POLITYKA WOODWARD DOTYCZĄCE BEZPIECZEŃSTWA KOMPUTERÓW I SYSTEMÓW INFORMATYCZNYCH

1 Wprowadzenie

1.1 Informacje ogólne

Niemalże każde istotne działanie w Woodward zależne jest od informacji i systemów informatycznych. Jeżeli informacje lub systemy informatyczne zostają postawione w sytuacji zagrożenia, Woodward może zostać narażony na m.in. stratę klientów, zmniejszenie obrotów czy też utratę reputacji. Z tego też względu, bezpieczeństwo informacji musi stanowić krytyczny element środowiska biznesowego firmy.

Firma wprowadziła pewne polityki dotyczące dopuszczalnego użytkowania i bezpieczeństwa zasobów komputerowych. Okresowo prowadzone są audyty pod kątem zgodności z politykami firmy dotyczącymi sprzętu komputerowego.

1.2 Cele

Niniejsza polityka przedstawia podstawowe środki kontroli bezpieczeństwa wdrożone w Woodward. Środki kontroli bezpieczeństwa to minimum wymagane do zarządzania różnego rodzaju ryzykiem, w tym: nadużyciami finansowymi, sprzeniewierzeniem środków finansowych, szpiegostwem na tle gospodarczym, przypadkami sabotażu, nieuprawnionym dostępem, niewłaściwym wykorzystaniem, utratą integralności danych, przypadkowym zniszczeniem, niedostępnością systemów oraz zgodnością z przepisami prawa. Zaleca się, aby poszczególne siedziby Woodward zastosowały bardziej rygorystyczne wymagania dotyczące bezpieczeństwa od tych, które zostały zdefiniowane w dalszej części niniejszego dokumentu.

1.3 Zgodność

Konsekwencje naruszenia postanowień niniejszych polityk mogą obejmować podjęcie czynności dyscyplinarnych, które mogą m.in. obejmować rozwiązanie umowy o pracę. Naruszenia mogą również skutkować powiadomieniem Działu Personalnego, Działu Globalnego Bezpieczeństwa, Ryzyka i Zgodności IT, lidera danego pracownika, Komitetu Nadzoru nad Postępowaniem w Biznesie oraz innych przedstawicieli kadry menedżerskiej Woodward, jak również podmiotów zewnętrznych, w tym organów egzekwowania prawa i/lub organizacji ds. regulacji, akredytacji i licencjonowania. Utrata akredytacji lub unieważnienie certyfikacji bądź licencji może skutkować nałożeniem kar finansowych, a osoby naruszające prawo cywilne lub karne mogą podlegać karze więzienia.

2 Odpowiedzialna struktura organizacyjna

2.1 Technologie informatyczne – Bezpieczeństwo informacji

Dział Globalnego Bezpieczeństwa, Ryzyka i Zgodności IT odpowiedzialny jest za stworzenie i udokumentowanie polityk, procedur i standardów związanych z bezpieczeństwem. Dział sprawuje kontrolę i zapewnia monitoring, których celem jest ułatwienie ochrony danych Woodward przed przypadkowym zniszczeniem, złośliwymi atakami, nieuprawnionym dostępem lub modyfikacjami, jak również zgodność z wymaganiami w zakresie przechowywania danych i licencji oprogramowania, HIPAA, SOX, Polityką Bezpieczeństwa w Zakresie Ochrony Prywatności (Safe Harbour)/Prawem europejskim w zakresie ochrony prywatności, przepisami dotyczącymi eksportu, Międzynarodowymi Przepisami w zakresie Obrotu Bronią (International Traffic in Arms Regulations - ITAR) oraz innymi obowiązującymi przepisami w zakresie ochrony i prywatności danych.

Dział Globalnego Bezpieczeństwa, Ryzyka i Zgodności IT w przypadku potrzeby zapewnia przeglądy pod kątem bezpieczeństwa (w tym nowych przejęć) i jest odpowiedzialny za budowanie zespołów pracowników świadomych w kwestiach bezpieczeństwa poprzez wdrożenie stosownych programów. Dział Globalnego Bezpieczeństwa, Ryzyka i Zgodności IT nadzoruje tworzenie i utrzymanie Planów Przywrócenia Gotowości do Pracy po Wystąpieniu Sytuacji Nadzwyczajnej. Dział ten jest również odpowiedzialny za spełnianie wymogów i monitorowanie zgodności z niniejszymi Politykami, jak również Politykami Dopuszczalnego Użytkowania Komputerów i Sieci 1-31 oraz innymi stosownymi Politykami i procedurami.

2.2 Technologia informatyczna - Infrastruktura

Dział Globalnej Infrastruktury odpowiedzialny jest za zarządzanie niniejszymi Politykami oraz standardami odnoszącymi się do wszystkich aspektów bezpieczeństwa WAN/LAN, infrastruktury Active Directory (w tym serwerów), środowiska komputerowego systemów biznesowych, Internetu, intranetu, systemów EDI, danych systemów e-Biznes, centrów danych, w których znajdują się komputery systemów biznesowych oraz infrastruktury systemów poczty elektronicznej, w tym bramek poczty elektronicznej dostępnych w Internecie. Dział Globalnej Infrastruktury IT oraz Dział Globalnych Usług IT dla Klientów ponoszą wspólną odpowiedzialność za zapewnienie zgodności z Polityką dotyczącą Dopuszczalnego Użytkowania Komputerów i Sieci (Polityka Woodward 1-33).

2.3 Technologia informatyczna - Usługi serwisowe

Dział Globalnych Usług IT dla Klientów odpowiedzialny jest za zarządzanie niniejszymi Politykami oraz standardami dotyczącymi wszystkich aspektów bezpieczeństwa stacjonarnych komputerów osobistych, stacji roboczych UNIX oraz wszystkich typów mobilnego sprzętu komputerowego, w tym m.in. smartfonów, tabletów i laptopów. Dział Globalnych Usług IT dla Klientów oraz Dział Globalnej Infrastruktury IT ponoszą wspólną odpowiedzialność za serwery lokalnych plików, serwery wydruku oraz serwery aplikacji w miejscach, gdzie pracownicy Działu Globalnej Infrastruktury IT nie są fizycznie obecni. Pracownicy Działu Lokalnej Infrastruktury IT oraz Działu Globalnych Usług IT dla Klientów są również odpowiedzialni za zapewnienie zgodności z Politykami Dopuszczalnego Użytkowania Komputerów i Sieci (Polityka 1-33) w odniesieniu do swoich obszarów odpowiedzialności.

2.4 Technologia informatyczna - Systemy biznesowe

Dział Globalnych Systemów Biznesowych IT odpowiedzialny jest za stworzenie, wdrożenie i utrzymanie systemów i aplikacji, które przyczyniają się do zachowania bezpiecznego środowiska komputerowego, zgodnego z regułami zawartymi w niniejszych politykach. Podczas tworzenia aplikacji, kodów i kontroli dostępu mających na celu ochronę poufności, integralności i dostępności informacji Woodward, należy wziąć pod uwagę bezpieczeństwo danych.

2.5 Audyt wewnętrzny

Departament Audytu Wewnętrznego Woodward okresowo przeprowadza audyty, których celem jest zapewnienie, że wymagania dotyczące bezpieczeństwa informacji zostały wdrożone i są przestrzegane, oraz że wdrożono środki kontroli finansowej, takie jak podział obowiązków.

2.6 Organizacje niezwiązane z Woodward

Podmioty niezależne, którym przyznano dostęp do systemów komputerowych, odpowiedzialne są za przestrzeganie standardów bezpieczeństwa Woodward w procesie uzyskiwania dostępu do systemów komputerowych Woodward. Podmioty takie są również odpowiedzialne za stosowanie standardów bezpieczeństwa Woodward na urządzeniach, które mogą uzyskiwać dostęp do środowiska komputerowego Woodward. Odpowiedzialność taka musi zostać uwzględniona w

porozumieniach umownych z firmami niezależnymi, którym przyznawany jest dostęp do systemów komputerowych Woodward. Standardy bezpieczeństwa Woodward stanowią część polityk dotyczących Bezpieczeństwa Systemów Informatycznych i Komputerów (1-41) oraz polityk Dopuszczalnego Użytkowania Komputerów i Sieci (1-33). Porozumienia umowne muszą zostać zatwierdzone przez radcę prawnego Woodward oraz Wiceprezesa ds. IT. Podmioty niezależne to przedsiębiorstwa joint venture, firmy nabyte, firmy sprzedane oraz inne firmy niezależne niepowiązane z Woodward. (Odpowiedzialność w kwestii bezpieczeństwa za rutynowe transakcje typu e-Biznes klientów/dostawców wiążące się z dostępem do informacji przez strony internetowe uwzględniona została w odpowiedniej umowie Woodward o dostępie do usług typu e-Biznes. Żadne inne porozumienia umowne nie są wymagane.)

3 Standardy bezpieczeństwa

Oczekuje się, że wszyscy pracownicy IT Woodward będą stosować się do Polityk etycznych Woodward oraz Kodeksu Postępowania Woodward w odniesieniu do obszaru IT.

3.1 Poufność

IT ustanowi Polityka i procedury mające na celu ochronę biznesu oraz danych zastrzeżonych Woodward przed przypadkowym uszkodzeniem, skutkami katastrof naturalnych, nieuprawnionym dostępem, złośliwymi atakami lub modyfikacjami. Wszystkie dane zawarte w systemach informatycznych Woodward muszą być dostępne dla uprawnionych pracowników IT. W przypadku danych, które obejmują dokumenty zastrzeżone, tajemnice handlowe, elektronicznie chronionych informacji zdrowotnych (ePHI) lub innych informacji poufnych lub uprzywilejowanych (i) uprawnieni do otrzymania dostępu są jedynie specjalnie upoważnieni pracownicy IT, a (ii) taki dostęp będzie podlegać odstępstwom od polityk prywatności określonym w Sekcji 3.5 w dalszej części niniejszego dokumentu. Pracownikom IT w żadnym przypadku nie wolno ujawniać żadnych dokumentów zastrzeżonych, tajemnic handlowych, elektronicznie chronionych informacji zdrowotnych (ePHI) lub innych informacji poufnych lub uprzywilejowanych osobom nieupoważnionym, jak również wykorzystywać takich informacji w celu osiągnięcia korzyści osobistej, w tym ujawniać lub wykorzystywać w inny niewłaściwy sposób.

Konsultanci, audytorzy, niezależni pracownicy IT, niezależni dostawcy oraz wszelkie inne osoby, które uzyskały jakikolwiek rodzaj informacji poufnych dotyczących systemów komputerowych, konfiguracji systemowych, infrastruktury sieciowej Woodward itp., muszą podpisać umowę o zachowaniu poufności przed uzyskaniem dostępu do takich informacji. Wystarczy jedna umowa o nieujawnianiu informacji dla danej firmy. Kopię podpisanej umowy należy przechowywać w dokumentacji.

3.2 Integralność i dostępność danych

Liderzy oraz pracownicy muszą mieć zaufanie, że informacje, które wykorzystują w celu podejmowania decyzji biznesowych oraz tworzenia produktów są dokładne i że w żaden sposób nie zostały zmienione ani zmodyfikowane. Pracownicy IT odpowiedzialni są za zapewnienie, że tworzone są kopie zapasowe wszystkich danych serwerów sieciowych i komputerów systemów biznesowych, a nośniki kopii zapasowych są dostępne i zabezpieczone przed utratą na skutek zaniedbania, katastrofy naturalnej lub kradzieży.

3.3 Upoważnienie

Jedynie osoby posiadające odpowiednie upoważnienie mają prawo do uzyskania dostępu do danych i systemów komputerowych Woodward. Nikt nie może autoryzować swojego własnego dostępu. W większości przypadków, dostęp autoryzowany jest przez przełożonego danego pracownika lub właściciela danych/informacji.

3.4 Właściwe wykorzystanie

Systemy oraz zasoby komputerowe Woodward przeznaczone są do użytku związanego z realizacją celów biznesowych firmy. Właściwe wykorzystanie zostało zdefiniowane w Polityce 1-33 (Dopuszczalne Użytkowanie Komputerów i Sieci).

3.5 Prywatność

Woodward zobowiązany jest do ochrony danych pracowników przed nieuprawnionym dostępem wewnętrznym lub zewnętrznym. Praktyki i narzędzia bezpieczeństwa Woodward wykorzystywane są w celu ochrony prywatności danych klientów, dostawców i pracowników, jak również informacji biznesowych Woodward.

Woodward zastrzega sobie prawo, jak również może podjąć decyzję o upoważnieniu pracowników IT do monitorowania lub zbadania wszelkich aspektów systemów komputerowych, systemów sieciowych oraz infrastruktury, w tym m.in. monitorowania stron internetowych odwiedzanych przez pracowników, monitorowania aktywności na czatach i w ramach grup dyskusyjnych, weryfikacji materiałów pobieranych lub zamieszczanych w internecie przez pracowników, weryfikacji plików lub aplikacji przechowywanych na dyskach sieciowych i lokalnych, jak również weryfikacji wiadomości mailowych. Co więcej, jeśli wymagać będą tego okoliczności, Woodward może prowadzić działania związane z tworzeniem spisów procesu zarządzania mieniem, wyszukiwaniem e-discovery, audytami licencji oprogramowania, zapobieganiem utracie/wyciekowi danych oraz inne działania dochodzeniowe. W związku z tym, osoby korzystające z systemów Woodward nie mogą oczekiwać żadnej prywatności podejmowanych przez siebie działań lub przekazywanych wiadomości.

3.5.1 Przepisy UE w zakresie danych osobowych oraz inne przepisy dotyczące ochrony prywatności

Woodward zobowiązany jest do stosowania się do wytycznych UE w zakresie ochrony prywatności oraz danych osobowych zgodnych z Polityką Prywatności dla Ochrony Danych Osobowych w Unii Europejskiej (Polityka 5-24).

3.5.2 Kontakty objęte tajemnicą zawodową

Pracownikom IT nie wolno przeglądać dokumentów prawnych ani wiadomości mailowych przesyłanych pomiędzy Firmą a jej radcą prawnym i/lub innymi osobami posiadającymi stosowne kwalifikacje, których kontakty z firmą objęte są tajemnicą zawodową. Działania związane z uzyskiwaniem dostępu, przeglądaniem lub ujawnianiem informacji w ramach kontaktów objętych tajemnicą zawodową muszą być prowadzone jedynie w sposób zalecony przez radcę prawnego Woodward.

3.5.3 Elektronicznie chronione informacje zdrowotne (e-PHI)

Pracownikom IT nie wolno przeglądać dokumentów medycznych, w tym (i) wiadomości mailowych lub innych elektronicznie chronionych informacji zdrowotnych (e-PHI) oraz (ii) wszelkich innych poufnych informacji medycznych oraz dokumentacji pochodzących lub dostarczanych przedstawicielom służby zdrowia. Działania związane z uzyskiwaniem dostępu, przeglądaniem lub ujawnianiem poufnych informacji medycznych muszą być prowadzone jedynie w sposób zalecony przez dyrektora ds. medycznych, w tym zgodnie ze wszystkimi wymaganiami dotyczącymi poufności nałożonymi na mocy Ustawy o przenoszeniu i odpowiedzialności za ubezpieczenia zdrowotne (Health Information Portability and Accountability Act - HIPAA).

4 Zarządzanie bezpieczeństwem użytkowników

4.1 Aktywacja konta i pozwolenia

Na pracownikach Działu Personalnego spoczywa obowiązek zapewnienia, że Polityka 1-33 (Polityka dotycząca Dopuszczalnego Użytkowania Komputerów i Sieci) została podpisana przez wszystkich pracowników zatrudnionych w pełnym wymiarze godzin, pracowników zatrudnionych na pół etatu, pracowników czasowych, zleceniobiorców i stażystów przed uzyskaniem przez nich dostępu do systemów komputerowych Woodward. Wszystkie inne osoby muszą podpisać umowę o nieujawnianiu informacji lub Politykę dotyczącą Dopuszczalnego Użytkowania Komputerów i Sieci (1-33), zanim przyznany im zostanie dostęp do systemów komputerowych Woodward.

4.1.1 Konta pracowników

Dział Personalny powiadomi IT o potrzebie utworzenia konta dla nowego pracownika. Odpowiedzialność za powiadomienie IT o istnieniu jakichś obszarów, do których danemu pracownikowi nie należy przyznawać dostępu, spoczywać będzie albo na menedżerze/kierowniku danego działu, albo na Dziale Personalnym.

