

---

## DOPUSZCZALNE UŻYTKOWANIE KOMPUTERÓW I SIECI

### Cel

Firma Woodward używa systemów i zasobów komputerowych do wsparcia różnych rodzajów swojej działalności na poziomie całej firmy i oczekuje, że każdy będzie z tych zasobów korzystał w odpowiedzialny sposób.

Firma stosuje określone zasady dotyczące dopuszczalnego korzystania z zasobów komputerowych i ich bezpieczeństwa. Każda osoba używająca systemów komputerowych w firmie musi podpisać i zwrócić dokument „Zobowiązanie do przestrzegania zasad dopuszczalnego użytkowania komputerów i sieci (ang. „Acceptable Computer and Network Usage Agreement”), potwierdzając tym samym przyjęcie zasad określonych w polityce. Dotyczy to nowo zatrudnionych pracowników, zlecenioborców i pracowników tymczasowych. Nieprzestrzeganie zasad może być uznane za podstawę do podjęcia działań dyscyplinarnych, łącznie z rozwiązaniem stosunku pracy, i/lub wszczęcia postępowania cywilnego i karnego. Kontrole dotyczące przestrzegania zasad użytkowania komputerów w firmie będą przeprowadzane w ramach zwykłej działalności. Na życzenie uprawnionych działów (Zarządzania Zasobami Ludzkimi, Prawnego, Audytu Wewnętrznego oraz innych działów wskazanych przez wiceprezesa nadzorującego kadry lub dyrektora generalnego), informacje zebrane podczas kontroli zostaną im udostępnione.

Celem polityki jest zabezpieczenie firmy i jej pracowników przed przerwami w działalności lub odpowiedzialnością związaną z niewłaściwym korzystaniem z zasobów komputerowych firmy. Określa ona obowiązki osób, definiując standardy, które:

- chronią dane komputerowe o kluczowym znaczeniu dla działalności firmy i stanowią zabezpieczenie przed ich utratą,
- chronią integralność i poufność informacji dotyczących prowadzonej działalności, danych osobowych pracowników oraz danych dotyczących dostawców/klientów,
- umożliwiają zachowanie zgodności danych pomiędzy zakładami,
- zapewniają przestrzeganie wymogów licencji zakupionego oprogramowania,
- zapewniają odpowiedni dostęp do danych firmowych,
- zapewniają właściwe, etyczne i zgodne z prawem użytkowanie zasobów komputerowych firmy.

### Zakres obowiązywania

Zasady niniejszej polityki stosują się do wszystkich pracowników zatrudnionych we wszystkich zakładach firmy Woodward oraz do innych osób<sup>1</sup>, którym zezwolono na korzystanie z zasobów informatycznych firmy Woodward. Polityka odnosi się do wszystkich systemów komputerowych i zasobów informatycznych firmy Woodward, zarówno sterowanych indywidualnie jak i dzielonych (wspólnych), niezależnych (autonomicznych) i łączonych w sieć. Dotyczy wszystkich urządzeń komputerowych i urządzeń komunikacji komputerowej będących własnością firmy Woodward, dzierżawionych, obsługiwanych lub użytkowanych na podstawie umów przez firmę Woodward. Obejmują one, choć nie wyłącznie, komputery osobiste, urządzenia przenośne takie jak palmtopy czy BlackBerry, telefony z dostępem do internetu,

---

<sup>1</sup> Między innymi, choć nie wyłącznie, pracowników tymczasowych, zlecenioborców, dostawców, konsultantów i pracowników magazynów zakładowych.

---

bezwolne urządzenia komunikacyjne, stacje robocze, serwery, mikrokomputery oraz urządzenia sieciowe wraz z urządzeniami peryferyjnymi i oprogramowaniem, niezależnie od tego, czy wykorzystywane są do celów administracyjnych, badawczych, przeprowadzania testów, czy też do innych celów.

#### **Dostęp do systemów komputerowych**

Aby uzyskać dostęp do systemów komputerowych firmy Woodward, użytkownicy muszą się zalogować, podając ID użytkownika i hasło. Obowiązkiem użytkownika jest zagwarantowanie poufności wszystkich haseł dostępu do systemu i zmiana wszystkich tych haseł co najmniej raz na pół roku. Haseł nie należy przechowywać w możliwych do odczytania plikach wsadowych, skryptach automatycznego logowania, makrach oprogramowania, itp. lub w innych miejscach, w których mogą je znaleźć nieupoważnione osoby.

Użytkownicy powinni wybrać hasła trudne do odgadnięcia. Nie należy stosować pochodnych ID użytkownika i prostych sekwencji cyfr takich jak 123456. Należy też unikać informacji powszechnie znanych takich jak marka samochodu, imiona członków rodziny, zwierząt domowych, itp.

