AFG
Building the Difference

Wytyczne w sprawie
- korzystania z internetu, poczty elektronicznej i telefonu oraz jego nadzorowania; oraz
- wglądu do konta użytkownika współpracownika

29 sierpnia 2013 r.

Spis treści

Preambuła....3
1. Korzystanie z usług internetowych i telefonicznych....3
2. Nadzorowanie usług internetowych i telefonicznych....3
2.1 Protokołowanie....3
2.2 Zakaz stosowania programów szpiegowskich....3
2.3 Analiza protokołów....4
2.4 Nadzorowanie w ramach gwarancji bezpieczeństwa i sprawności firmowego elektronicznego systemu przetwarzania danych....4
2.5 Okres przechowywania....4
3. Rozróżnienie między prywatnymi i służbowymi wiadomościami elektronicznymi....4
4. Sankcje za nadużycia....5
5. Administrowanie pocztą elektroniczną w czasie nieobecności/odejścia z pracy....5
5.1 Przewidywalna nieobecność....5
5.2 Nieprzewidywalna nieobecność....5
5.3 Dłuższa nieprzewidywalna nieobecność....5
5.4 Odejście współpracownika z pracy....5
6. Wgląd do konta użytkownika współpracownika....6
7. Podejrzenie o popełnieniu czynu karalnego....6
8. Informacje....6
9. Wejście w życie....7
Załącznik: Formularz wniosku o prawo do wglądu do konta użytkownika współpracownika....8

AFG
Building the Difference

Preambuła

Niniejsze wytyczne określają, czy i w jaki sposób współpracownicy spółek koncernowych AFG Arbonia-Forster-Holding AG (zwanych dalej „AFG") mogą korzystać z internetu i telefonu. Ponadto wytyczne te mają na celu ochronę współpracowników i AFG w przypadku nadzorowania tych usług oraz wglądu do konta użytkownika. Należy przestrzegać przepisów, które są bardziej surowe lub które stosuje się podczas realizacji wytycznych.

1. Korzystanie z usług internetowych i telefonicznych

Każdy współpracownik w oparciu o osobiste hasło ma dostęp do usług internetowych (internet/e-mail). Korzystanie z usług internetowych i telefonicznych ma służyć zasadniczo do celów służbowych oraz lepszego i/lub bardziej racjonalnego bądź profesjonalnego wykonywania pracy.

Korzystanie z dostępnych usług internetowych i telefonicznych służy przede wszystkim celom przedsiębiorstwa. Wykorzystywanie ich do celów prywatnych jest tolerowane podczas przerw w pracy, a jego przypadki należy ograniczyć do minimum.

Nie wolno odwiedzać stron internetowych o treściach niezgodnych z prawem, pornograficznych i rasistowskich. Zabroniony jest również udział w określonych czynnościach (np. za pośrednictwem komunikatorów internetowych, czatów, wiadomości elektronicznych itp.). Automatyczne filtry blokują treści należące do określonych kategorii. Strony internetowe o następujących treściach są zablokowane dla współpracowników: pornografia, działania przestępcze, treści ekstremistyczne, internetowe rozgłośnie radiowe, czat, narkotyki.

Ze względów bezpieczeństwa wszystkie wiadomości elektroniczne i każdy dostęp do internetu, w tym pobierane pliki, są automatycznie sprawdzane pod kątem wirusów i treści niebezpiecznych i w razie potrzeby blokowane. Pomimo to wiadomości elektroniczne od nieznanych nadawców lub takie, których temat wskazuje na wirus, należy natychmiast usuwać bez ich otwierania. Zasadniczo komunikaty w internecie należy kasować, wybierając opcję „Nie" lub „Anuluj". Pod żadnym pozorem nie należy otwierać załączników do e-maili pochodzących od nieznanych nadawców.

Wszystkie zaszyfrowane połączenia z internetem (np. bankowość internetowa) są rozkodowywane i również automatycznie sprawdzane.

2. Nadzorowanie usług internetowych i telefonicznych

2.1 Protokołowanie

Dział informatyczny gromadzi informacje o aktywności w internecie. Telefoniczne połączenia przychodzące i wychodzące są rejestrowane przez dostawców usług internetowych. Rejestrowanie określa się jako ciągłą rejestrację głównych danych, takich jak „kto", „co", „kiedy" i w firmie AFG następuje ono w przypadku:

- internetu (odwiedzane strony internetowe, użytkownik, data, czas)
- e-maili (nadawca, odbiorca, data, czas, temat wiadomości)
- logowania do systemu (użytkownik, data, czas)
- telefonu (nr telefonów wszystkich uczestników rozmowy telefonicznej, czas, data, czas trwania)

2.2 Zakaz stosowania programów szpiegowskich

Stosowanie programów szpiegowskich (tzw. spyware) jest zakazane.

2.3 Analiza protokołów

Analiza protokołów przebiega na rożnych poziomach.

Analiza anonimowa: Służy ona do sporządzania statystyk, np. w celu strukturalnego odtworzenia przeciętnego korzystania z internetu, najczęściej odwiedzanych stron internetowych itp. Liczba badanych osób powinna być na tyle duża, aby wykluczyć możliwość zidentyfikowania poszczególnych współpracowników (np. wszyscy współpracownicy AFG Management AG).

Analiza indywidualna: Analiza indywidualna jest dozwolona tylko wówczas, jeżeli w anonimowej analizie stwierdzono nadużycie lub istnieje inne podejrzenie o nadużyciu. Za nadużycie uznaje się każde naruszenie postanowień dotyczących korzystania zgodnie z punktem 1 niniejszych wytycznych lub innych obowiązków wynikających z umowy o pracę.