Dział Personalny zweryfikuje status osoby w Stanach Zjednoczonych (obywatelstwo Stanów Zjednoczonych lub pozwolenie na pobyt stały) w momencie zatrudniania danej osoby. Informacje te zostaną wprowadzone do systemu Lawson lub innego systemu stosowanego w danym czasie przez Dział Personalny. Na podstawie informacji zostaną utworzone flagi pozwoleń i grupy pozwoleń, które mogą być stosowane jednostronnie w celu ograniczenia dostępu osób niebędących obywatelami Stanów Zjednoczonych do ITAR i innych informacji podlegających restrykcjom eksportu w Stanach Zjednoczonych.

IT utworzy wszelkie konieczne konta komputerowe i przypisze uprawnienia i pozwolenia. (Patrz: OP 3-09-4159 Procedura Aktywacji Kont.) Za każdym razem, gdy zezwala na to oprogramowanie systemowe, wymagane jest, aby użytkownicy zmienili hasło wszystkich nowych kont przy pierwszym logowaniu do systemu operacyjnego komputera.

Jeżeli z danym pracownikiem rozwiązano umowę o pracę, pracownik odszedł z firmy lub przeszedł na emeryturę, konto sieciowe Active Directory musi zostać ustawione w sposób odpowiadający nowemu kontu tej osoby, wygenerowanemu przez system Działu Personalnego.

W przypadku dostępu do Internetu, dostępu zdalnego i Użytkowania narzędzi współpracy i oprogramowania konferencyjnego w celu nawiązania kontaktu z miejscami poza Woodward, wymagana jest autoryzacja kadry menedżerskiej. Wymagana autoryzacja jest zgodna z Polityką Dopuszczalnego Użytkowania Komputerów i Sieci (1-33). Wszystkie pozwolenia związane z systemami, danymi i aplikacjami muszą zostać zaakceptowane przez upoważnioną osobę zatwierdzającą. Pozwolenia związane z systemami biznesowymi przypisywane są na mocy postanowień procedury operacyjnej pt. „Pozwolenia dotyczące aplikacji IT (WISE, Oracle, GL, Lawson, EFMS, SAP)” (OP-404). Pozwolenia związane z sieciami i Active Directory przypisywane są na mocy postanowień procedury operacyjnej „Pozwolenia dotyczące wymiany informacji (wymiana informacji poprzez sieć)” (OP-736).

4.1.2 Wewnętrzne konta osób niebędących pracownikami Woodward

Sieć Active Directory dla osób niebędących pracownikami Woodward oraz inne konta dla pracowników czasowych, audytorów, dostawców, konsultantów lub pracowników kontraktowych, którzy będą pracować poza siedzibą Woodward i których dane z jakiegokolwiek powodu nie zostały wprowadzone do oprogramowania Działu Personalnego, muszą być ustawione w sposób, który spowoduje ich wygaśnięcie w ciągu sześciu (6)

miesięcy lub okresu krótszego, liczonego od czasu utworzenia konta. Konta takie mogą być ponownie aktywowane, jeżeli pracownik będzie nadal aktywny w okresie przekraczającym początkowy czas sześciu (6) miesięcy.

4.1.3 Wewnętrzne konta osób niebędących pracownikami IT

Jakakolwiek osoba niebędąca pracownikiem Woodward zatrudniona do pracy w obszarze IT z wykorzystaniem komputerów, systemów informatycznych, infrastruktury sieciowej, systemów komunikacyjnych Woodward i/lub dowolnego typu informacji elektronicznych, musi podpisać umowę o zachowaniu poufności/nieujawnianiu informacji oraz Polityka Dopuszczalnego Użytkowania Komputerów i Sieci (1-33). Postanowienie to dotyczy m.in. osób zatrudnionych na kontrakt, poprzez agencję pracy tymczasowej lub podwykonawcę, jak również osób zatrudnionych przez firmę joint venture lub zaufany podmiot niezależny. Odpowiedni menedżer lub Dyrektor Działu IT odpowiedzialny jest za zapewnienie, że wszystkie konieczne formularze zostały wypełnione.

4.1.4 Wewnętrzne konta działów lub grup

Wykorzystanie kont działów lub współdzielonych kont sieciowych jest zabronione dla wszystkich osób pracujących w danym dziale, w tym m.in. w Dziale Medycznym lub Dziale Personalnym, gdzie odpowiedzialność osobista jest obligatoryjna. Co więcej, kont generycznych i grupowych nie wolno wykorzystywać w celu uzyskania dostępu do danych w przypadku, w którym istnieje konieczność weryfikacji statusu obywatelstwa. Konta współdzielone mogą przyczynić się do zwiększenia kosztów licencji oprogramowania w przypadku licencji opartych na modelu CAL (Client Access License), zmniejszenia stopnia bezpieczeństwa oraz ograniczenia odpowiedzialności w odniesieniu do zmian informacji i danych Woodward. Konta tego typu powinny być stosowane jedynie w przypadkach, w których potrzeby biznesowe uzasadniają dodatkowe ryzyko i wydatki. Przechowywanie danych współdzielonych jest dopuszczalne jedynie w sytuacji, w której pozwolenia zostały ustawione w sposób pozwalający na dostęp osobom potrzebującym dostępu do tych informacji.

4.1.5 Konta dostawców, klientów zewnętrznych i innych podmiotów niezależnych

Wnioski o ustanowienie konta dla dostawców, klientów i innych podmiotów niezależnych muszą przechodzić przez zaakceptowane kanały. (Patrz poniżej.) Każda osoba uzyskująca dostęp do systemów komputerowych lub aplikacji Woodward typu e-Biznes musi posiadać ID i hasło specyficzne dla użytkownika.

4.1.5.1 Dostawcy

Konta dostawców będą autoryzowane przez Dział Globalnych Zakupów. Wnioski dostawców o utworzenie Konta dostawcy będą weryfikowane i akceptowane (lub odrzucane) przez Menedżera ds. Zakupów. Wnioski powinny zawierać informację, że obowiązująca umowa Woodward o dostępie do systemów e-Biznes została zaakceptowana przez dostawcę.

4.1.5.2 Klienci

Konta klientów podlegają autoryzacji pracownika Woodward kontaktującego się z danym klientem, Rzecznika Klientów, Menedżera ds. Technicznych lub Menedżera Projektu. Autoryzacja taka polega na weryfikacji i akceptacji wniosku klienta o ustanowienie Konta klienta. Wnioski powinny zawierać informację, że obowiązująca umowa Woodward o dostępie do systemów e-Biznes została zaakceptowana przez klienta.

4.1.5.3 Spółki joint venture, spółki nabyte, spółki sprzedane, inne firmy niezależne

Wnioski o dostęp dla spółki joint venture lub podmiotu niezależnego lub dostęp potrzebny w celu ułatwienia zakupu lub zbycia należy składać na ręce Wiceprezesa ds. IT. Wnioski muszą określać poziom potrzebnego dostępu oraz wszelkie ograniczenia dostępu, które należy wdrożyć. Kopię wniosku powinny otrzymać następujące osoby: Dyrektor ds. Globalnej Infrastruktury IT, Dyrektor ds. Bezpieczeństwa IT, Dział Ryzyka i Zgodności, Generalny Radca Prawny, Specjalista ds. Zgodności oraz Wiceprezes ds. Personalnych.

Dział Personalny ma za zadanie zapewnić, że każda osoba podpisze Politykę Dopuszczalnego Użytkowania Komputerów i Sieci (1-33) przed uzyskaniem dostępu. Pracownicy Działu Personalnego są również odpowiedzialni za sprawdzenie, że osoby te są faktycznie przedstawicielami spółki joint venture lub podmiotu niezależnego i że zostały upoważnione do otrzymania przywilejów związanych z dostępem.

Po akceptacji Działu Personalnego, Dział Globalnych Usług IT dla Klientów, Dział Globalnej Infrastruktury IT lub upoważniony Administrator ds. Joint Venture utworzą ID użytkownika. Pozwolenia należy ustawiać w sposób, aby za pomocą ID nie można było uzyskać dostępu do ogólnych informacji firmy, lecz wyłącznie do informacji koniecznych do wykonania obowiązków służbowych. Jeżeli konto przeznaczone jest dla osoby niebędącej pracownikiem Woodward, konta tworzone są w sposób, aby ich zdefiniowana aktywność nie przekraczała okresu sześciu (6) miesięcy. Jeżeli konta potrzebne są przez dłuższy okres, przedłużenie ważności może być zrealizowane bezpośrednio przed datą wygaśnięcia konta.

4.2 Standardy dotyczące haseł

4.2.1 Konta użytkowników

Wszystkie konta użytkowników komputerów wymagają hasła, aby uzyskać dostęp do systemów AIX UNIX, Active Directory, WISE, Lawson, Oracle GL, SAP i wszystkich innych systemów komputerowych Woodward. Funkcja starzenia się hasła ustawiona jest tak, aby hasła wygasały co sto dwadzieścia (120) lub mniej dni. Hasła muszą zawierać minimum osiem (8) znaków i nie mogą być łatwe do odgadnięcia. Blokada konta ustawiona jest na pięć (5) nieprawidłowych prób logowania dla wszystkich systemów posiadających tę możliwość.

4.2.2 Konta gości

Domyślne konto gościa zostało zablokowane w domenach Active Directory systemu Windows.
Konta bezprzewodowe poszczególnych osób, które uwierzytelniają się w Sieci Bezprzewodowej dla Gości, a nie uwierzytelniają się w wewnętrznej sieci Woodward, można tworzyć dla dostawców, audytorów, gości itd. ID użytkowników/hasła będą generowane przez Dział Globalnych Usług IT dla Klientów i posiadać będą określoną datę wygaśnięcia.

4.2.3 Konta administratorów

Wszystkie domyślne hasła dla administratorów, systemów lub kont usług ustawione przez producenta oprogramowania muszą zostać zmienione, zanim jakikolwiek komputer lub system komunikacyjny będzie mógł zostać wykorzystany dla potrzeb biznesowych Woodward. Hasła dla kont administratorów lub kont usług z prawami administratora należy

zmieniać za każdym razem, gdy zmienia się personel administracyjny IT lub zaistniało podejrzenie, że bezpieczeństwo haseł zostało zagrożone.

Wszyscy pracownicy IT z podwyższonymi uprawnieniami dotyczącymi kont, muszą spełniać lub przewyższać takie same standardy, które odnoszą się do kont zwykłych użytkowników. Pracownikom IT nie wolno ustawiać swoich kont osobistych w sposób, który zwalnia ich z przestrzegania normalnych wymagań w zakresie bezpieczeństwa, np. ustawień funkcji starzenia się haseł. Wszyscy administratorzy kont AD systemu Windows oraz kont serwerów muszą zmienić nazwę na inną, która nie zawiera słów „administrator" ani „admin".

Od administratorów domen wymaga się, aby posiadali oddzielne konto administratora domeny i nie posiadali przywilejów administratora domeny przypisanych do konta zwykłego użytkownika. W celu umożliwienia kontroli, w przypadku pracy wymagającej zwiększonego stopnia dostępu, wymagane jest wykorzystanie oddzielnego konta administratora przez każdego z administratorów. Konta te muszą być dostosowane do normalnych standardów starzenia się haseł.

Dostęp roota do urządzeń UNIX, dostęp DBA do systemu Oracle oraz podstawowy dostęp administratora do systemu SAP ograniczony jest do kluczowego personelu i musi zostać zaakceptowany przez Dyrektora Globalnej Infrastruktury IT. Konta administratorów domen akceptowane są przez Dyrektora Działu Globalnego Bezpieczeństwa, Ryzyka i Zgodności IT. Inne konta z podwyższonym stopniem dostępu są również ograniczone i muszą być zaakceptowane przez właściwego Menedżera lub Dyrektora IT zgodnie z dokumentacją w Matrycy Kontroli IT SOX (IT SOX Controls Matrix).

Jakakolwiek osoba posiadająca dostęp roota lub DBA do systemów z danymi objętymi Międzynarodowymi Przepisami w zakresie Obrotu Bronią („ITAR") musi być albo obywatelem Stanów Zjednoczonych, albo posiadać Status Stałego Rezydenta. Administratorzy domen dla domeny Active Domain roota lub osoby posiadające dostęp administratora do serwerów z danymi ITAR, muszą również być obywatelami Stanów Zjednoczonych lub posiadać Status Stałego Rezydenta. Pozwolenia w ramach Active Directory dla administratorów, którzy nie są obywatelami Stanów Zjednoczonych ani nie posiadają Statusu Stałego Rezydenta mogą być kontrolowane przez pozwolenia Jednostki Organizacyjnej Active Directory (Active Directory Organizational Unit - OU) lub domeny zależne.

4.2.4 Ustawienia zabezpieczeń kont

Aby zapobiec atakom polegającym na odgadnięciu hasła oraz tam, gdzie pozwala oprogramowanie systemowe, aktywowano opcję blokady konta w przypadku wielu nieudanych prób wprowadzenia hasła. Nieudane próby logowania do systemów krytycznych są rejestrowane; kadra menedżerska IT wyznaczy osobę odpowiedzialną za monitorowanie plików dziennika.

Funkcja minimalnego i maksymalnego starzenia się haseł została skonfigurowana we wszystkich systemach, które umożliwiają takie ustawienia. Dodatkowo ustawiono historię haseł, aby użytkownicy nie mogli ponownie używać tego samego, niewielkiego zestawu haseł.

Konta usług i administratora, w przypadku których funkcja starzenia się haseł mogłaby skutkować przerwaniem usług, mogą być ustawione w sposób, który nie pozwala hasłu nigdy wygasnąć. (Przykład: jeżeli wygaśnie hasło administratora kopii zapasowej, kopia zapasowa może nie zostać uruchomiona.) Wszystkie inne konta, do których przypisane są rozszerzone przywileje, muszą być dostosowane do polityk starzenia się haseł.

4.3 Odejście personelu

4.3.1 Dezaktywacja konta

Pracownicy Działu Personalnego odpowiedzialni są za powiadomienie odpowiedniego personelu IT o przypadkach dobrowolnego lub niedobrowolnego zakończenia stosunku pracy. (Patrz Procedura Wygaśnięcia Konta OP 3-09-3588.) Dział IT odpowiada za dezaktywację wszystkich kont komputerowych (UNIX, Windows, SAP, WISE itd.) oraz zapewnienie, że wszystkie przywileje dostępu zdalnego zostały odwołane.

4.3.2 Usuwanie kont

W powodów biznesowych, dostęp do plików lub poczty elektronicznej osoby, która zakończyła swoją pracę w Woodward, może zostać przyznany innemu pracownikowi, jeżeli ten został upoważniony przez przełożonego osoby, która zakończyła pracę lub Dział Personalny. Pliki o charakterze biznesowym, które muszą pozostać w dokumentacji firmy, powinny zostać przekazane innej osobie. Wszystkie konta pracownika we wszystkich systemach, w tym konta poczty elektronicznej, powinny zostać usunięte w ciągu trzydziestu (30) dni lub czasu krótszego od momentu zakończenia pracy, chyba że Dział Globalnego Bezpieczeństwa, Ryzyka i Zgodności IT zaakceptował odstępstwo od tej Polityka.

4.3.3 Odejście administratora

Jeżeli pracownik posiadający przywileje administratora i/lub dostęp do haseł administratora odejdzie z firmy dobrowolnie lub niedobrowolnie, Dział Globalnych Usług IT dla Klientów odpowiedzialny jest za natychmiastowe cofnięcie praw związanych z dostępem zdalnym i zablokowanie wszystkich kont i danych uwierzytelniających administratora. Dział Globalnych Usług IT dla Klientów powinien również zmienić wszystkie lokalne hasła administratora. Dział Globalnej Infrastruktury IT odpowiedzialny jest za zmianę wszystkich haseł administratora systemu Enterprise oraz innych haseł globalnych, które odchodząca osoba mogła znać.

Jeżeli pracownik posiadający przywileje administratora i/lub dostęp do haseł administratora zmienia stanowisko wewnątrz firmy, należy przeprowadzić weryfikację praw użytkownika, pozwoleń i poziomów dostępu tej osoby. Dział Globalnych Usług IT dla Klientów musi wprowadzić odpowiednie zmiany, w tym zmiany haseł administratora, aby odzwierciedlić nowe obowiązki tego pracownika.

Wszystkie hasła administracyjne, hasła do baz danych i systemów powinny być znane przez przynajmniej dwie (2) osoby. W przypadku, w którym pracownik opuszcza firmę dobrowolnie lub niedobrowolnie i jest jedyną osobą, która zna hasło administratora do systemu komputerowego, bazy danych, oprogramowania aplikacji lub jakiegokolwiek dokumentu chronionego hasłem, osoba ta musi ujawnić to hasło w chwili opuszczania Firmy.

4.3.4 Dane uwierzytelniające dla dostępu zdalnego

Wszystkie dane uwierzytelniające dla celów dostępu zdalnego będą unieważnione natychmiast po otrzymaniu powiadomienia o zakończeniu stosunku pracy. Może to zostać wykonane poprzez zablokowanie dwuetapowego tokena uwierzytelniającego i/lub cofnięcie pozwoleń AD.

