych informacji jest zapewnienie wysokiego poziomu świadomości bezpieczeństwa pracowników firmy oraz zastosowanie niezbędnych rozwiązań technicznych.

Zarząd spółki wprowadzając Politykę Bezpieczeństwa Informacji, deklaruje, że wdrożona polityka będzie podlegać ciągłemu doskonaleniu i aktualizacji o wszelkie zmiany wynikające z rozwoju firmy, oraz powszechnie obowiązujących przepisów prawa regulujących sposób postępowania z informacjami.

Bezpieczeństwo informacji oznacza:

- ochronę zasobów informacji oraz środków służących do jej przetwarzania,
- zapewnienie bezpieczeństwa i ciągłości przetwarzania informacji,
- systematyczne zarządzanie ryzykiem poprzez identyfikację zagrożeń i opracowanie działać zabezpieczających.

Celem wprowadzenia Polityki Bezpieczeństwa Informacji jest osiągnięcie poziomu organizacyjnego i technicznego, który:

- będzie gwarantował ochronę danych Klientów oraz ciągłość procesu ich przetwarzania,
- zapewni zachowanie poufności informacji chronionych, integralności i dostępności informacji chronionych,
- zagwarantuje odpowiedni poziom bezpieczeństwa informacji, bez względu na jej postać, we wszystkich systemach jej przetwarzania,
- maksymalnie ograniczy występowanie zagrożeń dla bezpieczeństwa informacji, które wynikają z celowej bądź przypadkowej działalności człowieka oraz ich ewentualne wykorzystanie na szkodę firmy,
- zapewni poprawne i bezpieczne funkcjonowanie wszystkich systemów przetwarzania informacji,
- zapewni gotowość do podjęcia działań w sytuacjach kryzysowych dla bezpieczeństwa, firmy SQN, jej interesów oraz przetwarzanych przez nią informacji.

W realizacji powyższych celów ma pomóc między innymi wyznaczenie osób odpowiedzialnych za optymalny podział i koordynację zadań związanych z zapewnieniem bezpieczeństwa informacji oraz przyjęcia za obowiązujące przez wszystkich pracowników polityk i procedur bezpieczeństwa obowiązujące w firmie SQN. Określone zasady przetwarzania informacji będą okresowo przeglądane i aktualizowane przez wyznaczone do tego osoby w celu jak najlepszej reakcji na potencjalne zagrożenia i incydenty. Ciągłe doskonalenie systemu zapewni bezpieczeństwo informacji i pozwoli sprostać oczekiwaniom klientów i instytucji państwowych w zakresie ich przetwarzania.

Odstępstwa od któregokolwiek zapisu niniejszej Polityki Bezpieczeństwa Informacji wymagają pisemnej zgody zarządu.

VI. Postanowienia ogólne

Każdy pracownik firmy SQN jest zapoznawany z postanowieniami zawartymi w Polityce Bezpieczeństwa Informacji, Polityce Prywatności SQN oraz z aktualnymi procedurami ochrony informacji w obszarze wykonywanych obowiązków. Poniżej przedstawiono podstawowe zasady realizacji Polityki Bezpieczeństwa Informacji:

- Każdy pracownik przeszedł szkolenie z zasad ochrony informacji, spełnia kryteria dopuszczenia do informacji. Fakt odbycia szkolenia potwierdzany jest listą obecności na szkoleniu
- Każdy pracownik przeszedł szkolenie z zasad ochrony informacji w związku z wejściem w życie RODO Fakt odbycia szkolenia potwierdzany jest listą obecności na szkoleniu
- Każdy pracownik posiada wyłącznie konieczne do wykonywania powierzonych mu zadań prawa i zakres dostępu do informacji
- Każdy pracownik bierze udział w okresowych szkoleniach i podlega audytom prowadzonym przez firmę
- Wszyscy pracownicy są świadomi konieczności ochrony zasobów informacyjnych firmy i aktywnie uczestniczą w procesie jej ulepszania
- Za bezpieczeństwo poszczególnych elementów odpowiadają konkretne osoby, którym zostało powierzone takie zadanie.
- Dostęp do miejsc szczególnie chronionych, w tym do miejsc przechowywania informacji mają wyłącznie osoby upoważnione.
- System jest chroniony kompleksowo, uwzględniając różne stopnie i ogniwa ogólnie pojętego procesu przetwarzania informacji.