#### **Ochrona systemów i danych firmowych**

Użytkownicy są odpowiedzialni za ochronę systemów komputerowych firmy przed kradzieżą, utratą lub dostępem nieupoważnionych osób. Ponadto użytkownicy są odpowiedzialni za ochronę informacji poufnych i własnych firmy Woodward, informacji dotyczących dostawców i klientów, danych osobowych pracowników oraz wszelkich innych informacji, których utrata lub ujawnienie przyniosłoby szkodę firmie lub poszczególnym pracownikom.

Obchodzenie zabezpieczeń komputerowych takich jak, choć nie wyłącznie, oprogramowanie antywirusowe, szyfrowanie twardego dysku, podwójna autoryzacja, filtrowanie stron www, wykrywanie programów szpiegujących, itp. jest zabronione. Użytkownicy nie powinni pobierać i uruchamiać programów i urządzeń zabezpieczających, z zamiarem złamania zabezpieczeń systemów. Użytkownicy nie powinni ujawniać swoich ID i haseł, danych wymaganych do autoryzacji przy korzystaniu z dostępu wdzwanianego, plików konfiguracyjnych systemu ani też innych informacji, które mogą umożliwić osobom nieupoważnionym dostęp do danych firmowych.

Nie wolno umyślnie usuwać lub zmieniać danych, sprawiając tym samym kłopoty lub trudności firmie albo osobie. Umyślnie uszkodzenie zasobów komputerowych firmy takich jak komputery osobiste, serwery, urządzenia przenośne, telefony komórkowe czy infrastruktura sieciowa jest zakazane.

Nie wolno podejmować jakichkolwiek działań, których celem jest pogorszenie działania systemów, pozbawienie upoważnionych użytkowników dostępu do danych lub w jakikolwiek inny sposób uszkodzenie działalności firmy.

Nie wolno rozpowszechniać poufnych informacji dotyczących działalności firmy, planów, rysunków technicznych, itp. osobom, które nie powinny mieć do nich dostępu. Dotyczy to, choć nie wyłącznie, informacji podlegających ograniczeniom prawnym z uwagi na charakter wojskowy, postanowienia amerykańskich przepisów oraz regulacji eksportowych i importowych albo wymogi celne, a także informacji, których rozpowszechnianie reguluje Amerykańska Komisja Papierów Wartościowych i Giełd. Więcej informacji na ten temat zawiera Polityka 2-16 oraz zasady i wskazówki dotyczące eksportu i importu obowiązujące w firmie Woodward.

Firmowa poczta elektroniczna nie jest domyślnie szyfrowana, jednak z niektórymi klientami i sprzedawcami można się kontaktować za pośrednictwem bezpiecznych połączeń. Aby uzyskać pomoc w przypadku wątpliwości, czy szyfrowanie lub podobne

---

technologie winny być użyte w celu ochrony danych, należy skorzystać z lokalnej linii informacyjnej.

Użytkownikom nie wolno udostępniać serwerów firmowych ani jakichkolwiek elementów infrastruktury sieciowej bez uprzedniej zgody Działu IT i właściwego kierownictwa odpowiedzialnego za określony rodzaj działalności. Dotyczy to, choć nie wyłącznie, czynności takich jak zakładanie stron www, witryn FTP czy innych mechanizmów, stosowanych tak do celów prowadzenia działalności, jak i z nią niezwiązanych.

Nie należy zamieszczać w internecie informacji poufnych i firmowych, danych osobowych i informacji poufnych dotyczących pracowników oraz informacji, które mogą szkodzić interesom firmy. Dotyczy to, choć nie wyłącznie, zamieszczania tego rodzaju informacji na osobistych blogach, stronach www lub portalach społecznościowych takich jak MySpace czy Facebook.

Dane firmowe należy zgodnie z procedurami przechowywać na dyskach sieciowych. Dział Globalnego IT jest odpowiedzialny za archiwizowanie danych znajdujących się na serwerach sieciowych. Osoba przechowująca dane lub pliki w urządzeniach lokalnych takich jak laptop, komputer stacjonarny lub przenośne urządzenie do przechowywania danych ma obowiązek zadbać o to, by dostępna była kopia zapasowa z tymi danymi, na wypadek gdyby pliki zostały uszkodzone, skasowane lub utracone na skutek awarii albo kradzieży komputera czy też innego nieszczęśliwego zdarzenia.