Jakakolwiek osoba, której wydano karty elektroniczne, tokeny lub innego rodzaju dane uwierzytelniające, musi zwrócić je w przypadku dobrowolnego lub niedobrowolnego odejścia z firmy.

5 Infrastruktura LAN/WAN

5.1 Autentykacja

Uwierzytelnianie dostępu do systemu następuje za pomocą ID i hasła. Aby uzyskać dostęp z zewnątrz do prywatnej sieci Woodward, wymagana jest autentykacja dwuetapowa.

5.2 Administracja

Wszyscy pracownicy IT odpowiedzialni za sieć komputerową Woodward, niezależnie od tego, czy podleją pod Dział Globalnej Infrastruktury IT lub Dział Globalnych Usług IT dla Klientów oraz niezależnie od tego, czy ich stanowisko odzwierciedla ten obowiązek, ponoszą odpowiedzialność za bezpieczeństwo lokalnej sieci LAN. Od tego miejsca, jakakolwiek osoba odpowiedzialna za LAN będzie nazywana Administratorem LAN.

Naruszenie bezpieczeństwa jednej sieci LAN może zagrażać bezpieczeństwu innych systemów podłączonych do sieci rozległej WAN. W przypadku naruszenia bezpieczeństwa, które nie stanowi bezpośredniego ryzyka, należy skontaktować się z odpowiednim administratorem LAN i przekazać mu polecenie rozwiązania problemu w terminowy sposób. W przypadku, w którym inne sieci LAN Woodward narażone są na bezpośrednie ryzyko, Dyrektor Działu Globalnego Bezpieczeństwa, Ryzyka i Zgodności IT lub Dyrektor Działu Globalnej Infrastruktury IT może autoryzować podjęcie kroków koniecznych do przerwania lub ograniczenia połączeń zagrożonego urządzenia lub sieci LAN, nawiązywanych z innymi siedzibami Woodward do momentu rozwiązania problemu. Wszyscy administratorzy LAN muszą przejawiać chęć rozwiązania lub pomocy w rozwiązaniu wszelkich incydentów związanych z bezpieczeństwem lub naruszeniami zarządzanych przez siebie sieci.

W przypadku, w którym administrator LAN ma uzasadniony powód, aby wierzyć, że jakaś osoba lub jej urządzenie stanowią bezpośrednie i krytyczne ryzyko dla bezpieczeństwa, administrator lub Analityk IT ds. Bezpieczeństwa może podjąć odpowiednie działania bez uprzedniego powiadomienia użytkownika tego urządzenia. W takiej sytuacji, należy natychmiast powiadomić Dyrektora Działu Globalnego Bezpieczeństwa, Ryzyka i Zgodności IT oraz Dyrektora Działu Globalnej Infrastruktury IT. Powiadomienie powinno uwzględniać informacje, które pomogą zrozumieć rodzaj zagrożenia, typ podjętych działań oraz to, czy użytkownik został lub nie został powiadomiony. Jeżeli nie istnieje bezpośrednie niebezpieczeństwo, administrator LAN powinien powiadomić Dyrektora Działu Globalnego Bezpieczeństwa, Ryzyka i Zgodności IT oraz Dyrektora Działu Globalnej Infrastruktury IT przed podjęciem jakichkolwiek działań.

Oprogramowanie i sprzęt, które pozwalają na rejestrację i analizę informacji dotyczących LAN, mogą zostać wykorzystane przez personel Działu Globalnej Infrastruktury IT lub lokalnego administratora LAN, aby zidentyfikować problemy z sieciami LAN/WAN. W przypadku gdy zaistnieje potrzeba użycia tych narzędzi przez innych pracowników, konsultantów lub audytorów Woodward, wcześniej należy uzyskać pozwolenie Dyrektora Działu Globalnej Infrastruktury IT. Z narzędzi należy korzystać pod nadzorem pracowników Działu Globalnej Infrastruktury IT lub lokalnych administratorów LAN. Wszystkie dane zgromadzone za pomocą tych

narzędzi należy uważać za poufne. Jakikolwiek audytor lub konsultant korzystający z tych narzędzi w ramach zaakceptowanego projektu musi podpisać umowę o zachowaniu poufności.

5.3 Ochrona przed włamaniami (IDS, zapora sieciowa, serwery proxy aplikacji, DMZ)

Zewnętrzne i wewnętrzne sieci Woodward odseparowane są od siebie za pomocą jednego lub więcej DMZ (stref zabezpieczających przed atakami na sieć), które czasami noszą nazwę Monitorowanych Podsieci Drugiego Planu (Mid-ground Screened Subnets). Strefy te chronione są za pomocą zapór sieciowych i oprogramowania zapobiegającego włamaniom IPS, jak również monitorowane za pomocą internetowych systemów wykrywania włamań IDS. Wszystkie systemy zarządzane są zgodnie z regułami zdefiniowanymi w niniejszych politykach.

Zanim użytkownicy będą mogli przejść do ekranu logowania, wszystkie przychodzące i wychodzące w czasie rzeczywistym połączenia z sieciami wewnętrznymi Woodward muszą przejść przez zaporę sieciową. Żaden system komputerowy nie może być podłączony do Internetu, jeżeli nie zostanie założona ochrona w postaci zapory sieciowej. (Patrz sekcja 5.4 poniżej.)

Rutery, zapory sieciowe, przełączniki VPN itp. mogą być stosowane z myślą o ochronie sieci wewnętrznej Woodward podczas działań związanych z nabyciem, zbyciem, trwaniem relacji joint venture lub za każdym razem, gdy zaistnieje taka konieczność. Lista aktualnie zaakceptowanych usług przychodzących i wychodzących oraz opcji podłączenia do sieci musi być zawarta w dokumentacji i dostępna dla wszystkich administratorów systemów zgodnie z polityką ograniczonego dostępu i wytycznymi Dyrektora Działu Bezpieczeństwa, Ryzyka i Zgodności IT. Dostęp powinien zostać odmówiony w przypadku jakichkolwiek opcji podłączenia do sieci nieudokumentowanych na ww. liście.

Wszelkie zmiany parametrów konfiguracji zapory sieciowej, usług wspomaganych oraz dopuszczonych opcji podłączenia do sieci muszą być dokonywane w zgodzie z Procedurą Zmian Zapory Sieciowej (OP-690). Przywileje związane z modyfikacją funkcjonalności, opcji podłączenia do sieci i usług wspieranych przez zapory sieciowe muszą zostać ograniczone do kilku osób, których potrzeba posiadania tychże przywilejów wynika z potrzeb biznesowych. Nowe wersje oprogramowania, jego aktualizacje i poprawki zabezpieczeń muszą być instalowane w terminowy sposób, chyba że Analityk IT ds. Bezpieczeństwa lub Dyrektor Działu Bezpieczeństwa, Ryzyka i Zgodności IT zatwierdzili odstępstwo od tej Polityka. Zmiany należy przetestować przed instalacją lub zaplanować na czas, w którym przerwa będzie miała minimalny wpływ na procesy biznesowe.

5.4 Dostęp zdalny

W celu uzyskania dostępu do wewnętrznej sieci Woodward spoza granic sieci Woodward, wymagane jest zastosowanie autentykacji dwuetapowej. Wszystkie serwery zdalnego dostępu zostały skonfigurowane w sposób wymagający uwierzytelniania szyfrowanego.

5.4.1 Połączenia przychodzące (VPN, RAS itd.)

Zanim dostęp zdalny zostanie aktywowany, przełożony pracownika musi zatwierdzić wniosek o przyznanie dostępu zdalnego i autoryzować proces uzyskania dostępu. Wnioski o przyznanie dostępu zdalnego dla osób niebędących pracownikami Woodward muszą być zatwierdzone przez upoważnioną osobę poręczającą. Wniosek musi uwzględniać informację o tym, na jak długo dostęp jest wymagany.

Metoda i rodzaj przyznanego dostępu (VPN, Citrix, OWA, inny) powinien zostać określony według potrzeb pracownika, kosztów różnych opcji oraz wymagań w zakresie bezpieczeństwa. Poszczególni pracownicy mogą mieć różne wymagania zależne od tego, czy znajdują się w podróży służbowej, czy też uzyskują dostęp do sieci ze swojego domu. Przełożeni i osoby poręczające powinni żądać rodzaju dostępu faktycznie potrzebnego, a nie zawierającego wszystkie opcje.

5.4.1.1 VPN

Bramy VPN są ustanawiane i zarządzane przez Dział Globalnej Infrastruktury IT. Połączenia VPN powinny być konfigurowane w sposób, który uniemożliwia nawiązanie połączenia przez zdalnego użytkownika jednocześnie z siecią zdalną i siecią Woodward (np. za wykorzystaniem dzielonego tunelowania). Wszystkie komputery podłączone do sieci wewnętrznej Woodward za pomocą VPN lub dowolnej innej technologii, muszą posiadać i korzystać z aktualnego oprogramowania antywirusowego oraz szyfrowania IPSec. Dział Globalnych Usług IT dla Klientów zainstaluje oprogramowanie klienta VPN skonfigurowane w sposób umożliwiający realizację niniejszej Polityka. Podczas korzystania z technologii VPN w celu nawiązania połączeń z siecią Woodward, podłączone urządzenia stanowią de facto przedłużenie sieci Woodward i jako takie podlegają tym samym regułom i przepisom, które odnoszą się do sprzętu należącego do Woodward.

5.4.1.2 Dostęp z poziomu strony internetowej

Autentykacja dwuetapowa wymagana jest w przypadku dostępu z poziomu strony internetowej za pomocą programów Citrix, XenApps, Outlook Web Access (OWA) lub innych aplikacji internetowych dla pracowników, audytorów, konsultantów lub pracowników kontraktowych, którzy potrzebują dostępu do wewnętrznych zasobów informatycznych Woodward.

Dostęp do strony e-biznesowej Woodward wymaga ID i hasła.

5.4.1.3 Modemy

Serwery z modemami używanymi do wykonywania zakontraktowanych usług wspomagających powinny mieć deaktywowaną funkcję połączeń

analogowych dial-in, za wyjątkiem sytuacji, w których są aktywnie monitorowane przez administratora w ramach wezwania serwisowego.

Dostęp za pomocą funkcji dial-in dla pracowników wykorzystujących modemy do nawiązywania połączeń jest ograniczony do minimum. Wymagana jest autentykacja dwuetapowa.

5.4.2 Dostęp wychodzący

Nawiązywanie połączeń wychodzących za pomocą funkcji dial-out z komputerów osobistych i serwerów, znajdujących się w siedzibie Woodward, nie jest ogólnie promowane i musi zostać zatwierdzone przez Dyrektora Działu Bezpieczeństwa, Ryzyka i Zgodności IT lub Analityka IT ds. Bezpieczeństwa, jak również Dyrektora lub Menedżera Działu Globalnej Infrastruktury IT. Komputery te muszą być skonfigurowane w sposób pozwalający na użycie wyłącznie opcji dial-out.

Nawiązywanie połączeń wychodzących VPN z siedzibami nienależącymi do Woodward jest zabronione. Krótkoterminowe, krytyczne potrzeby biznesowe można zrealizować zgodnie z Procedurą Zmian Zapory Sieciowej (OP-690).

5.5 Rutery, przełączniki, koncentratory i inny sprzęt telekomunikacyjny

Wszystkie rutery, przełączniki, koncentratory i inny sprzęt telekomunikacyjny muszą być chronione hasłami. Hasła przechowywane w plikach konfiguracyjnych powinny zostać zaszyfrowane; niedopuszczalne jest stosowanie haseł domyślnych producentów.

Należy podjąć racjonalne działania, aby ograniczyć dostęp do portu konsoli, szczególnie w przypadku instalacji nowych sieci lub sprzętu. Wszystkie nowo zakupione urządzenia powinny mieć możliwość blokady portu konsoli, a dostęp do portu powinien mieć miejsce po zalogowaniu. Każde urządzenie powinno być w stanie obsługiwać hasła szyfrowane. Należy również zablokować usługi niepotrzebne (np. małe UDP, opcje ekranu dotykowego, http, jeżeli nie są używane). Oprogramowanie typu firmware musi być aktualizowane za każdym razem, gdy zidentyfikowane zostaną punkty newralgiczne, które mogą mieć negatywny wpływ na bezpieczeństwo danych lub systemów Woodward.

Rutery, przełączniki, koncentratory i inny sprzęt telekomunikacyjny nie mogą być zarządzane z poziomu Internetu.

Hasła ruterów, przełączników, koncentratorów i innego sprzętu telekomunikacyjnego nie mogą być łatwe do odgadnięcia i powinny składać się z przynajmniej sześciu (6) znaków; jednym ze znaków musi być liczba lub znak specjalny (np. $, #, *). Hasła należy zmieniać za każdym razem, gdy miejsce ma dobrowolne lub niedobrowolne zakończenie stosunku pracy lub przeniesienie pracownika, który prawdopodobnie zna hasła do tych urządzeń.

Połączenia z dowolną siecią LAN Woodward lub siecią nienależącą do Woodward, można nawiązywać jedynie za pomocą sprzętu zarządzanego lub zatwierdzonego przez Dyrektora Działu Globalnej Infrastruktury IT. Nawiązywanie połączeń przez

sieć Woodward z siecią nienależącą do Woodward wymaga także zatwierdzenia Wiceprezesa ds. IT. Co więcej, osoby niebędące pracownikami Działu Infrastruktury IT nie mogą dodawać ruterów, przełączników, koncentratorów ani żadnych innych urządzeń telekomunikacyjnych do sieci bez zatwierdzenia Dyrektora lub Menedżera Działu Globalnej Infrastruktury IT. Nieautoryzowany sprzęt zostanie odłączony od sieci.

Wszystkie nowe instalacje muszą wykorzystywać przełączniki lub innego rodzaju bezpieczne technologie, które wymagają wyższego poziomu skomplikowania urządzenia monitorującego ruch.

5.6 Linie telekomunikacyjne (T-1, sieć frame relay itd.)

Wszelki sprzęt telekomunikacyjny z danymi zwykłymi lub głosowymi należy przechowywać w zamkniętym pomieszczeniu lub bezpiecznym miejscu.

Wykorzystanie oprogramowania i urządzeń typu Sniffer na liniach telekomunikacyjnych przez osoby nieupoważnione jest zabronione. Upoważnienie do Użytkowania takiego oprogramowania lub urządzeń można otrzymać od Dyrektora Działu Bezpieczeństwa, Ryzyka i Zgodności IT, Dyrektora Działu Globalnej Infrastruktury IT lub Menedżera ds. Infrastruktury.

Wszystkie urządzenia typu CSU/DSU i Sniffer, serwery terminali wykorzystywane dla linii ISDN itp., powinny posiadać hasła, które nie są hasłami domyślnymi. Hasła powinny składać się z minimum sześciu (6) znaków i posiadać przynajmniej jeden (1) znak numeryczny lub specjalny (np. $, %, *). Hasła należy zmieniać za każdym razem, gdy miejsce ma dobrowolne lub niedobrowolne zakończenie stosunku pracy lub przeniesienie pracownika, który prawdopodobnie zna hasła do tych urządzeń.

5.7 Okablowanie (światłowodowe, miedziane)

Pojedyncze kable stacji roboczych i mini koncentratorów nie muszą być zabezpieczane. Wszelkie okablowanie zdalnych szafek kablowych powinno znajdować się w miejscach zamykanych na klucz lub być chronione za pomocą materiału ochronnego, np. rurek lub paneli izolacyjnych. Wszystkie połączenia wykorzystujące szybkozłączki powinny znajdować się w miejscach chronionych. Skrzynki z przyłączami kablowymi (zawierające szybkozłączki) powinny być zamykane za pomocą zdalnych przełączników, pozostających poza normalnym zasięgiem. Punkty połączeń okablowania w pośrednich szafkach kablowych lub głównych koncentratorach sieci powinny być przez cały czas zamknięte, a dostęp do nich powinien być ograniczony jedynie do odpowiednich urządzeń i personelu IT.

5.8 Komunikacja bezprzewodowa

Wszystkie sieci bezprzewodowe WLAN, przeznaczone dla pracowników lub gości w jakiejkolwiek siedzibie Woodward w dowolnym miejscu na świecie, muszą być wcześniej zatwierdzone przez Dyrektora Działu Globalnej Infrastruktury IT. Wszystkie sieci WLAN (dla pracowników lub gości) należy konfigurować i instalować zgodnie z zatwierdzonymi standardami Woodward dotyczącymi sieci WLAN.