Zabezpieczenie danych osobowych przetwarzanych w formie papierowej

SQN w głównej mierze przetwarza dane osobowe w formie elektronicznej. W przypadku przetwarzania danych osobowych w formie papierowej, zastosowanie znajdują poniższe procedury:

- Dane osobowe przetwarzane są wyłącznie w pomieszczeniu zabezpieczonym przed dostępem osób innych niż upoważnione do przetwarzania danych za pomocą zamka, do którego klucz posiada osoba upoważniona do przetwarzania danych, a klucz zapasowy znajduje się u bezpośredniego przełożonego lub klucz zapasowy znajduje się w zamykanym magazynie kluczy zapasowych, do których dostęp ma każdy członek zarządu
- W przypadku przetwarzania danych osobowych w formie papierowej w pomieszczeniu, do którego mają dostęp osoby nieupoważnione do przetwarzania danych osobowych, dokumenty zawierające dane osobowe przechowywane są w osobnej zamykanej szafie, lub kasie pancernej, do której dostęp ma wyłącznie osoba upoważniona do przetwarzania danych osobowych a klucz zapasowy znajduje się u bezpośredniego przełożonego lub klucz zapasowy znajduje się w zamykanym magazynie kluczy zapasowych, do których dostęp ma każdy członek zarządu .
- W formie papierowej przetwarzane są umowy handlowe SQN, umowy pracownicze SQN, CV i listy motywacyjne wykorzystywane w procesie rekrutacji.
- W sytuacjach gdy jest to możliwe, dokumenty zapisywane są w wersji elektronicznej, a oryginały są niszczone lub deponowane w miejscu przechowywania zabezpieczonym w sposób określony powyżej.
- Prawo wglądu do dokumentów pracowniczych przetwarzanych w formie papierowej mają określone osoby tj. Zarząd Spółki, bezpośredni przełożony danego pracownika, radca prawny. Dostęp do dokumentów pracowniczych odbywa się za pośrednictwem jednej osoby, która ma bezpośredni dostęp do tych dokumentów, na wniosek jednej z ww. osób.
- W przypadku konieczności udostępnienia danych pracowniczych przetwarzanych w formie papierowej innym niż ww. upoważnionym osobom, decyzję podejmuje indywidualnie członek zarządu, a fakt ten jest osobno rejestrowany.
- Zaleca się minimalizować liczbę wydruków dokumentów z danymi poufnymi i osobowymi. Nie należy pozostawiać w drukarce wydruków zawierających takie dane.

Odpowiedzialność użytkowników systemu informatycznego

Do obowiązków użytkowników systemów informatycznych należą:

- przestrzeganie zaleceń i instrukcji Administratora, a w przypadku powołania – także zaleceń i instrukcji IOD, w zakresie bezpieczeństwa i prawidłowego wykorzystania systemów, • ochronę przed zniszczeniem i kradzieżą powierzonych narzędzi pracy w tym: komputera, telefonu firmowego i innych, • wykorzystywanie powierzonych narzędzi pracy wyłącznie do celów związanych z realizacją obowiązków zawodowych,
- zachowanie poufności udostępnionych pracownikowi haseł dostępu i informacji będących tajemnicą przedsiębiorstwa,
- przestrzeganie polskiego prawa w zakresie wykorzystania oprogramowania, treści multimedialnych i elektronicznych form komunikacji, ochrony danych osobowych zgodnie z wytycznymi przekazanymi podczas szkoleń i zawartych w Polityce Prywatności SQN i Polityce Bezpieczeństwa Informacji SQN

- wprowadzenie pozyskanych danych osobowych, do rejestru zbiorów danych osobowych, celem wypełnienia obowiązku informacyjnego (o ile taki obowiązek wynika z powszechnie obowiązujących przepisów prawa), za pomocą jednorazowej informacji generowanej automatycznie przez system SQN,
- zgłaszanie do Działu IT nieprawidłowości w działaniu lub zauważonych zagrożeń bezpieczeństwa sprzętu komputerowego i wykorzystywanych systemów informatycznych (np. komunikaty o nieprawidłowo wykonanym automatycznym backupie komputera).
- poinformowanie o zleceniu firmie zewnętrznej prac nad aplikacjami webowymi (strony internetowe, kampanie mailingowe i podobne w celu weryfikacji przez Administratora a w przypadku jego powołania IOD, czy w danym projekcie będą zbierane dane osobowe i bezpieczeństwa samego rozwiązania),
- Przechowywanie danych firmowych w różnego rodzaju usługach chmurowych zewnętrznych firm jest dozwolone wyłącznie z wykorzystaniem tych, które maja potwierdzoną zgodność z RODO / GDPR. Listę takich usług prowadzi Dział IT
- w przypadku używania telefonu prywatnego do celów firmowych lub używania prywatnego telefonu w celu dostępu do zasobów firmowych (np. poczta elektroniczna) konieczne jest zgłoszenie takiego faktu w celu instalacji wymaganego dodatkowego oprogramowania, podobnie jak ma to miejsce na telefonach firmowych,
- niezwłoczne poinformowanie zarządu lub IOD o utracie urządzenia, które zawierało dane firmowe lub też utracie urządzenia, które posiadało dostęp do systemów firmowych, podobnie o podejrzeniu wycieku danych i zainfekowania urządzenia złośliwym oprogramowaniem,