Informacji firmowych nie należy przechowywać w sieci korzystając z serwisów oferujących miejsce do przechowywania plików (np. Box.net, Xdrive) z nieautoryzowanym dostępem. Transferu plików należy dokonywać korzystając z serwisów i metod zatwierdzonych przez firmę. Ponadto informacji firmowych nie należy przechowywać we własnych urządzeniach, w tym, choć nie wyłącznie, w domowych komputerach osobistych. Przechowywanie informacji firmowych w komputerach domowych sprawia, że takie komputery narażone są na przeszukiwanie, w celu znalezienia danych przechowywanych elektronicznie z zamiarem ich wykorzystania w postępowaniu dowodowym w procesach sądowych (ang. e-Discovery).

Nie należy przekazywać, ani ustnie ani w formie pisemnej, szczegółowych informacji znajdujących się w sieci lub bazach danych osobom trzecim bez uprzedniej zgody Działu Bezpieczeństwa Globalnego IT. Przed ujawnieniem informacji kluczowych lub poufnych, Dział Globalnego IT będzie wymagał od takiej osoby trzeciej podpisania umowy o zachowaniu poufności. Korzystanie przez osobę trzecią z uzyskanych informacji będzie się ograniczać do celów leżących w interesie firmy i informacje te zostaną zwrócone zgodnie z instrukcjami firmy.

### **Zdalna łączność**

Zdalny dostęp przyznawany jest indywidualnie i wymaga zatwierdzenia przez przełożonego. Tylko „właściciel” konta może korzystać z konta dostępu zdalnego. Oczekujemy od pracowników przestrzegania zasad bezpieczeństwa przy korzystaniu z tego konta, nigdy nie należy narażać systemów i/lub danych firmowych przez umożliwienie dostępu do nich nieupoważnionym osobom. Pracownik odpowiada za korzystanie z konta i ponosi odpowiedzialność w przypadku używania go w sposób naruszający zasady określone przez firmę. Mogą też obowiązywać dodatkowe wymogi bezpieczeństwa związane ze zdalną łącznością, takie jak podwójna autoryzacja z użyciem tokenów.

### **Komunikator internetowy**

Prawo korzystania z zatwierdzonego komunikatora internetowego do celów biznesowych przyznawane jest indywidualnie i wymaga zatwierdzenia przez przełożonego. Korzystanie z niezatwierdzonego komunikatora internetowego jest

---

zabronione. Pracownik ponosi odpowiedzialność za używanie komunikatora w sposób naruszający zasady określone przez firmę.

### **Urządzenia przenośne**

Urządzenia takie jak laptopy, palmtopy, BlackBerry, urządzenia komunikacji bezprzewodowej, telefony z dostępem do internetu, w których to urządzeniach można przechowywać dane dotyczące firmy Woodward lub przy pomocy których można uzyskać dostęp do tych danych, muszą być skonfigurowane w taki sposób, aby po ich włączeniu musiał być wprowadzony kod bezpieczeństwa lub hasło dostępu.

Informacji o kluczowym znaczeniu dla działalności firmy, informacji poufnych lub firmowych albo informacji umożliwiających identyfikację osób nie należy przechowywać w **niezaszyfrowanych** urządzeniach przenośnych takich jak laptopy, palmtopy, BlackBerry, urządzenia pamięci masowej USB, zewnętrzne twarde dyski, płyty CD, itp. Informacji firmowych nie należy przechowywać w urządzeniach prywatnych.

Każde urządzenie przenośne, w tym telefon z dostępem do internetu, winno być zwrócone do Działu IT, w celu właściwego usunięcia danych przed jego wyrzuceniem, podarowaniem lub przekazaniem innej osobie.

Osoby używające firmowych laptopów lub komputerów naręcznych, itp. winny zachowywać ostrożność, aby chronić te urządzenia przed kradzieżą lub uszkodzeniem. Nie należy pozostawiać ich w nie zamkniętych samochodach, salach konferencyjnych, pokojach hotelowych lub w innych niestrzeżonych miejscach.

Laptopy i inne urządzenia przenośne nie powinny być przewożone w bagażu nadanym w samolotach, autobusach czy innych publicznych środkach transportu.

### **Poczta elektroniczna**

Cała poczta elektroniczna, w tym wiadomości tworzone lub przekazywane przez systemy elektronicznej komunikacji, uważana jest za własność firmy Woodward Governor Company<sup>1</sup>. W zasadzie, poczta elektroniczna winna być wykorzystywana wyłącznie w związku z prowadzoną działalnością. Dopuszczalne jest okazjonalne wykorzystywanie jej do celów osobistych pod warunkiem, że:

- korzystanie z niej nie odbywa się kosztem pracy
- korzystanie z niej nie wpływa na wydajność pracowników i
- nie zużywa więcej niż niewielką część zasobów.

Intensywne używanie komputera i poczty elektronicznej do celów prywatnych w godzinach pracy stanowi niewłaściwe wykorzystanie czasu pracy, co jest podstawą do wszczęcia działań dyscyplinarnych, łącznie z rozwiązaniem stosunku pracy.