Jedynie zatwierdzone, zabezpieczone Punkty Dostępu mogą być podłączane do sieci bezprzewodowej Woodward (WLAN). Użytkownikom nie wolno instalować urządzeń, które umożliwiają uzyskanie bezprzewodowego dostępu do komputerów osobistych (lub serwerów). Wszelkie niezatwierdzone połączenia lub nielegalne punkty dostępu będą odłączane, a sprzęt osobisty będzie musiał być natychmiast usunięty z obiektu.

We wszystkich obiektach Woodward należy zainstalować bezprzewodowe czujniki wykrywania włamań (WIDS) w celu monitorowania sieci pod kątem niezatwierdzonych punktów dostępu i nielegalnych sieci WLAN.

Konfiguracja punktów dostępowych wykorzystuje unikalną Nazwę Sieci (identyfikator zestawu usług SSID), która jest inna od wszelkich nazw domeny Woodward. Lokalizacja wszystkich Punktów Dostępowych podlega ocenie, tak aby poziom zasięgu poza obiektem był akceptowalny dla Działów Globalnej Infrastruktury IT i Globalnego Bezpieczeństwa, Ryzyka i Zgodności IT. Co więcej, Dział Globalnej Infrastruktury IT oceni proponowane instalacje, aby określić, czy należy zainstalować zaporę sieciową pomiędzy Punktami Dostępu a wewnętrzną siecią LAN oraz aby zweryfikować, że wszystkie ustawienia domyślne (np. hasło administratora) zostały zmienione.

Wszystkie karty interfejsu sieci są skonfigurowane pod kątem WPA2 lub wyższego poziomu autentykacji w sieci, przy czym szyfrowanie danych TKIP oraz autentykacja użytkownika EAP (PEAP) stanowią minimalne wymagania. ID i hasła użytkowników będą zatwierdzane w Active Directory poprzez serwery uwierzytelniania Radius, niemniej w przypadku niektórych instalacji może być wymagana bardziej rygorystyczna identyfikacja w zależności od ryzyka. Jedynie urządzenia (laptopy, smartfony, tablety), które stanowią element domeny Woodward, mogą nawiązywać połączenia z wewnętrzną siecią LAN Woodward poprzez bezprzewodowe punkty dostępu.

Urządzenia mobilne, takie jak smartfony i tablety mogą nawiązywać połączenia z Internetem poprzez bezprzewodową sieć WLAN, przeznaczoną do użytku przez pracowników Woodward. Wykorzystanie tej sieci WLAN nie obejmuje dostępu do wewnętrznej sieci Woodward. Połączenia mogą być nawiązywane jedynie za pomocą zatwierdzonych urządzeń. Grupa ta może obejmować urządzenia stanowiące prywatną własność pracowników, wykorzystywane w ramach programu „Przynieś Swoje Własne Urządzenie” (Bring Your Own Device - BYOD).

Z myślą o upoważnionych gościach, którzy nie muszą uzyskiwać dostępu do wewnętrznej sieci Woodward, może zostać zapewniona oddzielna sieć bezprzewodowa LAN dla gości. Nawiązywanie jednoczesnych połączeń z dowolną siecią WLAN dla gości i sieciami przewodowymi i bezprzewodowymi LAN jest zabronione. Wnioski o ustanowienie bezprzewodowych kont dla gości muszą być składane przez pracowników Woodward poprzez system wniosków o świadczenie usług IT (IT Service Request System).

5.9 Kopie zapasowe (pamięć flash ROM, konfiguracje przełącznika/rutera, linie ISDN)

Każda siedziba powinna posiadać udokumentowaną procedurę plików przywracania konfiguracji na lokalnych urządzeniach komunikacyjnych. Jeżeli pliki przechowywane

są w udziale sieciowym, udział ten musi być uwzględniony w harmonogramie wykonywania kopii zapasowych danej siedziby. Informacje w formie wydruku powinny być dostępne w przypadku niedostępności kopii elektronicznej.

Należy wprowadzić, a następnie przestrzegać regularnego harmonogramu testowania linii zapasowej WAN.

5.10 Filtrowanie zawartości i adresów URL

5.10.1 Adres IP, gniazda, blokowane porty

Filtry treści internetowych stosowane są zgodnie z zatwierdzoną listą usług i łączności. Filtrowanie można wykonać na serwerze proxy, bezpiecznym urządzeniu bramy stron internetowych lub urządzeniu końcowym. Zmiany wytycznych dotyczących kategorii filtrowania URL muszą zostać zatwierdzone przez Dział Globalnego Bezpieczeństwa, Ryzyka i Zgodności IT. Odstępstwa mogą być zatwierdzone przez Dział Globalnego Bezpieczeństwa, Ryzyka i Zgodności IT i muszą spełniać konkretne wymagania przypisane do poszczególnych osób, działów, biznesu lub ról, w tym otwierania konkretnych stron w celu uzyskania dostępu przez wszystkich pracowników, niezależnie od tego, czy zaakceptowali, czy też nie zaakceptowali dostępu do internetu.

Oprogramowaniem blokującym treści internetowe zarządza Dział Globalnej Infrastruktury IT. Wszystkie ustawienia zostały udokumentowane i przechowywane są w bezpiecznym miejscu.

5.10.2 Filtrowanie wiadomości-śmieci (spamu) i treści wiadomości mailowych

Technologia pozwalająca zmniejszyć ilość niechcianych, zainfekowanych wirusami lub obraźliwych wiadomości mailowych (spamu), napływających do sieci poprzez maile, zarządzana jest w obszarze bramy poczty elektronicznej przez Dział Globalnej Infrastruktury IT. Wiadomości mailowe poddane kwarantannie mogą być weryfikowane przez pracowników Działu Globalnej Infrastruktury IT lub Działu Globalnego Bezpieczeństwa, Ryzyka i Zgodności IT w celu zmniejszenia liczby niedostarczonych wiadomości mailowych, dotyczących spraw biznesowych, jak również ochrony urządzeń Woodward przed wirusami i złośliwym oprogramowaniem.

5.11 Skanowanie punktów newralgicznych

Wewnętrzne testowanie punktów newralgicznych planowane i prowadzone jest w regularnych odstępach czasu, zgodnie z Politykami OP 3-09-4158 (Skanowanie Punktów Newralgicznych i Proces Usuwania Luk). Właściciele systemów odpowiedzialni są za naprawę zidentyfikowanych punktów newralgicznych. Rezultaty będą weryfikowane, a działania związane ze zgodnością z procesem usuwania luk będą monitorowane przez Analityka IT ds. Bezpieczeństwa lub inne odpowiedzialne osoby z Działu Globalnej Infrastruktury IT.

5.12 Dokumentacja WAN/LAN

Dział Globalnej Infrastruktury IT będzie prowadzić dokumentację i przechowywać opisy topologii sieciowej i architektury bezpieczeństwa Woodward. Dział Globalnej Infrastruktury IT będzie również dokumentować i prowadzić wykaz przypisanych zakresów adresów IP.

6 Systemy poczty elektronicznej

Systemy poczty elektronicznej oraz wszystkie wiadomości generowane lub obsługiwane przez systemy poczty elektronicznej, w tym kopie zapasowe, uważane są za własność Woodward. Dyrektor Działu Globalnego Bezpieczeństwa, Ryzyka i Zgodności IT przynajmniej raz w roku kalendarzowym wysyłać będzie powiadomienie przypominające wszystkim pracownikom o prawach własności firmy w stosunku do systemu mailowego, prawie firmy do dostępu lub innego sposobu monitorowania systemu, jak również o fakcie ograniczenia prywatności pracowników, wynikającym z ww. działań.

Wszystkie wiadomości mailowe wychodzące z firmy muszą zawierać automatyczną notę o zachowaniu poufności.

6.1 Autentykacja

Uwierzytelnianie dostępu do systemu poczty elektronicznej spoza Woodward lub przy logowaniu przez VPN następuje za pomocą ID i hasła użytkownika. Pojedyncze logowanie tam, gdzie hasło sieci AD (Active Directory) pozwala na dostęp do poczty elektronicznej jest dopuszczalne, jednak użytkownikom wolno skonfigurować indywidualnych klientów poczty elektronicznej pod kątem żądania hasła. Zewnętrzny dostęp do systemu poczty elektronicznej przez OWA (Outlook Web Access) wymaga autentykacji dwuetapowej (np. tokena).

6.2 Ochrona przed włamaniami

Przywileje użytkowników i administratorów w systemach komunikacji elektronicznej muszą być przypisywane w sposób, który uwzględnia wyłącznie prawa konieczne do wykonywania obowiązków służbowych.

ID i hasło konta administratora usług przekazywane jest administratorom poczty elektronicznej zgodnie z polityką ścisłej potrzeby. Hasło jest zmieniane za każdym razem, gdy administrator poczty elektronicznej, który może znać hasło, kończy pracę w Woodward lub znajomość hasła nie jest mu już potrzebna do wykonywania obowiązków służbowych. Wszystkie ID administratorów, które mogą być wykorzystane w celu uzyskania dostępu do systemu operacyjnego lub systemu poczty elektronicznej, będą łączyć się z bezpiecznymi hasłami, zgodnie z definicją znajdującą się w sekcji poświęconej standardom haseł w dalszej części niniejszego dokumentu.

6.3 Dostęp fizyczny i administracyjny

Wszystkie serwery poczty elektronicznej we wszystkich siedzibach muszą mieścić się w pomieszczeniu zamykanym na klucz, do których dostęp został ograniczony do grupy upoważnionych osób. Dostęp do urządzeń globalnej bramy poczty

elektronicznej i repozytoriów filtrowania spamu/treści, jak również serwerów poczty elektronicznej w siedzibach zlokalizowanych w Stanach Zjednoczonych, będzie ograniczony do osób będących obywatelami Stanów Zjednoczonych lub posiadających Status Stałego Rezydenta. Ma to na celu zabezpieczenie danych ITAR przed nieumyślnym dostępem. Zarządzanie serwerami poczty elektronicznej w Unii Europejskiej będzie zgodne z krajowymi/unijnymi dyrektywami o ochronie prywatności. Dostęp do wszystkich serwerów poczty elektronicznej będzie ograniczony jedynie do osób odpowiedzialnych za zarządzanie serwerami i zapewnianie odpowiednich kopii zapasowych w przypadku nieobecności administratora.

7 Intranet/Internet

7.1 Sieć wewnętrzna (Intranet)

O ile nie zostało to wcześniej zatwierdzone przez Wiceprezesa ds. IT i jednoznacznie wskazane na stronie intranetowej, wszystkie treści tworzone przez pracowników Woodward i zamieszczane w intranecie Woodward (Inside Woodward) stanowią własność Woodward. Strony SharePoint mogą zawierać repozytoria dokumentów z informacjami referencyjnymi pochodzącymi z innych źródeł. Wszystkie zewnętrznie tworzone dokumenty muszą być wykorzystywane zgodnie z notą właściciela nt. praw autorskich.

W przypadku użytkowników, którzy posiadają konto na komputerze Woodward, pozwolenia domyślne dla intranetu zezwalają jedynie na dostęp w trybie „Tylko do odczytu”. Dostęp anonimowy oraz dostęp gości nie jest dopuszczony. Wszystkie osoby, które nie powinny mieć dostępu do Intranetu (np. konsultanci, partnerzy biznesowi, pracownicy przejściowi w ramach procesu zbytu itd.), powinny zostać dodane do grupy pozwoleń tam, gdzie aktywna jest opcja Brak dostępu.

Pozwolenia dla stron internetowych lub repozytoriów dokumentów na stronach globalnych lub stronach działów serwisu SharePoint mogą być ustanawiane przez właściciela danych lub przez Dział Globalnych Usług IT dla Klientów. Treści zamieszczane w serwisie SharePoint NIE MOGĄ zawierać danych ITAR, ePHI lub innych informacji zastrzeżonych, o ile nie zastosowano technologii zapobiegających nieumyślnemu dostępowi na skutek niewłaściwie przypisanych pozwoleń.

7.2 Sieć zewnętrzna (Internet)

Anonimowe FTP należy deaktywować. Anonimowe zamieszczanie plików zakazane jest w odniesieniu do wszystkich innych aplikacji przesyłających pliki.

Transfer informacji typu FTP musi być wykonywany za pomocą MoveIT DMZ (wsft), HTTPS, SSH, SSL lub innych bezpiecznych protokołów.

Wszystkie publicznie dostępne katalogi z funkcją zapisu w intranecie Woodward podlegają przeglądom i czyszczeniu przynajmniej raz w tygodniu. Następujące elementy zostaną natychmiast usunięte, niezależnie od tego, gdzie zostaną znalezione: oprogramowanie pirackie, ukradzione numery kard kredytowych, hasła oraz niestosowne materiały słowne lub graficzne (np. materiały pornograficzne).

Przesyłanie takiego rodzaju materiałów za pomocą komputerów lub zasobów firmy jest zakazane.

W przypadku katalogów zawierających informacje przechowywane dla celów współpracy z partnerami biznesowymi, prawnikami itp. należy stosować jakąś metodę dostępu uwierzytelnianego. Katalogi te nie będą podlegać rutynowemu przeglądowi i czyszczeniu, jednak podlegają takim samym ograniczeniom związanym z przechowywaniem niestosownych materiałów, chyba że stanowią dowód w procesie sądowym.

Woodward będzie rutynowo rejestrować odwiedzane strony internetowe, pobierane pliki, czas spędzany w internecie oraz powiązane informacje. Firma może uniemożliwić użytkownikom łączenie się z pewnymi stronami internetowymi, które nie posiadają natury biznesowej. Niemniej, ktokolwiek zorientuje się, że zostało nawiązane połączenie ze stroną, która zawiera jednoznacznie seksualne, rasistowskie, nacechowane przemocą lub potencjalnie obraźliwie materiały, musi natychmiast rozłączyć się z tą stroną. Możliwość wejścia na konkretną stronę nie oznacza, że użytkownikom wolno odwiedzać takie strony.

7.2.1 Nowe aplikacje i technologie

W miarę rozwoju nowych aplikacji i technologii, należy je starannie ocenić pod kątem konsekwencji związanych z bezpieczeństwem przed podjęciem decyzji o zatwierdzeniu dla użytku przez firmę. Przykładem mogą być aplikacje P2P (peer-to-peer). W sytuacji, w której korzyści biznesowe przewyższają stopień ryzyka, konfiguracje należy ustawić w sposób minimalizujący ryzyko do akceptowalnego poziomu. Należy również ustalić, czy aplikacja powinna być udostępniona wszystkim, czy też jedynie osobom potrzebującym oprogramowania do wykonywania obowiązków służbowych oraz czy wykorzystanie danego oprogramowania lub technologii wymaga zatwierdzenia przełożonego lub menedżera.

7.2.2 Technologie komunikacyjne

Z myślą o szybkiej wymianie nieformalnych wiadomości biznesowych, Woodward zapewnia dostęp do zatwierdzonego i bezpiecznego komunikatora internetowego, który pokazuje informacje o statusie pracowników. Komunikaty internetowe nie są rejestrowane i uwzględniane w kopiach zapasowych planu odtwarzania awaryjnego ani w harmonogramach retencji rejestrów. Na urządzeniach Woodward nie wolno instalować niezatwierdzonych Komunikatorów internetowych; jeżeli zostaną znalezione, konieczne będzie ich usunięcie. Komunikowanie się za pomocą Komunikatorów internetowych z zewnętrznymi klientami komunikatorów internetowych jest zakazane. Wszelkie odstępstwa od tej polityki muszą być rzadkie, potrzeba musi mieć charakter krytyczny, a wyjątkowe przypadki muszą zostać zatwierdzone przez przełożonego danego pracownika. Licencja pozwalająca zatwierdzonemu klientowi Woodward przejść przez bramkę internetową i nawiązać połączenie z klientem komunikatora internetowego nienależącym do Woodward, musi zostać przypisana przez Analityka ds. Zasobów, Licencji i Zgodności IT przed dopuszczeniem do nawiązania połączenia.

Dla potrzeb biznesowych firmy nie należy korzystać z usług telefonii internetowej, o ile oprogramowanie nie zostało ocenione przez IT pod kątem zgodności ze standardami bezpieczeństwa firmy. Natomiast dopuszczone jest stosowanie telefonów programowych wydawanych przez administratorów ds. telekomunikacji Woodward oraz korzystanie ze sprzętu i oprogramowania telekomunikacyjnego zatwierdzonego przez Woodward. Wszystkie przypadki Użytkowania telefonów programowych muszą być zgodne z wymaganiami E911 tam, gdzie ma to zastosowanie.