- urządzenia mobilne (np. laptop, tablet, telefon) zawierające dane firmowe lub dostęp do systemów firmowych muszą być zaszyfrowane i posiadać odpowiednie oprogramowanie antywirusowe – F-Secure Client Security for Bussines jeśli do szyfrowania użyto hasła wtedy musi to być silne hasło, jeśli kod PIN musi to być kod PIN minimum 6 znaków, jeśli urządzenie było przywrócone do stanu fabrycznego lub sklepowego wtedy koniecznie musi zostać dostarczone do Działu IT. Zabronione jest instalowanie aplikacji, na które SQN nie posiada licencji i oprogramowania do zastosowania darmowego ale do zastosowań domowych. Oprogramowanie. Pracownicy nie mogą instalować na urządzeniach mobilnych aplikacji pochodzących spoza oficjalnych źródeł producenta systemu operacyjnego oraz w szczególności takich, które chcą uzyskać dostęp do kontaktów, poczty itp. Nie wolno również używać nieautoryzowanych modyfikacji systemu operacyjnego.
- W przypadku podejrzenia zainfekowania urządzenia lub nawet przypadkowego kliknięcia na np. zainfekowany załącznik lub link w mailu pracownik zobowiązany jest odłączyć komputer i/lub urządzenie mobilne od sieci przewodowej i bezprzewodowej, a następnie pilne poinformowanie Administratora, a w przypadku jego powołania IOD.
• Zabronione jest wykonywanie własnych backupów danych przy użyciu rozwiązań bez szyfracji danych.

Regulamin zarządzania hasłami

Systemy udostępniane pracownikom dają dostęp do kluczowych i bardzo cennych z punktu widzenia przedsiębiorstwa danych: transakcji handlowych, informacji o klientach, danych osobowych, zamówieniach itp. W związku z tym by utrudnić dostęp do tych danych osobom niepożądanym konieczne jest odpowiednie zabezpieczenie przechowywanych w systemach danych. Najprostszym sposobem jest stosowanie bezpiecznych haseł - tj. na tyle skomplikowanych by nie było możliwe łatwe ich odgadnięcie, a przy tym na tyle naturalne dla osoby je wykorzystujące by nie utrudniały dostępu do tych systemów.

Hasła przekazane pracownikowi stanowią tajemnicę przedsiębiorstwa co zobowiązuje pracownika do należytego ich chronienia a w przypadku nieuprawnionego udostępnienia bądź przekazania może stanowić podstawę pociągnięcia do odpowiedzialności karnej.

Wymogi odnośnie haseł

W każdym wykorzystywanym przez nas systemie wymagane jest od użytkowników stosowanie bezpiecznych haseł. Tam gdzie jest to możliwe system nie przyjmie od użytkownika hasła nie spełniającego minimalnych wymagań bezpieczeństwa, czyli:

- hasło musi mieć minimum 8 znaków,
- hasło musi składać się z 3 rodzajów znaków (np. duże litery, małe litery, cyfry lub znaki specjalne),

Hasła powinny być okresowo zmieniane by w przypadku wykradnięcia, wycieku hasła możliwie szybko zablokować dostęp osobie nieuprawnionej. W przypadku haseł w domenie Windows i systemów korzystających z kont domeny Windows system automatycznie wymusza zmianę hasła i zasady jego tworzenia.

Przekazywanie i przechowywanie haseł

Hasła do narzędzi firmowych generowane są dla każdego użytkownika i tylko jemu przeznaczone - udostępnianie haseł lub urządzeń zawierających dane firmowe lub posiadających dostęp do systemów firmowych innym osobom jest stanowczo zakazane.

Należy mieć na uwadze że udostępnione hasło może być wykorzystywane do nadużyć za co odpowiedzialność ponosi właściciel konta. Jeżeli celem udostępnienia hasła jest udostępnienie innej osobie konta z większymi uprawnieniami należy taką potrzebę zgłosić.

Hasła zapamiętywane w przeglądarce powinny być zabezpieczone hasłem głównym, którego wpisanie odblokuje dostęp do wszystkich zapisanych haseł.

Hasła powinny być przechowywane w dedykowanym do tego celu oprogramowaniu, które zabezpiecza dostęp do bazy haseł poprzez jej zaszyfrowanie i dostęp jest zabezpieczony za pomocą klucza prywatnego lub odpowiedniego hasła.