Wiadomości przekazywane za pośrednictwem poczty elektronicznej uważane są za dokumentację firmową i jako takie mogą być wykorzystane w postępowaniu administracyjnym, sądowym lub innym. Należy pamiętać, że wiadomości elektroniczne mogą być przekazywane dalej, przechwytywane, przeglądane, drukowane lub przechowywane przez inne osoby. Firma nie gwarantuje prywatności

---

<sup>1</sup> Te prawa własności obejmują dodatkowo prawnie chronioną komunikację elektroniczną między firmą a jej radcą prawnym i/lub niektórymi innymi fachowcami. Takie prawnie chronione informacje mogą być udostępnione lub ujawnione wyłącznie zgodnie z zasadami postępowania z tego rodzaju informacjami. Emaile lub inne wiadomości elektroniczne zawierające poufne dane medyczne albo inne informacje poufne będą chronione zgodnie ze stosownymi zasadami poufności.

---

poczty i innej komunikacji elektronicznej. Korzystanie z poczty elektronicznej (lub innych systemów komunikacji elektronicznej) oznacza zgodę na przeglądanie wszelkich elementów otrzymywanych lub wysyłanych, znajdujących się w systemie.

Nie wolno wykorzystywać systemów komunikacji elektronicznej dla własnego zysku, do prowadzenia prywatnych interesów lub w celach zabawowych/rozrywkowych. Nie wolno wysyłać w załącznikach plików w celach prywatnych lub rozrywkowych. Wykorzystywanie zasobów elektronicznych firmy do wysyłania wiadomości, które mogłyby być interpretowane albo postrzegane jako zawierające treści seksualne, treści wskazujące na dyskryminację etniczną lub rasową, bądź też w jakikolwiek inny sposób naruszające zapisy Polityki 6-16 stanowi podstawę do wszczęcia działań dyscyplinarnych, łącznie z rozwiązaniem stosunku pracy. Wiadomości nie powinny zawierać słów wulgarnych lub obraźliwych, a ich treść powinna być uprzejma i właściwa dla komunikacji biznesowej. Niedozwolone są długie prywatne rozmowy prowadzone za pośrednictwem poczty elektronicznej, polegające na wielokrotnej wymianie wiadomości między osobami.

Nie wolno wykorzystywać kont prywatnych (np. hotmail, yahoo, gmail, itp.) w działalności firmy. Ponadto nie wolno korzystać z serwisów online (np. YouSendIt Inc., SendThisFile Inc.) do wysyłania dużych załączników związanych z działalnością firmy. Użytkownicy powinni korzystać z usługi WSFT, dostępnej za pośrednictwem Działu Globalnego IT, aby bezpiecznie przesyłać duże pliki.

#### **Dostęp do internetu**

Użytkownicy mogą uzyskać dostęp do internetu, aby łatwiej im było wykonywać swoje obowiązki. Dostęp zapewniony jest na koszt firmy i ma służyć prowadzeniu interesów. Nie wolno korzystać z internetu do celów niezwiązanych z pracą, niezgodnych z prawem lub nieetycznych. Użytkownikom nie wolno wykorzystywać internetu do pobierania z sieci plików muzycznych, filmów, oprogramowania i innych plików służących celom prywatnym. Krótkotrwałe korzystanie z internetu w porze lunchu, podczas przerwy lub po godzinach pracy jest dozwolone pod warunkiem, że nie zakłóca to pracy firmy, także zakładów znajdujących się w innych strefach czasowych, nie narusza zasad bezpieczeństwa, nie wpływa na wydajność pracowników ani też w inny sposób nie narusza zasad obowiązujących w firmie. Korzystając z dostępu do internetu, który zapewnia firma pracownicy zgadzają się postępować zgodnie ze wskazówkami zawartymi w niniejszej polityce i spełniać wymogi w niej określone. Z wnioskiem o uruchomienie przez Dział Globalnego IT konta dla pracownika występuje jego kierownik, a informacja o tym przekazywana jest do Działu Zarządzania Zasobami Ludzkimi.

Firma zgodnie ze stosownymi procedurami zapewnia dostęp do stron internetowych i może mieć dostęp do informacji przeglądanych lub przekazywanych za pośrednictwem internetu. Pracownicy Działów: Globalnego Zarządzania Zasobami Ludzkimi, Audytu Wewnętrznego, Prawnego oraz Bezpieczeństwa Globalnego IT mogą przeglądać pliki logów. Firma może podjąć decyzję o blokowaniu dostępu do stron, które uważa za nie mające znaczenia z punktu widzenia prowadzonej działalności. Niezablokowania dostępu do strony nie należy interpretować jako jej dorozumianego zatwierdzenia.