7.2.3 Przechowywanie informacji biznesowych poza siedzibą

Przechowywanie danych lub informacji firmy poza siedzibą lub w internecie, w tym przechowywanie list kontaktów, jest zabronione, o ile usługa nie jest świadczona przez zatwierdzonego przez IT dostawcę, partnera biznesowego lub instytucję finansową. Praktyki Woodward związane z przechowywaniem informacji muszą spełniać standardy Safe Harbor oraz być zgodne z przepisami UE w zakresie ochrony prywatności.

7.2.4 Niezatwierdzone aplikacje podmiotów niezależnych

Wykorzystywanie niezatwierdzonych aplikacji podmiotów niezależnych w celu uzyskiwania dostępu do wewnętrznych komputerów osobistych, serwerów lub innych urządzeń Woodward jest zabronione. Akceptacja konkretnych odstępstw musi zostać zatwierdzona przez Dyrektora Działu Globalnego Bezpieczeństwa, Ryzyka i Zgodności IT lub Dyrektora Działu Globalnej Infrastruktury IT. Przykład obejmują m.in. Go2MyPC oraz PCAnywhere.

7.2.5 Wykorzystanie dla celów niezwiązanych z biznesem

Wykorzystanie aplikacji przetwarzania rozproszonego dla celów niezwiązanych z biznesem jest zabronione. (Przykład: w ramach projektu SETI@Home pojedyncze komputery wykorzystywane są do przetwarzania fragmentów danych w celu oceny informacji używanych do szukania oznak życia pozaziemskiego.)

Zakładanie stron internetowych, elektronicznych tablic komunikacyjnych lub wszelkich innych mechanizmów, które zapewniają dostęp publiczny do serwerów lub części infrastruktury sieciowej firmy dla celów niezwiązanych z biznesem jest zabronione.

8 e-Biznes

8.1 Autentykacja

Autentykacja użytkowników odbywa się za pomocą ID i hasła użytkownika. Wymagania i standardy odnoszące się do haseł są takie same, jak w przypadku wszystkich innych ID i haseł użytkowników. Do jednego ID musi być przypisany jeden użytkownik; konta współdzielone lub grupowe nie są dopuszczalne.

Serwery wykorzystywane dla potrzeb autentykacji do systemów e-Biznes znajdują się w sieci prywatnej w celu zapobieżenia dostępu przez internet i wykorzystywane są wyłącznie do autentykacji, a nie wykonywania innych czynności.

8.2 Ochrona przed włamaniami

Wszystkie ID użytkowników systemów e-Biznes są weryfikowane przynajmniej raz w roku kalendarzowym przez przypisanych do nich osób poręczających ze strony Woodward. Analityk IT ds. Bezpieczeństwa zapewni wykaz IT osobom poręczającym.

Reakcja na wszelkie włamania lub próby włamań przebiegać będzie zgodnie z wytycznymi zawartymi w Planie Reakcji na Incydenty związane z Bezpieczeństwem Komputerów. Jeżeli zajdzie taka konieczność, wszystkie zagrożone ID użytkowników systemów e-Biznes będą usunięte i odtworzone.

Od dostawców/klientów wymaga się, aby w trybie natychmiastowym powiadomili Woodward o zakończeniu stosunku pracy danego pracownika posiadającego dostęp do systemu e-Biznes w celu dezaktywacji profilu użytkownika. Odpowiednia osoba ds. zakupów, rzecznik klientów, menedżer działu itp. odpowiedzialni są za poinformowanie swojego administratora sieci zarządzającego zewnętrznymi ID o konieczności natychmiastowej dezaktywacji tych kont.

Dostęp systemów e-Biznes do informacji Woodward kierowany jest przez zaporę sieciową.

8.3 Bezpieczeństwo aplikacji i danych

Stosowane są odpowiednie środki kontroli mające na celu zapewnienie, że wszystkie transakcje są przetwarzane zgodnie z autoryzacją, transakcje autoryzowane nie są pomijane, a transakcje nieautoryzowane nie są dodawane. Zmiany aplikacji e-Biznes podlegają pod system kontroli wersji, a przed wdrożeniem przechodzą testy.

8.4 Dostęp fizyczny

Każdy rodzaj sprzętu produkcyjnego powiązany z systemami e-Biznes musi znajdować się w pomieszczeniu zamykanym na klucz, do którego dostęp mają wyłącznie osoby upoważnione.

9 Centra danych i serwerownie (lokalizacja fizyczna)

Dla celów niniejszych polityk, centrum danych zostało zdefiniowane jako pokój, w którym umieszczono serwery i bazy danych systemów biznesowych. Przykłady systemów biznesowych obejmują m.in. systemy WISE i SAP. Mogą to być także inne serwery. Serwerownia jest zazwyczaj mniejsza i mieści serwery systemów niezwiązanych z biznesem. Przykłady takich serwerów obejmują m.in. serwery poczty elektronicznej, serwery stron internetowych, serwery telekomunikacyjne, serwery plików i wydruku. W uzupełnieniu do specyficznych wymagań przedstawionych w dalszej części niniejszego dokumentu, należy przestrzegać wszystkie wymagania Polityk dotyczących Bezpieczeństwa Fizycznego.

9.1 Zawartość centrum danych i serwerowni.

Wszystkie serwery produkcyjne, komputery systemów biznesowych oraz sprzęt krytyczny powinny mieścić się w centrum danych lub serwerowni lokalnej siedziby.

9.2 Systemy wspomagające i środowisko (klimatyzacja, UPS itd.)

Wszystkie serwery produkcyjne, komputery systemów biznesowych oraz sprzęt krytyczny muszą znajdować się w środowisku z kontrolowaną temperaturą powietrza oraz być podłączone do źródła zasilania rezerwowego. Źródłem tym może być generator zapasowy lub zasilacz uniwersalny UPS. Dyrektor Działu Globalnej Infrastruktury IT, w porozumieniu z lokalnym menedżerem siedziby, ma za zadanie określić, czy ryzyko zaniku zasilania uzasadnia wydatki związane z generatorem.

Wszystkie centra danych i serwerownie muszą być wyposażone w maty antystatyczne lub maty i nadające się do użycia gaśnice przeciwpożarowe. Instalacja systemów gaśniczych jest wymagana w odniesieniu do wszystkich centrów danych.

9.3 Dostęp fizyczny

Wszystkie centra danych i serwerownie muszą być zamknięte na klucz. W mniejszych biurach lub siedzibach nieposiadających dedykowanych centrów danych lub serwerowni, serwery należy umieścić w zamkniętym miejscu, np. klatce lub szafce. Dostęp do wszelkich centrów danych z serwerami systemów biznesowych i bazami danych musi być ograniczony jedynie do osób posiadających identyfikator. Drzwi nie wolno zostawiać uchylonych bez nadzoru i zabezpieczeń. Pomieszczenia, w których znajdują się serwery telekomunikacyjne lub serwery poczty głosowej muszą spełniać takie same standardy, które obowiązują w przypadku serwerowni.

Ciągły niekontrolowany dostęp dozwolony jest wyłącznie w przypadku osób związanych z IT, obiektami lub bezpieczeństwem (np. pracowników ochrony), które muszą przebywać w centrum danych lub w serwerowni w ramach wykonywania swoich obowiązków służbowych. Jeżeli osoby z innych działów mają potrzebę uzyskania niekontrolowanego dostępu, muszą podpisać dokument zawierający akceptację odpowiedzialności, przekazany im przez Dyrektora Działu Globalnej Infrastruktury IT lub Dyrektora Działu Globalnego Bezpieczeństwa, Ryzyka i Zgodności IT.

Dyrektor Działu Globalnej Infrastruktury musi zatwierdzić nazwiska wszystkich osób, którym przyznano dostęp do centrów danych w Rockford, FTC, Skokie lub Santa Clarita. (Dostęp do centrum danych oznacza każdą osobę, która może uzyskać dostęp do centrum danych lub serwerowni bez konieczności umożliwiania jej dostępu przez inną osobę. Obejmuje to m.in. dostęp z identyfikatorem, dostęp za pomocą klucza, dostęp za pomocą klucza głównego, dostęp biometryczny itd.). Przynajmniej raz w roku Menedżer ds. Infrastruktury IT przygotuje dla potrzeb weryfikacji przez Dyrektora Działu Globalnego Bezpieczeństwa, Ryzyka i Zgodności IT wykaz nazwisk osób, które posiadają dostęp do centrum danych/serwerowni w Skokie, Santa Clarita i Rockford. Po zakończeniu procesu weryfikacji, wykaz osób posiadających zatwierdzony dostęp do centrum danych musi zostać przekazany osobom odpowiedzialnym za bezpieczeństwo w każdym obiekcie.

Przy każdym centrum danych, w którym znajdują się serwery i bazy danych systemów biznesowych, należy umieścić dziennik osób odwiedzających. Nazwiska wszystkich odwiedzających należy zapisywać na specjalnym arkuszu umożliwiającym złożenie podpisu, a osoba towarzysząca musi zameldować i wymeldować każdego gościa. Szczegółowe procedury zostały zawarte w OP 692.

10 Komputery systemów biznesowych

Komputery systemów biznesowych obejmują m.in. serwery hostujące systemy WISE, Lawson, Oracle GL oraz SAP.

10.1 Autentykacja

Autentykacja do aplikacji systemów biznesowych odbywa się za pomocą ID i hasła użytkownika.

10.2 Ochrona przed włamaniami

Serwery należy konfigurować w sposób, aby dostęp do usług, oprogramowania i plików zastrzeżonych przypisany był jedynie do osób mających prawo do ich Użytkowania.

Liczba osób posiadających pozwolenia „root" jest ograniczona do minimum. Hasło Super użytkownika znają jedynie osoby, które bezwzględnie muszą je znać. Nikt (za wyjątkiem Super użytkownika) nie jest w stanie zapisywać do plików będących własnością „root". Możliwość uruchamiania skryptów w ustawionym trybie ID użytkownika ograniczona jest jedynie do osób, które muszą uruchomić konkretny skrypt. Hasła Super użytkownika zmieniane są przynajmniej raz na sześć (6) miesięcy.

10.3 Aplikacja, bezpieczeństwo danych

Należy zastosować odpowiednie środki kontroli, aby zapewnić, że wszystkie transakcje WISE, Oracle GL, SAP oraz transakcje innych systemów biznesowych są przetwarzane zgodnie z autoryzacją, że żadna autoryzowana transakcja nie zostanie pominięta, a transakcje nieautoryzowane nie będą dodawane.

Autoryzacja dostępu administracyjnego do tych serwerów podlega zatwierdzeniu i rejestrowana jest w dokumentacji Procesu weryfikacji dostępu dla administratorów IT.

Zmiany WISE, EDI, systemów e-Biznes, aplikacji webowych intranetu, Lawson, Oracle GL i SAP wprowadzane są zgodnie z Politykami OP-576 i testowane przed wdrożeniem.

11 Serwery

Kategoria ta obejmuje wszystkie typy serwerów, w tym m.in. serwery aplikacji, plików, wydruku, baz danych, komunikacji elektronicznej, poczty głosowej oraz serwery wirtualne. Kategoria obejmuje też wszystkie systemy operacyjne. Uwzględnione zostały również systemy przestarzałe i specjalistyczne, np. EDI, Caferetia itd.

11.1 Autentykacja

Autentykacja odbywa się za pomocą ID i hasła użytkownika.

11.2 Ochrona przed włamaniami

Serwery należy konfigurować w sposób, aby dostęp do usług, oprogramowania i plików zastrzeżonych przypisany był jedynie do osób mających prawo do ich Użytkowania.

Pozwolenia lokalnego administratora ograniczone są do osób, które potrzebują takiego dostępu w związku z wykonywaną przez siebie pracą. Pozwolenia dla użytkowników zaawansowanych oraz inne ograniczone pozwolenia stosowane są dla potrzeb wsparcia pracowników tam, gdzie jest to możliwe.

Nieaktywne konsole są blokowane.

12 Systemy stacjonarne/Stacje robocze

12.1 Autentykacja

Uwierzytelnianie do sieci z obiektu Woodward odbywa się za pomocą ID i hasła użytkownika.

12.2 Ochrona przed włamaniami

Informacje poufne i krytyczne dla biznesu nie mogą być przechowywane na niezabezpieczonych komputerach osobistych lub stacjach roboczych. W sytuacji, w której aplikacje lub dane poufne lub krytyczne dla biznesu znajdują się na komputerze osobistym lub stacji roboczej, wymaga się, aby komputer był umieszczony w pomieszczeniu zamykanym na klucz, posiadał hasło bios lub system operacyjny, który wymaga użycia hasła przy uruchomieniu. Dopuszczalnym alternatywnym rozwiązaniem jest szyfrowanie, które wymaga użycia hasła przy uruchomieniu.

Od wszystkich użytkowników komputerów wymaga się, aby wylogowywali się z sieci i wszystkich systemów komputerowych w momencie opuszczania swojego miejsca pracy lub stosowali wygaszacz ekranu z funkcją auto wyłączania, która zapewnia ochronę za pomocą hasła. Wygaszaczy ekranu z funkcją auto wyłączania nie wolno deaktywować, a konfiguracji wygaszacza ustawiać na „żaden” na jakimkolwiek komputerze używanym do uzyskiwania dostępu do dowolnego rodzaju informacji zastrzeżonych lub poufnych, w tym m.in. danych e-PHI lub ITAR.

12.3 Zarządzanie zasobami

Komputerów nabiurkowych i stacji roboczych nie wolno wynosić poza obiekty Woodward bez pozwolenia menedżera działu danego pracownika. Menedżer działu odpowiedzialny jest za powiadomienie Działu Personalnego o fakcie konieczności odzyskania takiego sprzętu za każdym razem, gdy miejsce ma rozwiązanie umowy o pracę z danym pracownikiem.

13 Urządzenia mobilne

Niniejsza sekcja poświęcona jest laptopom, tabletom, smartfonom, telefonom komórkowym z dostępem do internetu i wszelkim innym urządzeniom mobilnym wykorzystywanym do przechowywania lub przekazywania danych. Połączenie z systemami i zasobami informatycznymi Woodward mogą nawiązywać jedynie urządzenia będące własnością Woodward lub zarządzane przez Woodward urządzenia prywatne. W celu skorzystania z prywatnego urządzenia mobilnego (takiego jak smartfon czy tablet) z myślą o uzyskaniu dostępu do poczty elektronicznej lub informacji Woodward, użytkownik musi podpisać Umowę o wykorzystaniu urządzeń mobilnych, a urządzenie musi być zarządzane poprzez BlackBerry Enterprise Server (BES) lub rozwiązanie Mobile Device Management (MDM). Urządzenia prywatne, za pomocą których uzyskiwany jest dostęp do informacji Woodward, muszą spełniać takie same standardy bezpieczeństwa, jakie spełniają urządzenia należące do Woodward.

13.1 Autentykacja

Uwierzytelnianie do wewnętrznej sieci Woodward następuje za pomocą ID i hasła użytkownika lub tokena autentykacji dwuetapowej, w zależności od tego, czy urządzenie nawiązuje połączenie z obiektu Woodward lub z zewnątrz.

Autentykacja urządzeń takich jak smartfony, urządzenia BlackBerry, iPhone, iPad i tablety, które nie są elementami domeny Woodward, obsługiwana jest przez BlackBerry Enterprise Server lub rozwiązanie Mobile Device Management. Dotyczy to zarówno urządzeń należących do Woodward, jak i zatwierdzonych urządzeń prywatnych.

13.2 Ochrona przed włamaniami

Wszystkie laptopy muszą być zaszyfrowane za pomocą oprogramowania, które wymaga hasła, aby osoby nieuprawnione nie mogły uzyskać dostępu do folderów poczty elektronicznej offline lub plików przechowywanych na lokalnych dyskach laptopów. Hasła muszą składać się z minimum 14 znaków. Haseł nie wolno przyklejać do urządzeń, przechowywać w teczce służącej do przenoszenia urządzenia i/lub umieszczać w jego pobliżu. Ze względu na fakt, że użytkownik musi mieć dostęp do urządzenia i znać dane służące do uwierzytelniania, hasła nie muszą być zmieniane, chyba że pracownik lub Dział Globalnych Usług IT uznają, że hasło jest zagrożone.

Wymagane jest, aby na wszystkich laptopach zainstalowany był hostowy system wykrywania i zapobiegania atakom (HIPS). Na wszystkich komputerach używanych do uzyskiwania dostępu do dowolnego rodzaju informacji zastrzeżonych lub poufnych

muszą być stosowane wygaszacze ekranu z funkcją auto wygaszania. Ustawienia wygaszacza nie mogę być skonfigurowane na „żaden".

Wszystkie bezprzewodowe połączenia z urządzeń mobilnych z siecią wewnętrzna Woodward muszą być szyfrowane.