Blokowanie dostępu w przypadku zgubienia hasła

W przypadku zgubienia hasła, podobnie jak w przypadku utraty urządzenia zawierającego dostęp do systemów firmowych lub dane firmowe (bądź podejrzenia jego wycieku np. na skutek działalności złośliwego oprogramowania) pracownik zobowiązany jest do natychmiastowego zgłoszenia Administratorowi a w przypadku jego powołania IOD, oraz niezależnie w Dziale IT konieczności zablokowania kont dostępu tak by możliwie jak najszybciej zablokować potencjalne próby wykorzystania zgubionego hasła. Blokada może być też zastosowana na wniosek przełożonego.

Blokowanie konta po nieudanych próbach logowania

W domenie Windows po 10 nieudanych próbach logowania konto użytkownika zostaje zablokowane na 30 minut. Tylko administrator może odblokować konto przed upływem tego czasu.

Resetowanie haseł

Ponieważ hasła w oryginalnej postaci w formacie tekstowym nie są przechowywane, nie jest możliwe ich odzyskanie. Możliwe jest natomiast zresetowanie hasła na wniosek użytkownika (wyłącznie dla jego kont) - w tym celu należy zgłosić taką potrzebę w Dziale IT.

W szczególnych przypadkach możliwe jest zresetowanie hasła pracownika na zlecenie jego przełożonego - np. w celu uzyskania dostępu do komunikacji pocztowej z klientem pod nieobecność handlowca.

Zasady korzystania z urządzeń mobilnych (przenośnych, jak np. laptop, tablet, telefon) i komputerów stacjonarnych.

Dla większości pracowników SQN głównym narzędziem pracy jest urządzenie mobilne (zwykle laptop) lub komputer stacjonarny - obowiązkiem pracownika jest dbanie o powierzony mu sprzęt i dane co w przypadku fizycznego uszkodzenia/zniszczenia może spowodować obciążenie pracownika kosztami naprawy/zakupu.

Powierzenie komputera, telefonu i oprogramowania

Dział IT zapisuje numer seryjny komputera i przypisuje do niego licencje zainstalowanego oprogramowania w tym: systemu operacyjnego, pakietu Office i innych programów komercyjnych. Tak przygotowany komputer zostaje przypisany do konkretnego pracownika i wtedy może nastąpić fizyczne przekazanie komputera do użytkowania.

Użytkowanie firmowych urządzeń i komputerów

Na każdym komputerze i telefonie przekazanym do użytku zainstalowane są programy niezbędne do pracy. Nie wolno instalować na komputerach i telefonach firmowych dodatkowych aplikacji (na komputerach możemy dodać tylko aplikacje dostępne w domenie firmowej) mogą zawierać złośliwe oprogramowanie, wykraść dane, zaszyfrować dyski sieciowe i lokalne, może to unieruchomić stanowisko pracy na czym straci pracownik i pracodawca.

Nie wolno samodzielnie instalować oprogramowania, na które SQN nie posiada licencji, w tym:

- nie wolno instalować tzw. oprogramowania pirackiego, oprogramowania do użytku
- nie wolno instalować oprogramowania z licencją do użytku domowego /niekomercyjnego.

Nie wolno udostępniać komputerów, telefonów firmowych osobom trzecim (np. gościom spoza firmy):

- mogą oni zainstalować oprogramowanie szpiegujące,
- wykraść lub zniszczyć dane,
- umyślnie lub nieumyślnie uszkodzić system.

Zabezpieczenia antywirusowe i firewall

Program antywirusowy F-Secure Client Security for Bussines jest obowiązkowy i domyślnie zainstalowany na firmowych komputerach i telefonach. Program F-Secure Client Security for Bussines zawiera wbudowaną zaporę ogniową skonfigurowaną do działania w sieci firmowej (przez nadanie centralnie zarządzanej polityki bezpieczeństwa). W sieciach innych niż firmowa zapora sieciowa chroni komputer przed atakami wirusów i szkodliwego oprogramowania. Administratorzy są powiadamiani o wykrytych zagrożeniach. W przypadku wykrycia złośliwego oprogramowania na komputerze lub telefonie automatycznie uruchamiane jest skanowanie całego komputera.

Dodatkowym zabezpieczeniem przed wirusami jest oprogramowanie na serwerze pocztowym dostarczane przez zewnętrznego usługodawcę hostingowego.

Usunięcie oprogramowania antywirusowego jest zabronione, i równoznaczne z wzięciem odpowiedzialności za ewentualnie wyrządzone szkody. Nie można instalować innego oprogramowania antywirusowego. Jeżeli na komputerze lub telefonie firmowym nie ma programu antywirusowego lub nie działa on prawidłowo należy ten fakt zgłosić do Działu IT.