#### **Licencjonowane oprogramowanie i materiały objęte prawami autorskimi**

Zasadą obowiązującą w firmie Woodward jest respektowanie wszystkich praw autorskich oprogramowania i praw własności intelektualnej oraz przestrzeganie warunków licencji całego oprogramowania zainstalowanego w systemach firmy Woodward. Użytkownicy muszą przestrzegać postanowień wszystkich umów licencyjnych dotyczących oprogramowania. Bezprawne kopiowanie, dalsza dystrybucja lub odsprzedaż jakichkolwiek materiałów podlegających licencji, objętych prawami autorskimi, posiadających zarejestrowany znak firmowy lub zastrzeżonych na rzecz właściciela jest surowo zabronione. Instalowanie licencjonowanego oprogramowania w urządzeniach firmy Woodward bez zakupu licencji jest zakazane.

---

Bezprawne kopiowanie oprogramowania lub innych materiałów objętych prawami autorskimi (takich jak filmy czy utwory muzyczne) może narazić zarówno pracownika jak i/lub firmę Woodward na kary wynikające z prawa cywilnego i z prawa karnego, przewidziane za naruszenie praw autorskich. W urządzeniach firmowych nie należy instalować prywatnego oprogramowania, plików i programów multimedialnych objętych prawami autorskimi.

### **Standardy dotyczące sprzętu i oprogramowania oraz zatwierdzanie zakupów**

Wszystkie zakupy sprzętu i oprogramowania muszą spełniać wcześniej przyjęte standardy firmowe i wymogi dotyczące jakości, a także muszą zapewnić kompatybilność z pozostałym sprzętem i oprogramowaniem komputerowym firmy. Zakazane są zakupy oprogramowania lub sprzętu komputerowego bez uprzedniego zatwierdzenia przez kierownictwo działu. Zakupy takie muszą być skoordynowane/rejestrowane przez odpowiedni Dział Globalnego IT. Całe oprogramowanie musi być kupowane zgodnie ze standardową procedurą dokonywania zakupów IT i nie należy go kupować korzystając z firmowych kart kredytowych, podręcznych środków pieniężnych czy w ramach wydatków przeznaczonych na podróże służbowe. Źródła zakupów są ograniczone, aby firma Woodward miała pełny rejestr całego oprogramowania zakupionego do komputerów firmowych. Oprogramowanie zakupione poza normalnymi źródłami zakupów Działu Globalnego Zaopatrzenia musi być zarejestrowane przez Analityka zasobów IT, umów i licencji. Dokumentacja taka jest potrzebna, aby firma Woodward mogła prowadzić rejestr oprogramowania, zapewnić jego wsparcie i uaktualnienie oraz mieć wgląd w licencje w przypadku kontroli. Obejmuje to również oprogramowanie, które może być pobierane i/lub kupowane przez internet.

### **Produkty komputerowe niestandardowe/stanowiące własność pracowników**

Firma zdecydowanie odradza korzystanie przez pracowników z własnego sprzętu i oprogramowania na terenie firmy, a pracownicy IT nie mają obowiązku udzielać wsparcia w zakresie takich produktów. Kierownik działu winien postępować zgodnie z ustalonymi procedurami, aby uzyskać/zapewnić pracownikom sprzęt lub oprogramowanie potrzebne do pracy w firmie.

Instalowanie niezatwierdzonego oprogramowania i/lub dokonywanie zmian w sprzęcie komputerowym, oprogramowaniu albo konfiguracji systemów bez uzyskania uprzedniej zgody Działu Globalnego IT jest zabronione. Jeżeli takie pliki zostaną znalezione w trakcie rutynowej pomocy technicznej lub kontroli komputerów, firma zastrzega sobie prawo do usunięcia programu lub danych naruszających zapisy niniejszej polityki. Naruszenie praw autorskich może podlegać karze, łącznie z rozwiązaniem stosunku pracy.

### **Implikacje prawne**

Firma ma prawo<sup>1</sup> i może podjąć decyzję o monitorowaniu wszelkich elementów swoich systemów komputerowych, w tym, choć nie wyłącznie, może kontrolować strony internetowe przeglądane przez pracowników, ich uczestnictwo w czatach i forach internetowych, materiały pobierane przez użytkowników z sieci lub w niej zamieszczane, pliki przechowywane na dyskach sieciowych i lokalnych, a także może przeglądać pocztę elektroniczną wysyłaną i otrzymywaną przez pracowników.