Smartfony, urządzenia BlackBerry oraz tablety muszą być skonfigurowane w sposób, który wymaga od użytkowników wprowadzenia kodu bezpieczeństwa lub hasła przy uruchamianiu urządzenia. Hasła i kody dostępu do oprogramowania lub sprzętu nie powinny być „zapisywane" w sposób umożliwiający osobom nieuprawnionym uzyskanie dostępu do informacji przechowywanych w sieci lub na lokalnym urządzeniu.

Wszystkie urządzenia mobilne uzyskujące dostęp do sieci Woodward należy skonfigurować w sposób, który daje możliwość zdalnego usunięcia informacji firmy z urządzenia, jeżeli zostanie ono skradzione lub stosunek pracy z pracownikiem używającym tego urządzenia zostanie rozwiązany. W tych okolicznościach Woodward przysługuje prawo do usunięcia danych z urządzeń; Woodward nie ponosi odpowiedzialności za dane usunięte w sposób nieumyślny. Pracownicy powinni mieć świadomość, że przechowywanie informacji firmy na prywatnych urządzeniach mobilnych lub nośnikach danych może skutkować tym, że urządzenie będzie podlegać wymogom ujawnienia w trakcie lub w oczekiwaniu na postępowanie sądowe.

Informacje poufne, w tym hasła do systemów komputerowych Woodward, numery kart telefonicznych, numery kontraktów, informacje zastrzeżone, dane finansowe itp. nie powinny być przechowywane na urządzeniach mobilnych, chyba że informacje te chronione są za pomocą oprogramowania umożliwiającego ochronę hasłem i szyfrowanie.

13.3 Zarządzanie zasobami

Menedżer działu odpowiedzialny jest za utrzymanie rejestru wszystkich urządzeń BlackBerry, iPhone/iPad, laptopów i innych urządzeń mobilnych używanych przez pracowników zarządzanych przez siebie działów, które mogą być rutynowo wynoszone poza obiekty Woodward. Jeżeli ktoś korzysta z urządzenia mobilnego i nie jest już pracownikiem firmy, menedżer działu odpowiada za powiadomienie Działu Personalnego, że urządzenia, które mogą zawierać informacje tajne, poufne lub zastrzeżone, muszą być odzyskane od byłego pracownika.

Aby zapobiec nieuprawnionemu ujawnieniu, wszystkie osoby znajdujące się w posiadaniu urządzeń mobilnych zawierających foldery poczty elektronicznej offline lub informacje tajne, poufne lub zastrzeżone, powinny stosować takie same środki ostrożności chroniące urządzenia mobilne, jakie stosowaliby do ochrony swoich portfeli lub torebek. Nadawanie urządzeń wraz z bagażem rejestrowanym, pozostawianie ich w systemach bagażowych linii lotniczych, schowkach w autobusach, u portierów hotelowych itp. nie jest dozwolone.

Wszystkie laptopy, urządzenia BlackBerry, iPad/iPhone oraz wszelkie inne urządzenia mobilne powinny być rozpoznawalne w prosty sposób, aby ułatwić ich odzyskanie w przypadku, w którym bardziej prawdopodobne było ich zgubienie, a nie kradzież. Na

urządzeniu powinny zostać umieszczone nazwa i numer telefonu firmy lub urządzenie powinno być skonfigurowane w sposób wyświetlający nazwisko użytkownika i jego informacje kontaktowe.

14 Kopie zapasowe i utrzymanie (serwery, aplikacje, bazy danych itd.)

W celu ochrony informacji Woodward przechowywanych elektronicznie przed utratą lub zniszczeniem, istnieje wymóg rejestrowania, kopiowania i przechowywania zasobów elektronicznych Woodward w bezpieczny sposób. Polityka Woodward dotyczące tworzenia kopii zapasowych mają na celu zapewnienie ciągłości działania w przypadku awarii całego systemu lub fabryki. Kopie zapasowe są również metodą przywracania informacji, które zostały usunięte w sposób przypadkowy lub celowy (w czasie cyklu życia nośnika kopii zapasowej). Termin „kopia zapasowa" może odnosić się do taśmy lub innego stosowanego nośnika kopii zapasowej. Systemy zapasowe Woodward nie mogą być używane dla celów rutynowej retencji dokumentacji.

14.1 Kopie zapasowe

Dział Globalnej Infrastruktury IT odpowiedzialny jest za udokumentowanie szczegółowych wymagań i procedur dotyczących tworzenia kopii zapasowych i przywracania danych w ramach oficjalnych Procedur Operacyjnych, zgodnych z wymaganiami przedstawionymi w niniejszym dokumencie.

Wszystkie nośniki kopii zapasowych zawierające elektronicznie chronione informacje zdrowotne (ePHI) lub innego rodzaju informacje o wysokim stopniu wrażliwości lub poufności, muszą być szyfrowane. Obejmuje to m.in. informacje finansowe, własność intelektualną oraz dane ITAR.

Nośniki kopii zapasowych muszą być jasno i wyraźnie opisane lub oznaczone kodami kreskowymi w celu łatwej identyfikacji daty i zawartości. Po zapisaniu nośnika, nie wolno go zostawiać bez nadzoru, o ile nie będzie przechowywany w zamykanej na klucz szafce lub pomieszczeniu.

14.1.1 Serwery aplikacji biznesowych (WISE, SAP AIX itd.)

Wszystkie dane, w tym baza danych WISE, będą kopiowane i zabezpieczane przynajmniej pięć (5) dni w tygodniu. Roczna, pełna kopia zapasowa bazy danych wykonywana jest pod koniec każdego roku finansowego. Roczna kopia zapasowa nie będzie wykonywana pod koniec każdego roku kalendarzowego.

Systemy SAP, AIC i WISE wykorzystują „progresywną" metodologię tworzenia kopii zapasowych, opartą na liczbie przeglądów pliku w miejsce dat. Kopia zapasowa wykonywana jest po pierwszym wdrożeniu.

Kolejne kopie zapasowe mają charakter przyrostowy i obejmują wszystkie pliki, które uległy zmianie od wykonania ostatniej pełnej kopii. Oprogramowanie przechowuje wcześniej ustawioną liczbę wersji każdego pliku. Najnowsza kopia każdego aktywnego pliku będzie znajdować się na nośniku kopii zapasowej, ale w zależności od częstotliwości dokonywania zmian, mogą (lub nie) istnieć wcześniejsze wersje pliku dostępne do odzyskania.

Kopie zapasowe usuniętych plików użytkownika przechowywane są przez minimum dwadzieścia jeden (21) dni i maksimum dziewięćdziesiąt (90) dni po usunięciu. Wcześniejsze wersje plików przechowywane są przez około trzydzieści (30) dni od daty dokonania przeglądu.

Kopie zapasowe usuniętych plików bazy danych WISE przechowywane są przez minimum dwadzieścia jeden (21) dni i maksimum dziewięćdziesiąt (90) dni po usunięciu. Wcześniejsze wersje są również przechowywane przez dwadzieścia jeden (21) do dziewięćdziesięciu (90) dni od daty dokonania przeglądu.

W miarę „starzenia się" plików w systemie, następuje ich usuwanie z bazy danych oprogramowania kopii zapasowych; odzyskanie ich staje się niemożliwe. Jest to nieodłączny element sposobu funkcjonowania oprogramowania progresywnych kopii zapasowych. Kiedy na nośniku kopii zapasowych znajduje się mniej niż 25% aktywnych plików, oprogramowanie utworzy zapis skonsolidowany i „wycofa" stare pliki. Przestrzeń ta może być następnie wykorzystana dla potrzeb nowych kopii zapasowych.

Należy podjąć decyzję i udokumentować ją w procedurach operacyjnych dotyczących kopii zapasowych odnośnie tego, czy jakiekolwiek serwery aplikacji Woodward w trakcie nabywania lub wdrażania będą podlegać podobnym procedurom lub czy należy przyjąć procedurę związaną z serwerami plików i aplikacji. Decyzja zależna jest od tego, czy wybrano progresywny, czy też bardziej tradycyjny system tworzenia kopii zapasowych.

Administrator każdego systemu odpowiedzialny jest za udokumentowanie harmonogramu wykonywania kopii zapasowych, procedury rotacji nośników oraz szczegółowej procedury tworzenia kopii zapasowych i procesu odzyskiwania.

14.1.2 Pliki, aplikacje, e-Biznes, archiwum poczty elektronicznej i serwery wydruku

Kopia zapasowa systemu operacyjnego każdego serwera wykonywana jest natychmiast po postawieniu serwera. Dodatkowo, nowa kopia zapasowa wykonywana jest po wprowadzeniu znaczących zmian do systemu operacyjnego.

Pełne kopie zapasowe krytycznych dla biznesu informacji, aplikacji, rysunków itp., wykonywane są przynajmniej raz w tygodniu. Przyrostowe kopie zapasowe są wykonywane każdego dnia w przypadku gdy pełna kopia nie jest zaplanowana.

Każdy Dział IT odpowiedzialny jest za udokumentowanie i publikację harmonogramu kopii zapasowych dla wszystkich serwerów, za które ponosi odpowiedzialność. Harmonogram kopii zapasowych obejmuje pełne i przyrostowe kopie, aby zapewnić, że wszystkie dane znajdujące się na serwerach Woodward są odpowiednio zabezpieczone, a informacje mogą zostać odzyskane w trakcie działań podejmowanych w ramach Odtwarzania Awaryjnego.

14.1.3 Poczta elektroniczna

Oprogramowanie archiwizacji poczty elektronicznej stanowić będzie główną metodę dla poszczególnych skrzynek pocztowych we wszystkich miejscach, gdzie wdrażana jest archiwizacja. Tam, gdzie to możliwe, archiwizacja zastąpi kopie zapasowe krytycznych, indywidualnych skrzynek pocztowych.

14.2 Utrzymanie

14.2.1 Kopie zapasowe systemów operacyjnych dla nowych lub zaktualizowanych konstrukcji

Nośniki kopii zapasowych, które zawierają wyłącznie System Operacyjny serwera, mogą być przechowywane przez czas nieokreślony.

14.2.2 Dokumenty istotne z punktu widzenia postępowania prawnego

Informacje podlegające wymaganiom dotyczącym przechowywaniu dokumentów istotnych z punktu widzenia postępowania prawnego są zwolnione z obowiązku zgodności z Polityką Retencji – dopóki Istotny Dokument nie zostanie usunięty przez Generalnego Radcę Prawnego Woodward lub wyznaczonego pracownika Działu Prawnego Woodward. Analityk ds. Programu Retencji Rejestrów będzie utrzymywać wykaz pracowników włączanych do powiadomień związanych z Istotnymi Dokumentami wysyłanymi do Działu IT przez Dział Prawny Woodward.

14.2.3 Systemy biznesowe (WISE, SAP itd.)

Kopie zapasowe systemów biznesowych powinny być przechowywane w następujący sposób: Kopię wszystkich progresywnych kopii zapasowych należy przechowywać poza siedzibą. Kiedy kopie zapasowe zostaną skonsolidowane, a nośniki nie będą dłużej potrzebne dla celów odzyskiwania, nośniki zostaną zwrócone Woodward do ponownego Użytkowania. Jeżeli Cincom lub inne oprogramowanie systemów biznesowych zakupione przez Woodward wykorzystywać będzie bardziej tradycyjny system zapasowy, stosowane będę takie same okresy retencji, jak te stosowane dla potrzeb serwerów plików, aplikacji i wydruku.

Pod koniec każdego roku finansowego należy wykonać pełną kopię zapasową, która następnie ma być przechowywana przez dwa (2) lata. Wszystkie nieaktywne nośniki zostaną ponownie wykorzystane w ciągu dwóch (2) lat; w innym przypadku należy wymazać ich zawartość lub je zniszczyć.

14.2.4 Nośniki kopii zapasowych dla plików, aplikacji, systemów e-Biznes, archiwum poczty elektronicznej, poczty głosowej i serwerów wydruku

Nośniki kopii zapasowych serwerów plików, aplikacji, systemów e-biznes, poczty głosowej, archiwum poczty elektronicznej i wydruku będą przechowywane przez minimum piętnaście (15) miesięcy oraz maksimum dwa (2) lata. Polityka retencji dokumentów należą do zakresu obowiązków

jednostki biznesowej; należy unikać zależności od dostępności nośników kopii zapasowych.

14.2.5 Baza danych Exchange

Kopie zapasowe bazy danych Exchange, w której wdrożono proces archiwizacji, będą przechowywane przez minimum czternaście (14) dni i maksimum dwa (2) lata. Kopie zapasowe tego typu wymagane są jedynie dla potrzeb odtwarzania awaryjnego. Archiwum zapewnia dodatkowe funkcje odtwarzania awaryjnego i odzyskiwania zależnego od poziomu elementu. Siedziby nieposiadające rozwiązania archiwizującego muszą przestrzegać okresów retencyjnych dla serwerów plików i aplikacji.

14.2.6 Przechowywanie w siedzibie i poza siedzibą

Wszystkie nośniki kopii zapasowych należy jasno opisać i przechowywać w bezpieczny sposób w siedzibie przez okres jednego (1) tygodnia lub krótszy, a następnie przenieść do bezpiecznego miejsca poza siedzibą, zgodnie z Procedurami Operacyjnymi dotyczącymi Kopii Zapasowych, udokumentowanymi przez Dział Infrastruktury IT. W zewnętrznym centrum przechowywania zawsze powinny być dostępne minimum dwie (2) pełne kopie zapasowe. Każda siedziba odpowiedzialna jest za wybór bezpiecznego centrum przechowywania, znajdującego się przynajmniej w odległości dziewięciu (9) km od miejsca, w którym taśmy przechowywane są na terenie obiektu Woodward. Taśmy wracające z zewnętrznego centrum przechowywania powinny być zabezpieczone do momentu ponownego Użytkowania lub zniszczenia. Transport taśm kopii zapasowych z/do zewnętrznego centrum przechowywania powinien odbywać się w zamkniętej walizce.

14.3 Urządzenia nieuwzględnione w procesach tworzenia kopii zapasowych przez Dział IT

Dział IT nie tworzy kopii zapasowych komputerów osobistych, laptopów, urządzeń mobilnych, smartfonów ani wymiennych urządzeń magazynujących klientów. Dział Globalnego Bezpieczeństwa, Ryzyka i Zgodności IT odpowiedzialny jest za coroczne informowanie użytkowników, że kopie wszystkich informacji krytycznych dla biznesu, znajdujące się na urządzeniach klientów i urządzeniach mobilnych nie są tworzone, a kopia powinna być przechowywana na serwerze sieciowym, tak aby mogła zostać włączona do procesu tworzenia kopii zapasowej serwera.

Jeżeli pracownik IT ma świadomość lub podejrzewa, że informacje krytyczne dla biznesu są przechowywane na twardym dysku komputera osobistego i w żaden sposób nie mogą zostać skopiowane do sieci, Dział IT odpowiedzialny jest za udzielenie pracownikowi pomocy w kwestii konfiguracji alternatywnego rozwiązania związanego z tworzeniem kopii zapasowej.

Nośniki kopii zapasowych muszą być jasno i czytelnie opisane, tak aby znajdujące się na nich daty i treści były łatwe do zidentyfikowania. Jeżeli nośnik został zapisany, nigdy nie powinien być pozostawiany bez nadzoru, chyba że przechowywany jest w

zamykanej na klucz szufladzie, szafce lub pomieszczeniu. Jeżeli nośnik nie jest już potrzebny, powinien zostać zniszczony w bezpieczny sposób.

15 Odtwarzanie awaryjne

Każda siedziba powinna posiadać udokumentowany Plan Odtwarzania Awaryjnego, który należy poddawać corocznej weryfikacji. Pracownicy Działu Globalnego Bezpieczeństwa, Ryzyka i Zgodności IT oraz lokalni pracownicy IT odpowiedzialni są za zapewnienie, że Plany Odtwarzania Awaryjnego znajdują się we wszystkich siedzibach.

15.1 Plany odtwarzania awaryjnego

Wszystkie siedziby Woodward powinny posiadać udokumentowany Plan Odtwarzania Awaryjnego, który obejmuje zastąpienie serwera, procedury oraz ocenę długości okresu potrzebnego na odzyskanie danych.

Dokumentacja sporządzona przez administratora systemu powinna zawierać informacje na temat zakresu utraconych danych, który miałby miejsce, jeżeli awaria wymagałaby przywrócenia z nośników kopii zapasowych przechowywanych poza obiektem. Wiceprezes ds. IT odpowiedzialny jest za zapewnienie, że potencjalna ilość utraconych danych oraz udokumentowane zakłócenia są akceptowalne z biznesowego punktu widzenia.