Jeśli telefon prywatny ma dostęp do systemów firmowych lub danych przetwarzanych przez SQN, obowiązują takie same zasady bezpieczeństwa jak dla telefonów firmowych.

Dostęp do internetu

Komputery firmowe domyślnie konfigurowane są w sposób umożliwiający połączenie z Internetem. Połączenie można uzyskać wpinając się w gniazdko sieciowe w biurze - w przypadku (gdy gniazdko nie jest podłączone należy ten fakt zgłosić do Działu IT) lub dedykowaną odpowiednio zabezpieczoną sieć bezprzewodową. Telefony zawierają pakiety danych, które umożliwiają dostęp do Internetu.

Wykorzystywanie aplikacji typu P2P w sieci firmowej jest zabronione podobnie jak pobieranie nielegalnych danych i udostępnianie nielegalnych danych.

Firma SQN loguje ruch wychodzący do internetu co w przypadku wykrycia wykorzystania w sieci firmowej aplikacji P2P lub pobierania, udostępniania nielegalnych treści (np. pirackiego oprogramowania, filmów i muzyki) umożliwia wskazanie konkretnej osoby odpowiedzialnej za złamanie prawa.

Dostęp zdalny do sieci firmowej

Dostęp zdalny do sieci firmowej możliwy jest poprzez wykorzystanie oprogramowania VPN, certyfikatów i połączeń SSL. Niezbędne aplikacje domyślnie instalowane są na wszystkich komputerach przenośnych. Do logowania służą loginy i hasła wykorzystywane standardowo do logowania w domenie Windows lub dedykowane certyfikaty generowane z określonym terminem ważności dla każdego pracownika.

Zasilanie awaryjne komputerów pracowników

W przypadku komputerów przenośnych zasilanie awaryjne zapewnia bateria.

Kradzieże urządzeń firmowych (laptopy, tablety, telefony)

Każde urządzenie np. prywatne zawierające dostęp do systemów firmowych lub dane firmowe jest traktowane pod względem bezpieczeństwa tak samo jak firmowe. Wymagane jest zgłoszenie takiego faktu i przygotowanie takiego urządzenia pod bezpieczeństwa tak samo jak urządzenia firmowego.

Co ważne sama strata sprzętu nie stanowi dla firmy tak dużego zagrożenia jak możliwość wycieku bądź złego wykorzystania zawartych na komputerze danych. Osoba nieupoważniona może np. uzyskać dostęp do danych osobowych, kontaktów do klientów by rozesłać im złośliwe maile, udostępnić pliki w internecie, itd.

W przypadku kradzieży należy niezwłocznie powiadomić administratora a w przypadku jego powołania IOD, oraz niezależnie Dział IT by zablokować wszystkie konta.

By uniknąć kradzieży komputera przenośnego nie wolno pozostawiać go w samochodzie.

Szczególnie niebezpieczne jest zamykanie notebooka w bagażniku w miejscu publicznym.

Zwrot komputera i oprogramowania

Zwrot komputera pracownika może nastąpić w przypadku

- wymiany komputera na nowy,
- rozwiązania umowy o pracę.

Może też mieć miejsce czasowe przekazywanie komputera do Działu IT na potrzeby naprawy lub instalacji niektórego oprogramowania.

Zasady korzystania z telefonów firmowych

Udostępnienie pracownikowi telefonu będącego własnością firmy zobowiązuje pracownika do dbania o stan techniczny telefonu. Pracownik jest zobowiązany do zgłaszania usterek i uszkodzeń aparatu do osoby administrującej telefonami. W przypadku uszkodzenia telefonu pracownik może być zobowiązany do pokrycia kosztów napraw wszelkich szkód wynikających z jego zaniedbania.

Serwisowanie, zwrot lub wymiana telefonu

Telefony komórkowe pozwalają na integrację z wieloma firmowymi sytemami, np. poprzez synchronizację kontaktów firmowych, możliwości pobierania poczty firmowej - pracownik zobowiązany jest do ochrony telefonu jako nośnika tych informacji tak samo jak komputera. Dlatego w przypadku:

- przekazywania telefonu do serwisu,
- zwrotu telefonu,
- wymiany telefonu,

pracownik zobowiązany jest dostarczyć telefon do Działu IT w celu weryfikacji zabezpieczeń, szyfrowania, wcześniej pracownik zobowiązany jest do wykonania kopii danych znajdujących się na telefonie.