Korzystając z zasobów komputerowych firmy należy zawsze przestrzegać obowiązujących w niej zasad i wskazówek dotyczących miejsca pracy wolnego od molestowania. Przykłady niewłaściwego korzystania obejmują, choć nie wyłącznie, rozpowszechnianie, przeglądanie lub gromadzenie plików zawierających obraźliwe słownictwo, treści pornograficzne, możliwość uprawiania hazardu, niesmaczne żarty, czy treści i/lub obrazy wulgarne.

---

<sup>1</sup> Firma będzie wykonywać te prawa z zastrzeżeniem i pod warunkiem przestrzegania zasad prawnie gwarantowanej ochrony i poufności.

Oprócz wewnętrznych regulacji i polityk firmy mają również zastosowanie wszystkie lokalne i krajowe przepisy prawa. W sytuacji gdy krajowe przepisy prawa, których określony zakład firmy Woodward ma obowiązek przestrzegać, wykluczają stosowanie się do zapisów Polityki 1-33 lub pozostają z nimi w sprzeczności, przepisy krajowe będą nadrzędne w stosunku do warunków określonych w polityce.

Pracownik ponosi odpowiedzialność za korzystanie z zasobów komputerowych firmy. Używanie komputerów, systemów i sieci firmy Woodward oznacza przyjęcie wszystkich warunków zawartych w polityce. Niewłaściwe korzystanie z zasobów komputerowych, sieciowych lub informacyjnych może spowodować podjęcie działań dyscyplinarnych, łącznie z rozwiązaniem stosunku pracy, i/lub wszczęcie postępowania na mocy stosownego przepisu prawa cywilnego i karnego. Wszelkie działania, które są niezgodne z prawem, naruszają zasady obowiązujące w firmie lub jej interesy są surowo zabronione i mogą być powodem dochodzenia. Uzasadnione skargi sugerujące niewłaściwe korzystanie z zasobów komputerowych należy kierować do właściwego lokalnego Działu Zarządzania Zasobami Ludzkimi, Działu Prawnego, Działu Audytu Wewnętrznego lub Działu Bezpieczeństwa Globalnego IT, celem podjęcia stosownych kroków, czy to wewnętrznych działań dyscyplinarnych, czy też postępowania na mocy stosownego przepisu prawa cywilnego i/lub karnego.

Nielegalne kopiowanie oprogramowania i materiałów chronionych prawami autorskimi podlega odszkodowaniu na mocy prawa cywilnego oraz karom wynikającym z prawa karnego, łącznie z grzywną i karą pozbawienia wolności.

Wszystkie urządzenia, w których przechowywane są dane firmy Woodward podlegają obowiązkowi okazania i ujawnienia znajdujących się w nich informacji w związku z prowadzonym postępowaniem cywilnym. Obejmuje to komputery, serwery, taśmy archiwalne, palmtopy, telefony komórkowe, napędy USB, płyty CD, itp. Prokuratorzy i adwokaci mogą uzyskać dostęp do systemów komputerowych, w celu zebrania dowodów w postępowaniu prawnym. Informacje firmowe znajdujące się w domowych komputerach, na prywatnych kontach emailowych lub w innych prywatnych urządzeniach również podlegają obowiązkowi okazania i ujawnienia znajdujących się w nich informacji. W związku z tym, należy pracować zgodnie z najwyższymi standardami etycznymi, mając świadomość, że informacje znajdujące się w komputerze (także te, które zostały usunięte) mogą być wykorzystane przeciwko pracownikowi, firmie i innym osobom w trakcie postępowania prawnego.

Internet traktowany jest jako narzędzie w prowadzeniu interesów i pełni funkcję forum publicznego, z którego korzysta cały świat. Dlatego też, niewłaściwe oświadczenie złożone w internecie może spowodować poważne szkody, ponieważ informacje mogą być w nim szybko i skutecznie rozpowszechniane. Pracownik może i będzie ponosić odpowiedzialność za obraźliwe, dyskryminujące, oszczercze i szkalujące oświadczenia składane za pośrednictwem internetu lub innych środków komunikacji elektronicznej.

### **Praca na odległość**

Pracownik uczestniczący w programach pracy na odległość/pracy w domu prowadzonych przez firmę musi przestrzegać zapisów tej polityki tak, jakby pracował na terenie firmy. W szczególności, zobowiązany jest do przestrzegania zasad dotyczących telepracy i wymaganych zabezpieczeń chroniących sprzęt i dane będące własnością firmy przed uszkodzeniem i nieuprawnionym użyciem.

Firma Woodward nie ponosi odpowiedzialności za uszkodzenie własności pracownika wynikające z jego uczestnictwa w programie pracy na odległość i nie odpowiada za koszty eksploatacyjne, koszty utrzymania domu czy inne koszty dodatkowe związane z wykorzystaniem miejsca zamieszkania do wykonywania pracy.