Każdy rodzaj oprogramowania koniecznego do odbudowy serwera lub reinstalacji aplikacji, usług lub systemu operacyjnego powinien być przechowywany razem w bezpiecznym miejscu, np. w obiektach firmy specjalizującej się w przechowywaniu taśm kopii zapasowych, innym obiekcie Woodward lub w banku. Co więcej, inna kopia powinna być przechowywana w bezpiecznym miejscu, poza siedzibą lub w siedzibie w sejfie odpornym na działanie ognia.

Każda fabryka musi posiadać udokumentowaną procedurę przechowywania poza obiektem. Nośnik kopii zapasowych lub kopia nośnika zapasowego muszą być przechowywane poza siedzibą w bezpiecznym miejscu. Miejsce to musi znajdować się w odległości przynajmniej dziewięciu (9) km od obiektu, aby zmniejszyć ryzyko narażenia na skutki tej samej katastrofy.

Plan Odtwarzania Awaryjnego obejmować będzie serwery, w tym serwery aplikacji, wydruku, baz danych, poczty głosowej, komunikacji elektronicznej i plików. Do grupy tej należą również wszystkie stacje robocze oraz komputery osobiste zawierające informacje medyczne, objęte przepisami HIPAA. Systemy operacyjne obejmują m.in. Windows, AIX, Linux i UNIX. Krytyczne dla biznesu zapisy lub systemy specjalistyczne takie jak EDI, Cafeteria itp. powinny również zostać włączone do tego procesu.

Każda siedziba powinna posiadać udokumentowaną i przetestowaną procedurę związaną z zewnętrznym przechowywaniem ustawień konfiguracji krytycznego sprzętu dla dowolnego sprzętu LAN, np. koncentratorów, przełączników lub ruterów, zlokalizowanych w siedzibie.

15.2 Plany centrów danych systemów biznesowych

Wszystkie postanowienia sekcji dedykowanej Odtwarzaniu Awaryjnemu dotyczą siedzib z Systemami Biznesowymi (WISE, SAP, Lawson), jak również następujących postanowień dodatkowych.

Dyrektor Działu Globalnej Infrastruktury IT oraz Dyrektor Działu Globalnego Bezpieczeństwa, Ryzyka i Zgodności IT odpowiedzialni są za udokumentowanie kompleksowego Planu Odtwarzania Awaryjnego systemów biznesowych dla centrów danych. Plan ten powinien uwzględniać postanowienia dotyczące wymiany sprzętu, przechowywania danych i linii komunikacyjnych i, o ile to konieczne, przeniesienia do alternatywnego obiektu. Kontrakty dotyczące usług przechowywania zewnętrznego powinny znajdować się w każdej siedzibie, w której stosowane są systemy biznesowe (WISE, SAP, Lawson).

W przypadku niedostępności wersji elektronicznej Planu Odtwarzania Awaryjnego należy posiadać wersję drukowaną. Personel mający krytyczne znaczenie dla biznesu powinien otrzymać kopie Planu Odtwarzania Awaryjnego oraz informacje nt. komunikacji awaryjnej, które mają być przechowywane poza siedzibą w miejscach dostępnych dla tych pracowników. Wydruki należy aktualizować i przygotowywać do kontroli wersji.

15.3 Utrzymanie i testowanie planów odtwarzania awaryjnego

15.3.1 Weryfikacja i aktualizacja planów

Wszystkie Plany Odtwarzania Awaryjnego powinny podlegać corocznym przeglądom i aktualizacjom. Dział Globalnego Bezpieczeństwa, Ryzyka i Zgodności IT ma za zadanie zagwarantować, że wszystkie plany są zaktualizowane. Odpowiedzialność za aktualizację planów ponoszą lokalni pracownicy IT i Działu Globalnej Infrastruktury IT.

15.3.2 Testowanie centrum danych w Rockford

Zdolność firmy do przywrócenia danych systemów biznesowych i bram krytycznej infrastruktury poczty elektronicznej w zakontraktowanym obiekcie odzyskiwania powinna być testowana nie rzadziej niż corocznie w ramach odwiedzin obiektu i przywracania danych. Wymóg ten może również dotyczyć centrum danych w Skokie lub innych centrów, które Woodward może nabyć, jeśli (lub o ile) zawierają dane krytycznych systemów biznesowych.

15.3.3 Testowanie procesu odzyskiwania danych

Testy mające na celu zweryfikowanie, że nośniki kopii zapasowych w każdym lokalnym obiekcie mogą zostać odzyskane na sprzęcie zlokalizowanym w jednej lub więcej siedzibach Woodward, należy przeprowadzać raz w roku.

15.3.4 Testowanie scenariuszowe

Test oparty na scenariuszu, test symulacyjny lub test przeglądowy należy przeprowadzić w ciągu jednego (1) roku od utworzenia Planu Odtwarzania

Awaryjnego dla konkretnej siedziby. Podobne powtarzające się testy należy przeprowadzać dla potrzeb wszystkich siedzib Woodward w cyklu rotującym w ramach wszystkich obiektów, przy czym w skali roku należy wykonać minimum dwa (2) testy.

16 Działania prewencyjne i naprawcze

16.1 Ochrona przed wirusami, oprogramowaniem szpiegującym i oprogramowaniem złośliwym

Każdy oddział musi przestrzegać minimalne standardy firmy dotyczące skanowania antywirusowego i stosować się do procedur opisanych w Planie Woodward dotyczącym Ochrony i Reakcji na Wirusy. Plan ten jest weryfikowany i aktualizowany przynajmniej raz w roku przez Dział Globalnego Bezpieczeństwa, Ryzyka i Zgodności IT. Oprogramowanie skanowania antywirusowego oraz pliki definicji wirusów muszą być zawsze aktualne. Zainfekowane pliki należy wyczyścić, usunąć lub poddać kwarantannie.

Faksy, drukarki i inne urządzenia wielofunkcyjne podłączone do sieci Woodward mogą być narażone wirusy i inne ataki. Dział IT może odłączyć takie urządzenia od sieci wedle własnego uznania, jeżeli będą wywierać negatywny wpływ na działanie sieci lub bezpieczeństwo danych.

Oprogramowanie skanowania antywirusowego musi zostać zainstalowane i być aktywne na serwerach sieciowych, w tym na serwerach poczty elektronicznej. Oprogramowanie chroniące przed wirusami powinno być skonfigurowane w sposób umożliwiający skanowanie wszystkich dostępnych wiadomości.

Oprogramowanie skanowania antywirusowego musi skanować wiadomości pod kątem wirusów wchodzących do systemu poczty elektronicznej Woodward z Internetu.

Przychodzący ruch internetowy musi być skanowany pod kątem obecności wirusów.

Wszystkie stacje robocze, komputery nabiurkowe i laptopy muszą posiadać oprogramowanie antywirusowe, hostowe systemy wykrywania i zapobiegania atakom (HIPS) oraz oprogramowanie wykrywające programy szpiegujące.

Woodward zastrzega sobie prawo, aby wymagać obecność oprogramowania antywirusowego na urządzeniach mobilnych nawiązujących połączenia z siecią Woodward, jeżeli poziom ryzyka zagrożenia wirusami jest uważany za wystarczający, aby żądać tego zabezpieczenia z myślą o bezpieczeństwie danych Woodward.

16.2 Bezpieczna transmisja danych i przechowywanie na nośnikach przenośnych

Niestety, transmisja danych lub ich przechowywanie nie są w 100% bezpieczne. Niemniej, Dział IT Woodward odpowiedzialny jest za podjęcie racjonalnych działań mających na celu zastosowanie odpowiednich zabezpieczeń w celu wsparcia autentyczności, integralności i poufnych danych firmy oraz elektronicznie chronionych informacji zdrowotnych (ePHI).

Jakakolwiek osoba przesyłająca zastrzeżone lub poufne informacje biznesowe, dane zastrzeżone lub informacje ePHI powinna upewnić się, że transmisje danych są zaszyfrowane i/lub stosowana jest inna bezpieczna metoda transmisji. Poziomy szyfrowania powinny być zgodne z postanowieniami Safe Harbor HIPAA oraz Ustawy HITECH.

Jeżeli informacje biznesowe lub informacje ePHI przechowywane są na dyskietkach, urządzeniach USB lub innych lekkich nośnikach przenośnych, użytkownik odpowiedzialny jest za zapewnienie, że nośnik nie ulegnie zgubieniu, kradzieży lub zawieruszeniu. Informacje ePHI należy przechowywać na nośnikach szyfrowanych lub szyfrować pliki przed skopiowaniem ich na nośnik niezaszyfrowany.

Informacje poufne obejmujące hasła do systemów komputerowych Woodward, numery kart telefonicznych, numery umów o świadczeniu usług, informacje zastrzeżone, dane finansowe itp. nie powinny być przechowywane na przenośnych nośnikach magazynowania, w tym m.in. na tradycyjnych pamięciach, pamięciach USB lub płytach CD, chyba że informacje zabezpieczone są za pomocą oprogramowania umożliwiającego ochronę hasłem i szyfrowanie.

Woodward może wykorzystać technologię kontroli urządzeń w celu ograniczenia typu stosowanych nośników magazynowania i rodzaju informacji kopiowanych na te nośniki.

16.3 Zgodność z przepisami dotyczącymi eksportu

Systemy i procesy IT muszą wspierać wymagania związane z przepisami eksportowymi.

16.3.1 Utrzymanie i dostęp do systemów, prawa dotyczące dostępu do sieci

Do systemów i obsługi systemów zostaną przypisane pozwolenia skonfigurowane w sposób uniemożliwiający uzyskanie dostępu do kontrolowanych danych technicznych znajdujących się w systemach IT Woodward przez osoby niebędące obywatelami Stanów Zjednoczonych lub nieposiadające Statusu Stałego Rezydenta. (Osoba niebędąca obywatelem Stanów Zjednoczonych lub nieposiadająca Statusu Stałego Rezydenta to osoba, która nie posiada obywatelstwa amerykańskiego, Statusu Stałego Rezydenta zgodnie z definicją 8 U.S.C. 1101(a)(20) lub której nadano status uchodźcy zgodnie z definicją 8 U.S.C. 1324b(a)(3)).

Serwery, na których znajdują się dane kontrolowane przez Stany Zjednoczone muszą być umieszczone w Stanach Zjednoczonych. Wszyscy pracownicy IT, którzy posiadają dostęp do tych systemów, muszą być obywatelami Stanów Zjednoczonych, posiadać Status Stałego Rezydenta lub specjalne pozwolenie od Rządu Stanów Zjednoczonych na uzyskanie dostępu.

16.3.2 Identyfikacja i segregacja danych technicznych

Systemy ERP Woodward muszą być w stanie sklasyfikować towary w dół do poziomu części elementu.

16.3.3 Podwykonawcy IT

Wszelkie osoby posiadające dostęp do komputerów Woodward, na których znajdują się kontrolowane dane techniczne, muszą być obywatelami Stanów Zjednoczonych lub posiadaczami Statusu Stałego Rezydenta i nie mogą znajdować się na liście zakazanych podmiotów, chyba że posiadają specjalne pozwolenie Rządu Stanów Zjednoczonych na uzyskanie dostępu. Dział IT będzie współpracować z Działem Zgodności Eksportu w celu otrzymania licencji dla podwykonawcy, jeżeli będzie taka potrzebna. Wszyscy podwykonawcy będą informowani o wymaganiach w zakresie kontroli eksportu przed rozpoczęciem pracy.

16.3.4 Przechowywanie kopii zapasowych

Przechowywanie kopii zapasowych systemów i danych IT musi spełniać wymagania w zakresie kontroli eksportu. Jeżeli przechowywanie zostało zlecone podmiotowi niezależnemu, usługodawca taki musi spełniać wymagania dotyczące przechowywania informacji kontrolowanych ITAR i EAR. Dostawca musi również stosować wszystkie konieczne środki kontroli technicznej, wymagane do ochrony tego rodzaju informacji.

16.3.5 Prowadzenie dokumentacji

Wszystkie dokumenty i rejestry odnoszące się do środków kontroli Technologii Informatycznych będą prowadzone zgodnie z procedurami firmy i przepisami rządowymi.

Jeżeli pracownicy Woodward udają się w podróż z kontrolowanymi danymi technicznymi zapisanymi na swoich laptopach, muszą trzymać wykaz danych kontrolowanych przez pięć (5) lat po dacie podróży. Wszystkie dane i rejestry powinny być prowadzone zgodnie z procedurą firmy (BDDS 4-06-3102).

16.4 Utylizacja sprzętu i danych

Przed pozbyciem się nośnika magnetycznego lub innego typu nośnika, który może zawierać poufne lub zastrzeżone informacje biznesowe lub elektronicznie chronione informacje zdrowotne, należy podjąć stosowne kroki, aby zapewnić, że informacje umieszczone na nośnikach nie mogą zostać odtworzone. Obejmuje to m.in. taśmy kopii zapasowych, dyskietki oraz dyski twarde komputerów osobistych lub innego sprzętu przekazywanego do szkół, organizacji non-profit, sprzedawanego firmom złomującym lub utylizowanego na śmietniskach.

Przed utylizacją wszystkie dyski twarde muszą zostać zniszczone, odmagnetyzowane lub wyczyszczone zgodnie ze standardami Departamentu Obrony. Taśmy kopii zapasowych, płyty CD, wymienne pamięci masowe i inne podobne urządzenia muszą zostać zniszczone lub wyczyszczone zgodnie ze standardami Departamentu Obrony. Niszczenie może być wykonane przez personel Woodward lub przez uznanych dostawców tego typu usług. Standardy Departamentu Obrony zgodne są z następującą publikacją: NIST SP 800-88, Wytyczne dotyczące niszczenia nośników elektronicznych.

16.5 Narzędzia bezpieczeństwa systemu

Za każdym razem, kiedy będzie to uzasadnione z punktu widzenia kosztów, w odniesieniu do komputerów i sieci firmy należy stosować zautomatyzowane narzędzia wyszukiwania i obsługi powszechnych problemów związanych z bezpieczeństwem.

16.6 Poprawki zabezpieczeń, service packi, hot fixy oraz nowe wersje produktów

Analityk ds. Bezpieczeństwa IT ma za zadanie polecić, które poprawki zabezpieczeń, service packi, hot fixy oraz nowe wersje produktów należy zainstalować na urządzeniach klientów Woodward oraz serwerach we wszystkich siedzibach, zgodnie z polityką ryzyka i kosztów związanych z rozlokowaniem. Analityk ds. Bezpieczeństwa IT określi racjonalne ramy czasowe dla rozlokowania na podstawie powiązanego ryzyka i ilości zasobów potrzebnych do zastosowania poprawek, ilości czasu poświęconego na testowanie oraz możliwego planu wycofania. Dział Globalnych Usług IT dla Klientów oraz Dział Globalnej Infrastruktury IT odpowiedzialne są za pomoc w procesie testowania poprawek zabezpieczeń i opcji rozlokowania poprzez ich wykorzystanie na zagrożonej aplikacji lub urządzeniach oraz powiadamianie Analityka ds. Bezpieczeństwa IT o wszelkich problemach napotkanych podczas instalacji.

Ocena, rekomendowanie oraz testowanie poprawek we wszystkich środowiskach za wyjątkiem systemu Windows należy do zakresu obowiązków administratora danego systemu.

Administratorzy systemów i personel obsługi technicznej mogą podjąć decyzje o instalacji dodatkowych poprawek, szczególnie na aplikacjach specjalistycznych i niestandardowych lub sprzęcie, który musi być wykorzystywany przez wszystkie siedziby. Dodatkowo, instalacja nowych wersji oprogramowania itp. może być wymagana przez kadrę menedżerską IT w celu realizacji celów Firmy, takich jak potrzeba łatwej wymiany informacji pomiędzy pracownikami, sprawy związane z licencjami itd.

Przed wdrożeniem do środowiska produkcyjnego, wszystkie poprawki muszą zostać zatwierdzone przez odpowiedniego Dyrektora lub wyznaczonego zastępcę, zgodnie z zaleceniami OP-694.

Dział Globalnej Infrastruktury IT będzie prowadzić regularnie zaplanowane skanowanie, mające na celu weryfikację statusu poprawek na wszystkich urządzeniach, jak również identyfikację innych punktów newralgicznych systemów. Wyniki skanowania będą przedkładane odpowiedzialnym administratorom serwerów, Analitykowi ds. Bezpieczeństwa Informacji oraz Dyrektorowi Działu Globalnego Bezpieczeństwa, Ryzyka i Zgodności IT.

16.7 Ujawnianie informacji systemowych

Wewnętrzne adresy, konfiguracje oraz informacje projektowe nt. systemów powiązanych z komputerami i sieciami firmy mają charakter poufny; ich ujawnianie podmiotom niezależnym, które nie mają upoważnienia do wykonywania szczególnych zadań, jest zabronione. Także środki bezpieczeństwa stosowane w celu ochrony

komputerów i sieci firmy mają charakter poufny i powinny być chronione w ten sam sposób. Wszelkie osoby otrzymujące dostęp do takich informacji muszą podpisać Oświadczenie o zachowaniu poufności zgodnie z poleceniem w Sekcji 3.1.