Instalowanie oprogramowania

Pracownik zobowiązany jest do korzystania jedynie z zainstalowanych przez Dział IT aplikacji i zabronione jest instalowanie innych aplikacji. Zwłaszcza zabronione jest instalowanie aplikacji na które SQN nie posiada licencji, a tym bardziej aplikacji pirackich i nieznanego pochodzenia. Oprócz oczywistego faktu łamania prawa, może też dojść w takim przypadku do zainstalowania na telefonie wirusów, dialerów i innych szkodliwych aplikacji, które mogą przyczynić się do strat finansowy firmy bądź być źródłem wycieku kluczowych danych. W takim przypadku pracownik zostanie obciążony kosztami wyrządzonych szkód.

ICE to międzynarodowy skrót informujący ratowników do kogo powinni dzwonić w razie nagłego wypadku. W książce adresowej należy wpisać numer telefonu do wybranej osoby i podpisać jako ICE. W przypadku chęci wpisanie kilku osób należy je opisać kolejno: ICE1, ICE2, itd.

Kradzież telefonu

W przypadku kradzieży telefonu komórkowego należy niezwłocznie powiadomić Administratora, a w przypadku jego powołania IOD, oraz niezależnie Dział IT i samodzielnie zablokować kartę, dzwoniąc do Biura Obsługi Klienta - pomoc 24 godziny na dobę, 7 dni w tygodniu.

Kradzież telefonu powinna być też zgłoszona na Policji, dzięki czemu możliwe jest zablokowanie nie tylko karty, ale i aparatu na podstawie unikalnego numeru IMEI (znajduje się na obudowie aparatu oraz w karcie gwarancyjnej).

Standardy sieci WAN i LAN

WAN

W centrali firmy zainstalowane są dwa łącza internetowe przy czym jedno wykorzystywane jest przez pracowników do uzyskania dostępu do internetu, a drugie pracuje w technologii Failover.

Szyfrowane sieci VPN

W każdej zdalnej placówce firmy SQN łącze internetowe udostępniane jest przez dedykowany firewall obsługujący logowanie ruchu internetowego, oraz umożliwiający zestawienie bezpiecznych szyfrowanych tuneli do centrali firmy z wykorzystaniem technologii VPN.

Bezpieczeństwo sieci WAN

W przypadku dostępu do sieci Internet pracownik odpowiada za pobrane i udostępniane danych, dlatego zalecana jest szczególna ostrożność przy:

- pobieraniu plików z sieci (WWW, poczta, itp),
- odczytywaniu załączników z nieznanych źródeł,
- plików i odnośników przesyłanych przez komunikatory, pocztę
- braniu udziału w ankietach - niektóre mogą być próbą wyłudzenia poufnych informacji o pracownikach i firmie.

Do komunikacji wewnętrznej zalecane jest oprogramowanie Slack.

Komunikacja pomiędzy serwerami pocztowymi nie jest szyfrowana, więc nawet przy zapewnieniu szyfrowanego połączenia z serwerem pocztowym z komputera pracownika - informacje przesyłane pomiędzy serwerami mogą zostać odczytane. Dlatego zabronione jest wysyłanie poufnych danych drogą pocztową nawet do zaufanych odbiorców. Dane takie można przesłać np. szyfrując dane w pliku ZIP a hasło do pliku podając inną drogą (sms, rozmowa telefoniczna).

Podczas korzystanie z dostępu do Internetu zabronione jest wykorzystywanie łączy firmowych do pobierania programów i materiałów multimedialnych łamiących prawa autorskie, w tym:

- pirackich utworów muzycznych,
- pirackich filmów,
- pirackich programów,
- i innych danych naruszających prawa autorskie.

Połączenia wychodzące logowane są dla celów diagnostycznych ale mogą zostać wykorzystane w celu zidentyfikowania osoby łamiącej prawa autorskie lub przeciążającej łącza sieciowe.

LAN

W centrali firmy i jej oddziałach pracownicy uzyskują dostęp do zasobów sieci przez podpięcie swoich komputerów do sieci LAN lub dedykowanej odpowiednio zabezpieczonej sieci WiFi. Z sieci LAN można uzyskać dostęp do kluczowych aplikacji.

Dostęp do zasobów sieciowych (dysków sieciowych)

W centrali firmy standardowo pracownikom przydzielany jest dostęp do kilku dysków sieciowych umożliwiających na współdzielenie plików i wygodniejszą pracę grupową.

Zabronione jest przechowywania na Wymianie kopii zapasowych i archiwalnych, ponieważ do tego zasoby dostęp ma zbyt wiele osób co może doprowadzić do nieautoryzowanego dostępu do poufnych danych. Kopie zapasowe i archiwalne powinny być przechowywane na dysku R.