### **Używanie sprzętu będącego własnością firmy poza jej terenem**

Z wyjątkiem sprzętu komputerowego przeznaczonego do używania w podróży (np. notebooki i komputery nareczne), aby wynieść sprzęt komputerowy poza teren firmy konieczna jest zgoda kierownika danego działu i Działu Wsparcia Globalnego IT. Nie wolno udostępniać sprzętu osobom nie będącym pracownikami firmy Woodward (członkom rodziny, dzieciom, przyjacielom). Zaginięcie lub kradzież sprzętu należy natychmiast zgłosić.

Używanie sprzętu firmy Woodward w celu osiągnięcia zysku lub korzyści osobistych jest surowo zabronione i muszą być przestrzegane wszystkie zasady i procedury dotyczące korzystania z komputerów i sieci obowiązujące w firmie. Instalowanie lub używanie własnego oprogramowania, gier, plików muzycznych, wideo, dostępu do internetu lub korzystanie w inny sposób niezwiązany z pracą ze sprzętu należącego do firmy bez jej uprzedniej zgody jest zabronione.

### **Oprogramowanie opracowane przez użytkownika i towarzysząca dokumentacja**

Programy opracowane przez użytkowników (w tym bazy danych, arkusze kalkulacyjne czy makra do edytorów tekstów) muszą być dokładnie przetestowane i przeanalizowane zanim zostaną faktycznie użyte do wsparcia operacji związanych z prowadzoną działalnością. Powinna być opracowana pisemna dokumentacja dla każdego kluczowego programu/raportu używanego do wsparcia funkcji biznesowych. Cała dokumentacja dotycząca programu musi być dostępna dla pozostałych osób, odpowiednio na dysku sieciowym, w internecie lub w formie papierowej.

Oprogramowanie opracowane przez użytkownika i/lub towarzysząca dokumentacja są własnością firmy i żadnemu pracownikowi nie wolno ich sprzedawać lub wykorzystywać w celu osiągnięcia zysku, nie będą one też udostępniane ani ujawniane osobom trzecim bez zgody kierownictwa.

### **Wsparcie techniczne**

Aby uzyskać wsparcie techniczne, użytkownicy komputerów powinni najpierw zwrócić się do Działu Usług Wsparcia Globalnego IT, używając w tym celu formularza Prośba o usługę (ang. Service Request). Z wyjątkiem specjalistycznego oprogramowania, użytkownik *nie* powinien kontaktować się bezpośrednio ze sprzedawcą lub firmą, która je opracowała. Wsparcie techniczne dotyczące sprzętu i oprogramowania używanego poza terenem firmy w ramach pracy na odległość ograniczone jest do sprzętu będącego własnością firmy udostępnionego pracownikowi.

### **Kontrole komputerów**

Przeprowadzane będą rutynowe, zaplanowane i niezaplanowane kontrole komputerów, aby zapewnić przestrzeganie zapisów niniejszej polityki. Nielegalne urządzenia, oprogramowanie i/lub dane znalezione w trakcie kontroli komputerów lub rutynowej pomocy technicznej zostaną usunięte i w stosunku do ich użytkownika mogą być podjęte działania dyscyplinarne.

### **Rozwiązanie umowy o pracę**

Wszystkie informacje znajdujące się w systemach komputerowych są własnością firmy Woodward. Sprzęt komputerowy i zainstalowane systemy muszą być zwrócone w dobrym stanie przed opuszczeniem firmy w ostatnim dniu pracy. Jeżeli sprzęt znajduje się poza terenem firmy, jego użytkownik musi zorganizować dostarczenie całego sprzętu należącego do firmy w ciągu 24 godzin od rozwiązania umowy o pracę.

Używanie zasobów komputerowych po dobrowolnym lub przymusowym rozwiązaniu umowy o pracę jest surowo zabronione i może podlegać dochodzeniu.

### **Odpowiedzialność**

Za nadzór nad realizacją niniejszej polityki i przestrzeganiem związanych z nią standardów odpowiada Dział Globalnego IT. W razie potrzeby, można się również



---

konsultować w kwestiach z nią związanych z Działem Zarządzania Zasobami Ludzkimi, Prawnym, Audytu Wewnętrznego oraz kierownikami poszczególnych grup działalności.

Użytkownicy są odpowiedzialni za ochronę systemów komputerowych i danych własnych firmy przed utratą lub dostępem nieupoważnionych osób. Zabrania się umyślnego podejmowania działań, które pogarszają lub zakłócają pracę systemów albo uniemożliwiają dostęp do nich uprawnionym użytkownikom. Celowe obchodzenie zabezpieczeń i zasad bezpieczeństwa jest zakazane. Nie wolno rozpowszechniać ani udostępniać poufnych informacji dotyczących prowadzonej działalności, dokumentów lub planów osobom, które nie powinny mieć do nich dostępu.