16.8 Pliki dziennika

W stopniu dopuszczalnym przez oprogramowanie systemowe, w ramach przetwarzania przez serwer informacji wrażliwych, cennych lub krytycznych, należy prowadzić rejestrację wszystkich zdarzeń mających znaczenie dla bezpieczeństwa. Wykaz zdarzeń dotyczących bezpieczeństwa, które powinny być rejestrowane przez każdy system operacyjny serwera, jest weryfikowany i dokumentowany przez Dział Globalnej Infrastruktury IT oraz Dział Globalnego Bezpieczeństwa, Ryzyka i Zgodności IT.

Zdarzenia mające znaczenie dla bezpieczeństwa ze wszystkich dzienników, zidentyfikowane jako krytyczne dla biznesu, powinny zostać skopiowane do głównego miejsca przechowywania, zanim zostaną nadpisane w ramach normalnego, cyklicznego procesu rejestracji.

Ze względu na fakt, iż dzienniki są bardzo ważne dla celów naprawy błędów, odzyskiwania po naruszeniu bezpieczeństwa i dochodzeń, muszą zostać zabezpieczone w sposób umożliwiający ich odczytanie jedynie przez osoby uprawnione. Co więcej, po zdarzeniu do żadnych plików dziennika nie wolno wprowadzać żadnych zmian, dlatego też prawo do zapisywania powinno być przyznawane w przypadkach absolutnej konieczności.

Dzienniki zawierające zdarzenia mające znaczenie dla bezpieczeństwa serwerów, muszą być włączone do harmonogramu nośników zapasowych.

Osobą odpowiedzialną za weryfikację krytycznych dzienników będzie wyznaczony pracownik Działu Globalnych Usług IT. Obowiązek ten może być przyznany różnym osobom, które zajmować się będą różnymi systemami. Co więcej, pracownicy IT odpowiedzialni za konkretne systemy, mogą weryfikować pliki dziennika jako konieczne do zapewnienia bezpieczeństwa i właściwego działania systemów, za które są odpowiedzialni. Pliki dziennika dowolnych bądź wszystkich systemów mogą być także przeglądane przez Analityka ds. Bezpieczeństwa IT. W celu skrócenia czasu potrzebnego do weryfikacji dzienników i identyfikacji zdarzeń lub czynności o wysokim stopniu ryzyka, można zastosować automatyczny monitoring dzienników z Oprogramowaniem Zarządzania Zdarzeń Związanych z Bezpieczeństwem oraz inne zautomatyzowane narzędzia.

16.9 Punkty newralgiczne związane z włamaniami (wewnętrznymi i zewnętrznymi)

Wszyscy pracownicy IT odpowiedzialni są za zgłaszanie wszelkich znanych lub podejrzanych punktów newralgicznych dotyczących bezpieczeństwa do Działu Globalnego Bezpieczeństwa, Ryzyka i Zgodności IT. Dodatkowo, wszyscy pracownicy IT ponoszą odpowiedzialność za naprawę wszystkich przypisanych im punktów newralgicznych, niezależnie od tego, czy punkty te były zidentyfikowane jako część wewnętrznego lub zewnętrznego audytu lub oceny, skanowania punktów newralgicznych, inspekcji kodu, analizy lub obserwacji.

16.10 Szkolenie w zakresie świadomości w kwestii bezpieczeństwa

Prowadzone są formalne, udokumentowane szkolenia w zakresie świadomości w kwestii bezpieczeństwa. Okresowe przypomnienia o politykach bezpieczeństwa i alerty o wirusach/zagrożeniach wysyłane są do wszystkich pracowników. W intranecie prowadzona będzie strona dedykowana kwestiom bezpieczeństwa w celu przekazania stosownych informacji wszystkim pracownikom IT i Woodward. Powiadomienia o bezpieczeństwie będą również publikowane w intranecie Woodward.

16.11 Obsługa incydentów bezpieczeństwa

Dział Globalnego Bezpieczeństwa, Ryzyka i Zgodności IT będzie prowadzić aktualny dokument opisujący procedury, których należy przestrzegać w przypadku wystąpienia incydentu związanego z bezpieczeństwem. W dokumencie zostaną określone osoby odpowiedzialne za każdy rodzaj incydentu, jak również wytyczne dotyczące reakcji. Dział Globalnego Bezpieczeństwa, Ryzyka i Zgodności IT będzie również przekazywać wszystkim siedzibom Woodward na całym świecie aktualne informacje o sytuacjach awaryjnych. Plan Reakcji na Incydenty dotyczące Bezpieczeństwa Komputerów oraz informacje o sytuacjach awaryjnych dostępne są dla wszystkich pracowników IT na stronie SharePoint.

16.12 Zdalne zarządzanie serwerami i komputerami

Połączenia zdalne za pomocą serwera Terminal, zdalnego pulpitu lub podobnych narzędzi dla celów instalacji oprogramowania i poprawek, rozwiązywania problemów, pomocy użytkownikom, monitorowania serwerów itp. mogą być nawiązywane przez pracowników Działu Globalnej Infrastruktury IT oraz Działu Globalnych Usług IT dla Klientów. Pracownicy, którzy sprawują podobne obowiązki, mogą również korzystać z tych narzędzi, ale ich dostęp musi być ograniczony do tych urządzeń, które są przez nich obsługiwane w sposób bezpośredni.

Procedury dotyczące użycia oprogramowania zarządzania zdalnego powinny dostać udokumentowane przez Dział Globalnego Bezpieczeństwa, Ryzyka i Zgodności IT. Połączeń nie wolno nawiązywać bez wcześniejszej zgody właściciela komputera osobistego, otrzymanej w momencie połączenia lub wcześniej. Zamierzone połączenia mogą być nawiązywane po otrzymaniu uprzedniej zgody Działu Prawnego lub Działu Personalnego, tak aby pracownicy Działu Globalnego Bezpieczeństwa, Ryzyka i Zgodności IT lub inni upoważnieni pracownicy IT mogli pomóc Działowi Personalnemu, Działowi Prawnemu lub Komitetowi Nadzoru nad Postępowaniem w

Biznesie przeanalizować rzekome uchybienia. Nawiązywanie innych połączeń zamierzonych jest zabronione.

Oprogramowanie połączeń zdalnych instalowane na komputerach osobistych używanych przez Dział Personalny, Dział Medyczny, wszystkich Członków Zarządu Firmy, Dział Prawny, Dział Kadr, Liderów IT, Administratora systemu Lawson, wszystkich administratorów UNIX i Oracle DBA musi być skonfigurowane w sposób, który wymaga od użytkownika komputera osobistego aktywnej akceptacji żądania połączenia w celu nawiązania połączenia zdalnego.

Niewłaściwe zastosowanie jakiegokolwiek narzędzia umożliwiającego nawiązanie zdalnego połączenia z serwerami lub komputerami osobistymi pracowników stanowi naruszenie niniejszych polityk i może być uważane za powód do podjęcia czynności dyscyplinarnych aż do zakończenia stosunku pracy.

17 Usługi i procedury związane z kwestią bezpieczeństwa

17.1 Audyty

Rutynowe, zaplanowane i nieogłaszane audyty bezpieczeństwa i zgodności prowadzone są zgodnie z zezwoleniem udzielonym przez Dział Globalnego Zarządzania IT, Dział Personalny, Dział Prawny lub Dział Audytu Wewnętrznego w celu zapewnienia zgodności z niniejszymi Politykami. Naruszenie postanowień niniejszych polityk może być uważane za powód do podjęcia działań administracyjnych, w tym czynności dyscyplinarnych aż do zakończenia stosunku pracy.

Regularnie prowadzone jest wewnętrzne skanowanie punktów newralgicznych; wyniki poddawane są ocenie w celu podjęcia działań naprawczych.

Audyty prowadzone są również w celu lepszego zarządzania zasobami IT i zapewnienia zgodności z licencjami oprogramowania.

17.2 Monitoring

Firma posiada prawo i może podjąć decyzję o monitorowaniu wszelkich i wszystkich systemów komputerowych, w tym m.in. monitorowania stron internetowych odwiedzanych przez pracowników, aktywności pracowników na czatach i w grupach dyskusyjnych, weryfikacji materiałów pobieranych i zamieszczanych przez pracowników oraz wiadomości mailowych wysyłanych i otrzymywanych przez użytkowników, chyba że działania te są wyraźnie zakazane na mocy obowiązującego prawa lub sekcję dotyczącą prywatności niniejszych polityk. Firma może także monitorować wszystkie przypadki zewnętrznego dostępu do systemów lub danych Woodward, niezależnie od dostępu przez przeglądarkę lub VPN.

Wszelkie nielegalne działania, naruszenia polityk firmy lub czynności sprzeczne z interesami firmy zidentyfikowane w trakcie monitoringu mogą (w zależności od indywidualnych okoliczności) zostać ujawnione Działowi Globalnego Bezpieczeństwa, Ryzyka i Zgodności IT, Działowi Personalnego, Radcy Prawnemu Woodward, Działowi Audytu Wewnętrznego, przełożonemu użytkownika i/lub odpowiedniemu organowi egzekwowania prawa.

Nazwisk osób zaangażowanych w incydent nie wolno przekazywać nikomu, komu takie informacje nie są potrzebne. Wszystkie inne dane osobowe zidentyfikowane w trakcie monitorowania, audytu lub dochodzeń traktowane są jako poufne. Wyłączenie to nie dotyczy informacji anonimowych lub zbiorczych. (np. piętnastu (15) pracowników udostępniło swoje hasła osobom nieupoważnionym.)

17.3 Zapobieganie utracie danych

Firma podjęła decyzję o wdrożeniu procedur i rozwiązań technicznych w celu zredukowania lub wyeliminowania ryzyka kradzieży lub przypadkowej utraty/wycieku własności intelektualnej, danych zastrzeżonych, informacji biznesowych lub danych na temat pracowników. Technologie te mogą obejmować m.in. oprogramowanie zapobiegające wyciekowi danych, wymagania szyfrowania, oprogramowanie kontroli urządzenia oraz oprogramowanie zarządzające prawami. Dział Globalnego Bezpieczeństwa, Ryzyka i Zgodności IT jest odpowiedzialny za ustalanie polityk, zarządzanie raportami dotyczącymi incydentów oraz współpracę z konkretnymi działami, w tym m.in. Działem Personalnym, Działem Świadczeń, Działem Prawnym i Zgodności z przepisami, Działem Technicznym oraz Działem Finansowym w celu zmniejszenia ryzyka utraty danych.

17.4 Zarządzanie zmianą

Powiadomienia na temat zmian będą wysyłane do Liderów IT i odpowiedniego personelu IT przed wprowadzeniem znaczących zmian do infrastruktury, serwerów, aplikacji, systemów operacyjnych, procedur i procesów. Jeżeli będzie to uważane za konieczne przez jakiegokolwiek pracownika Działu Globalnego Zarządzania IT, powiadomienia na temat zmian mogą być również wysyłane do pracowników, których zmiana dotyczy.

17.5 Procesy związane z zarządzaniem bezpieczeństwem

Testy bezpieczeństwa prowadzone są regularnie w celu uzyskania pewności, że opcje bezpieczeństwa systemu są adekwatne do stopnia ryzyka. Testy powinny obejmować ręczną lub automatyczną identyfikację punktów newralgicznych, testy funkcyjne i penetracyjne oraz weryfikację. Testy obejmować będą również systemy używane do przechowywania poufnych i zastrzeżonych informacji biznesowych oraz informacji ePHI.

Analiza ryzyka prowadzona jest w celu identyfikacji zasobów informatycznych, zagrożeń oraz prawdopodobieństwa i kosztów negatywnych okoliczności. Zidentyfikowane obszary bezpieczeństwa zarządzane są przez stosowanie efektywnych pod względem kosztów rozwiązań w zakresie bezpieczeństwa w celu zmniejszenia prawdopodobieństwa i stopnia strat poniesionych na skutek negatywnych okoliczności. Ocena ryzyka może być prowadzona na dowolnym systemie informatycznym, w tym aplikacjach, serwerach i sieciach, jak również w odniesieniu do dowolnej procedury lub procesu, za pomocą których systemy są zarządzane i/lub obsługiwane.

17.6 Zasoby, zgodności z prawami autorskimi i licencjami

Woodward ma bardzo poważne podejście do zarządzania zasobami, zgodności z prawami autorskimi oraz licencjami oprogramowania.

Oprogramowanie zarządzania zasobami zostanie zainstalowane na każdego rodzaju sprzęcie należącym do Woodward, np. komputerach nabiurkowych, stacjach roboczych i laptopach. Regularnej inwentaryzacji podlegały będą także serwery i sprzęt sieciowy, chyba że nie zostały włączone do inwentarza oprogramowania zarządzania zasobami. Dodanie do sieci sprzętu nienależącego do Woodward wymaga wcześniejszej, specyficznej dla urządzenia autoryzacji Działu IT i kadry menedżerskiej IT; proces ten musi być również śledzony przez Dział Globalnych Usług IT dla Klientów.

Każdy rodzaj oprogramowania zainstalowanego na serwerach, biznesowych systemach komputerowych, komputerach firmy oraz sprzęcie LAN/WAN musi posiadać wszystkie stosowne licencje. Dział Infrastruktury IT odpowiada za zapewnienie zgodności z licencjami oprogramowania zainstalowanego na komputerach nabiurkowych i urządzeniach mobilnych. Dział Infrastruktury IT odpowiada również za zapewnienie zgodności z licencjami oprogramowania zainstalowanego na sprzęcie LAN/WAN, serwerach i innych urządzeniach infrastruktury. Zgodność z licencjami oprogramowanie specjalistycznego należy do zakresu obowiązków działu, który posiada/korzysta z takiego oprogramowania. Analitycy ds. Zasobów, Licencji i Zgodności IT odpowiedzialni są za monitorowanie i doradzanie pracownikom IT oraz biznesowi w zakresie kwestii związanych ze zgodnością z licencjami.

Inwentaryzacji podlegać będą komputery osobiste oraz serwery w celu identyfikacji oprogramowania nielicencjonowanego, fałszywego i prywatnego. Dział Globalnych Usług IT dla Klientów i/lub Dział Globalnej Infrastruktury IT są upoważnione do usuwania wszelkiego rodzaju oprogramowania osobistego, fałszywego lub nielicencjonowanego zidentyfikowanego przez Analityka ds. Zasobów, Licencji i Zgodności IT i/lub Dział Globalnego Bezpieczeństwa, Ryzyka i Zgodności IT. Dział Globalnych Usług IT dla Klientów lub Dział Globalnej Infrastruktury IT mogą również usunąć nielicencjonowane lub osobiste pliki, pliki muzyczne, obrazy itp., które zajmują przestrzeń dyskową, tworzą konflikty z innymi zatwierdzonymi aplikacji, naruszają politykę zgodności z licencją oprogramowania lub narażają informacje Woodward na ryzyko nieuprawnionego dostępu.

17.7 Proces weryfikacji polityk i procedur

Polityka Woodward dotycząca Bezpieczeństwa Systemów Komputerowych i Informatycznych, Polityka Dopuszczalnego Użytkowania Komputerów i Sieci, Plan Reakcji na Incydenty Komputerowe, Plan Komunikacji Awaryjnej oraz inne Procedury Operacyjne związane z bezpieczeństwem powinny być weryfikowane przez Dział Globalnego Bezpieczeństwa, Ryzyka i Zgodności IT przynajmniej raz w roku kalendarzowym. Każda siedziba (w tym Dział Globalnej Infrastruktury IT) odpowiedzialny jest za weryfikację harmonogramów i procedur tworzenia kopii zapasowych oraz Planów Odtwarzania Awaryjnego przynajmniej raz w roku kalendarzowym. Wszystkie aktualizacje i zmiany podlegać będą normalnemu procesowi zatwierdzania.

18 Odstępstwa od polityki (wyjątkowe przypadki)

Odstępstwa od niniejszej polityki powinny być rzadkie i udokumentowane w formie pisemnej. Odstępstwa od niniejszej polityki muszą zostać zatwierdzone przez Wiceprezesa ds. Technologii Informatycznych.

Matt Cook
Wiceprezes ds. Technologii Informatycznych

Osoby niebędące pracownikami Woodward, które podpisały Politykę 1-33, podlegają takim samym przepisom, którym podlegają pracownicy firmy. Z tego też względu, za każdym razem, gdy w politykach używany jest termin „pracownicy”, dotyczy on również osób niebędących pracownikami Woodward, które posiadają konta w systemach Woodward, chyba że wyraźnie stwierdzono inaczej.