Zabronione jest przechowywanie na zasobach sieciowych materiałów multimedialnych i programów łamiących prawa autorskie. Dane zawierające dane osobowe nie mogą być przechowywane w katalogach publicznych. Wymiana danych powinna odbywać się pomiędzy konkretnie nazwanymi osobami a nie poprzez upublicznianie pliku (np., wysłanie mailem zabezpieczonego hasłem pliku ZIP lub użycie dedykowanego folderu z określonymi uprawnieniami danej grupy). Przesyłanie danych osobowych między współpracownikami z wewnątrz firmy bezwzględnie wymaga używania firmowego konta pocztowego (ze względu na szyfruję protokołu pocztowego).

Zabronione jest przechowywanie na zasobach sieciowych prywatnych plików pracowników.

Bezpieczeństwo sieci LAN

Sieć LAN umożliwia połączenie z kluczowymi systemami obsługującymi szereg procesów firmowych dlatego sieć ta powinna być szczególnie chroniona. Z tego względu kategorycznie zabronione jest udostępnianie dostępu do sieci LAN osobom nie pracującym w SQN. Dostęp dla klientów możliwy jest z wykorzystaniem sieci gościnnej. Zabronione jest wykorzystywanie „niepewnych" komputerów (np. komputerów prywatnych nie posiadających zainstalowanego oprogramowania antywirusowego i firewalla) do komunikacji z aplikacjami firmowymi, a w szczególności zabronione jest:

- kopiowanie na takie komputery poufnych danych, w tym danych osobowych, • instalowanie i korzystanie z klienta VPN,
- logowanie do poczty.

Zabronione jest samodzielne wpinanie do sieci LAN urządzeń aktywnych np.: switchy, routerów i bezprzewodowych punktów dostępowych. Wpięcie źle skonfigurowanego urządzenia może spowodować awarię sieci uniemożliwiając procę wielu osobom w firmie. Źle zabezpieczone urządzenie może pozwolić na dostęp osobom nieuprawnionym. W obu wymienionych wcześniej przypadkach pracownik ponosi pełną odpowiedzialność za wyrządzone szkody.

Regulamin korzystania z poczty elektronicznej

Poczta elektroniczna będąc istotnym kanałem komunikacji z klientem wymaga szczególnej dbałości o bezpieczeństwo. Wiele przekazywanych danych ma status poufnych lub stanowiących dane osobowe a dostęp osób trzecich do tych danych jest realną stratą finansową dla SQN oraz naraża na naruszenie bezpieczeństwa przetwarzania danych osobowych. Hasło do systemu pocztowego dla naszego konta jest generowane przez Dział IT i zalecana jest jego zmiana raz na kwartał, zakazane jest stosowanie w przypadku poczty elektronicznej haseł prostych. Hasło do systemu pocztowego musi mieć minimum 12 znaków, zawierać małe i duże litery, cyfry, znaki specjalne, nie może zawierać słownikowych fragmentów. Zalecaną formą zmiany hasła pocztowego jest zlecenie zmiany do Działu IT. Hasło takie musi być skomplikowane i trudne do złamania ze względu na dane osobowe, i inne, które czasem zwierają skrzynki pocztowe, a samego hasła nie musimy pamiętać ponieważ jest zapisane w programie pocztowym.

Adresy e-mail

Każdy pracownik otrzymuje do dyspozycji konto pocztowe, którego adres tworzony jest według wzorca: imie.nazwisko@wsqn.pl - jest to standard firmowy, którego świadomość mają nasi pracownicy oraz klienci co ułatwia komunikację.

W szczególnych przypadkach, np. dublujące się nazwiska pracownika możliwe jest przyjęcie innego schematu adresu email.

Aliasy e-mail

Użytkownicy są też standardowo podpinani pod pewne ogólno-firmowe aliasy, np:

ekipa@wsqn.pl - wszyscy pracownicy naszej firmy.

Zakładanie nowych aliasów

Jeżeli zachodzi potrzeba utworzenia nowego aliasu, np. na potrzeby kontaktu z pewną grupą klientów, promocji, itp., należy utworzyć sprawę IT, zaproponować nazwę aliasu i osoby, które powinny być pod niego podpięte. Dział IT zweryfikuje czy taki alias nie jest już wykorzystywany.

Możliwe jest zakładanie aliasów w większości domen, które posiadamy na naszych serwerach.

Bezpieczeństwo

Do odbierania i wysyłania poczty należy korzystać z szyfrowanych połączeń SSL lub TLS - domyślnie wszystkie komputery konfigurowane w Dziale IT są tak ustawione.