Podejrzane incydenty związane z bezpieczeństwem danych firmowych, komputerów, serwerów lub infrastruktury sieciowej winny być niezwłocznie zgłaszane Działowi Bezpieczeństwa Globalnego IT lub Działowi Zarządzania Zasobami Ludzkimi. Jednym ze sposobów, w jaki można to zrobić jest wysłanie emaila zaadresowanego „Bezpieczeństwo komputerowe”. Jeżeli incydent stanowi natychmiastowe zagrożenie dla bezpieczeństwa fizycznego centrum danych, sieci, itp., należy od razu powiadomić strażnika.

**Naruszenia i kary**

Naruszenie zapisów niniejszej polityki może stanowić podstawę do wszczęcia działań administracyjnych, które mogą obejmować kroki dyscyplinarne, łącznie z rozwiązaniem stosunku pracy. Kary za naruszenie polityki wymierzać będzie Dział Zarządzania Zasobami Ludzkimi. Naruszenie stosownych przepisów prawa będzie również powodem wszczęcia działań dyscyplinarnych oraz postępowania cywilnego lub karnego. Nielegalne kopiowanie oprogramowania chronionego prawami autorskimi podlega odszkodowaniu na mocy prawa cywilnego oraz karom wynikającym z prawa karnego, łącznie z grzywną i karą pozbawienia wolności. Pracowników obowiązują także zapisy Polityki 1-41 firmy Woodward, Bezpieczeństwo komputerów, oraz inne stosowne zasady i procedury.

/-/ Thomas A. Gendron  
Prezes Rady Nadzorczej i Dyrektor Generalny

**Zobowiązanie do przestrzegania zasad dopuszczalnego użytkowania komputerów i sieci**

## PODSUMOWANIE

**Nadzór nad realizacją polityki**

Za nadzór nad realizacją niniejszej polityki i przestrzeganiem związanych z nią standardów odpowiada Dział Globalnego IT. W razie potrzeby, można się również konsultować w kwestiach z nią związanych z innymi działami, w tym, choć nie wyłącznie, z Działem Zarządzania Zasobami Ludzkimi, Prawnym, Audytu Wewnętrznego. Dział Zarządzania Zasobami Ludzkimi jest odpowiedzialny za rekomendowanie i podejmowanie działań dyscyplinarnych w związku z naruszeniem polityki. Użytkownicy mają obowiązek przestrzegać zapisów polityki i zgłaszać jej naruszenia Działowi Bezpieczeństwa Globalnego IT.

Komputery firmy Woodward są jej własnością i jako takie podlegają kontrolom i monitorowaniu. Firma ma prawo i może podjąć decyzję o monitorowaniu wszelkich elementów swoich systemów komputerowych oraz działań związanych z ich użytkowaniem.

**Ochrona systemów, sprzętu i danych własnych firmy**

Użytkownicy są odpowiedzialni za ochronę systemów komputerowych, sprzętu i danych własnych firmy przed utratą lub dostępem nieupoważnionych osób. Zabrania się umyślnego podejmowania działań, które pogarszają lub zakłócają pracę systemów, powodują obejście zabezpieczeń albo uniemożliwiają dostęp do nich uprawnionym użytkownikom. Celowe obchodzenie zabezpieczeń i zasad bezpieczeństwa jest zakazane. Nie wolno rozpowszechniać ani udostępniać poufnych informacji dotyczących prowadzonej działalności, dokumentów lub planów osobom, które nie powinny mieć do nich dostępu.

**Zobowiązanie użytkownika**

Jestem świadomy (-a), że muszę ściśle przestrzegać zapisów Polityki 1-33 i postępować zgodnie z jej zasadami. Naruszenie tego zobowiązania może być uznane za podstawę do podjęcia działań dyscyplinarnych, łącznie z rozwiązaniem stosunku pracy, i/lub wszczęcia postępowania cywilnego albo karnego.

Zapoznałem (-am) się z treścią niniejszego zobowiązania i będę go przestrzegać.

\_\_\_\_\_  
**Imię i nazwisko (drukowanymi literami)**

\_\_\_\_\_  
**Podpis**

\_\_\_\_\_  
**Data**

## **POLITYKA**

INDEKS: Administracja  
Nazwa: Dopuszczalne użytkowanie komputerów i sieci  
Numer: 1-33  
Strona: 11 z 11  
Data: 2009-1-12  
Dotyczy: Firmy Woodward na całym świecie

---

(Proszę podpisać tę stronę i zwrócić ją do lokalnego Działu Zarządzania Zasobami Ludzkimi. Pozostałą część dokumentu należy zachować dla siebie.)