Należy mieć świadomość że pomimo ustawienia szyfrowanych połączeń do i z serwera pocztowego, komunikacja pomiędzy serwerami pocztowymi przebiega w sposób nieszyfrowany. Dlatego w przypadku potrzeby przesłania informacji o wysokim poziomie poufności należy dodatkowo zaszyfrować wiadomość.

Zasady blokady, zmiany i usuwania konta e-mail

Do zablokowania konta pocztowego może dojść w przypadku:

- odejścia pracownika,

Rozwiązanie umowy z pracownikiem

W przypadku rozwiązania umowy z pracownikiem jego przełożony zgłasza ten fakt do Działu IT, który wyłącza konto użytkownika. Możliwe jest też przekierowanie aliasów byłego pracownika na jego zastępcę co umożliwia przechwycenie całej przyszłej korespondencji.

Limity, archiwizacja poczty

Każda skrzynka pocztowa na serwerze ma rozmiar limitowany do 15 GB

Ochrona antywirusowa i antyspamowa

Na serwerze pocztowym działa kilka mechanizmów mających na celu zmniejszenie wolumenu SPAM'u który trafia na firmowe skrzynki pocztowe.

Filtr antywirusowy

Każdy mail przychodzący i wychodzący z serwera pocztowego jest filtrowany przez program antywirusowy na serwerze i w przypadku wykrycia wirusa kasowany.

Dodatkową ochronę stanowią zainstalowane na komputerach pracowników programy antywirusowe, które również skanują pocztę przychodzącą i wychodzącą.

Filtr antyspamowy

Wszystkie maile skanowane są przez filtr antyspamowy, który ocenia SPAM systemem punktowym i powyżej 6 punktów oznacza wiadomość jako SPAM. Maile takie trafiają do katalogu Spam/Junk w skrzynce pocztowej danego odbiorcy.

Można zmienić domyślną wartość przy jakiej maile uznawane są za SPAM dla danego użytkownika, w konfiguracji skrzynki pocztowej w Webmailu, zakładka Spam. Możliwe jest też ustawienie reguł dla poszczególnych nadawców, bądź serwerów nadawców - by były traktowane jako SPAM, bądź by były przepuszczane.

Zasady korzystania z konta pocztowego

Konto nie może być wykorzystywane w wysyłkach masowych a w szczególności do rozsyłania SPAM'u. Nie wolno też podawać adresów pocztowych w serwisach nie związanych z pracą - mogą one generować duży ruch, np. poprzez częste wysyłanie powiadomień co zwiększy obciążenie serwera pocztowego, a w skrajnych przypadkach może uniemożliwić normalne korzystanie z poczty.

Zasady realizacji przez SQN uprawnień osób, których dane osobowe są przetwarzane

W przypadku otrzymania przez pracownika SQN żądania realizacji nw. praw przysługujących osobom, których dane osobowe przetwarza SQN:

1) prawo do informowania o przetwarzaniu danych osobowych

2) prawo dostępu do treści przetwarzanych danych osobowych

3) prawo do sprostowania danych

4) prawo żądania od Administratora usunięcia danych

5) prawo żądania od Administratora ograniczenia przetwarzania danych

6) prawo do przenoszenia danych

7) prawo wniesienia sprzeciwu wobec przetwarzania danych

8) prawo wniesienia skargi do polskiego organu nadzorczego lub organu nadzorczego innego państwa członkowskiego Unii Europejskiej

9) prawo do cofnięcia zgody na przetwarzanie danych osobowych w dowolnym momencie

10) prawo do uzyskania interwencji ludzkiej ze strony Administratora, wyrażenia własnego stanowiska i do zakwestionowania decyzji opartej na zautomatyzowanym przetwarzaniu danych.

11) pracownik ma obowiązek niezwłocznie poinformować o tym Administratora, a w przypadku jego powołania IOD, a w przypadku nieobecności – osobę wskazana jako zastępstwo na czas nieobecności.

W przypadku wykorzystywania przez pracowników narzędzi i/lub infrastruktury SQN w celach prywatnych (w tym do przetwarzania danych osobowych niezwiązanych z celami służbowymi), oraz urządzeń prywatnych - używanych w celach służbowych - do przetwarzania prywatnych danych osobowych (niezwiązanych z celami służbowymi), administratorem tych danych osobowych jest pracownik, który powierza dane SQN do przetwarzania wyłącznie w celu ich przechowywania, a SQN jest Podmiotem przetwarzającym te dane wyłącznie w celu przechowania. W zakresie tych danych SQN realizuje wyłącznie obowiązki Podmiotu przetwarzającego, na pracowniku ciążą wszelkie obowiązki administratora danych osobowych, i pracownik ponosi pełną odpowiedzialność z tego wynikającą.