Indywidualna analiza następuje na wniosek przełożonego i jest przeprowadzana przez właściwy dział kadr we współpracy z działem informatycznym oraz pełnomocnikiem ds. ochrony danych — o ile jest on ustanowiony. Jeżeli podejrzenie o nadużycie nie potwierdzi się, analizy indywidualne zostają natychmiast wstrzymane, a zgromadzone dane — zniszczone.

2.4 Nadzorowanie w ramach gwarancji bezpieczeństwa i sprawności firmowego elektronicznego systemu przetwarzania danych.

Jeżeli pomimo technicznych środków zabezpieczających wystąpi usterka elektronicznego systemu przetwarzania danych, podczas poszukiwania przyczyny usterki mogą być wykorzystywane protokoły. Jeśli przyczyną usterki jest nadużycie, wobec zidentyfikowanego współpracownika zgodnie z punktem 4 niniejszych wytycznych można zastosować sankcje.

2.5 Okres przechowywania

W celu zabezpieczenia dowodów protokoły aktywności internetowej są przechowywane przez cztery tygodnie, chyba że procedura związana z sankcją lub karą wymaga dłuższego okresu przechowywania. Przechowywanie protokołów telefonicznych jest uzależnione od obowiązujących lokalnie przepisów telekomunikacyjnych.

3. Rozróżnienie między prywatnymi i służbowymi wiadomościami elektronicznymi

Konto poczty elektronicznej służy przede wszystkim do celów służbowych. Prywatne wiadomości należy ograniczyć do minimum. AFG nie dokonuje wglądu ani edycji wiadomości elektronicznych, które są oznakowane jako prywatne. Jeżeli korespondencja prywatna i służbowa nie jest oznakowana w celu jej rozróżnienia i na podstawie elementów adresowania nie można rozpoznać prywatnego charakteru wiadomości lub domniemywać tego w inny sposób, AFG może zakładać, że jest to wiadomość służbowa. W przypadku wątpliwości co do charakteru wiadomości elektronicznej należy to wyjaśnić ze współpracownikiem.

W razie potrzeby służbowe wiadomości elektroniczne można zabezpieczyć.

W przypadku rozpoznania, że wiadomość elektroniczna ma charakter prywatny, AFG nie może zapoznać się z jej treścią. Zasada ta dotyczy również sytuacji, w których podejrzewa się, że za pośrednictwem wiadomości elektronicznej zostało popełnione przestępstwo lub nastąpiło inne nadużycie zgodnie z punktem 1 niniejszych wytycznych.

AFG
Building the Difference

4. Sankcje za nadużycia

Jeżeli wymagania i zasady nadzorowania były przestrzegane i okazało się, że doszło do nadużycia, mogą zostać nałożone sankcje zgodnie z kodeksem pracy (upomnienie, blokada dostępu do internetu, wypowiedzenie itp.).

Przed skasowaniem plików uzyskanych w efekcie nadużycia współpracownik zostanie poinformowany i — o ile będzie to uzasadnione — otrzyma on możliwość zapisu tych plików (np. prywatnych wiadomości elektronicznych) na prywatnym nośniku danych.

5. Administrowanie pocztą elektroniczną w czasie nieobecności/odejścia z pracy

5.1 Przewidywalna nieobecność

W przypadku nieobecności od konkretnego dnia w Outlooku należy uaktywnić funkcję automatycznej odpowiedzi. W komunikacie o nieobecności należy podać osobę zastępującą (wraz z danymi kontaktowymi) na wypadek pilnych spraw oraz informację, czy przychodzące wiadomości będą automatycznie przekierowywane czy też nie. Automatyczne przekierowanie wszystkich wiadomości do osoby zastępującej może następować tylko w wyjątkowych przypadkach.

Jeżeli współpracownik przez przeoczenie zapomniał uaktywnić funkcję automatycznej odpowiedzi, należy postępować zgodnie z punktem 6.

5.2 Nieprzewidywalna nieobecność

W przypadku nieprzewidywanej nieobecności (np. choroba, wypadek) współpracownik ma obowiązek w miarę możliwości jak najszybciej zapewnić przekierowanie przychodzących wiadomości. W tym celu można skorzystać z bezpiecznego portalu Outlook Web Access (http://service.afg.ch). Współpracownik może również ustanowić zastępcę, który będzie uprawniony do wglądu do nadchodzących służbowych wiadomości elektronicznych i w razie potrzeby do ich opracowania. Jeżeli współpracownik nie może zapewnić przekierowania wiadomości, należy postępować zgodnie z punktem 6.

5.3 Dłuższa nieprzewidywalna nieobecność

Jeżeli w przypadku nieobecności nie można przewidzieć terminu powrotu do pracy lub nieobecność trwa szczególnie długo (ponad 4 tygodnie), zgodnie z punktem 6 możliwy jest (dalszy) wgląd w korespondencję.

5.4 Odejście współpracownika z pracy

Współpracownik odchodzący z pracy jest odpowiedzialny za przekazanie wszelkich dokumentów służbowych. Przed odejściem ma obowiązek wyczyścić dyski i skrzynkę poczty elektronicznej. Niezałatwione jeszcze sprawy, takie jak wiadomości elektroniczne itp. lub inne niezbędne lub przydatne dla AFG informacje, należy przekazać.

Współpracownik odchodzący z pracy ma możliwość skasowania lub zapisania prywatnych wiadomości elektronicznych i innych prywatnych dokumentów na prywatnym nośniku danych.

Najpóźniej ostatniego efektywnego dnia w pracy nastąpi zablokowanie konta użytkownika (w tym adresu poczty elektronicznej). Jeżeli po zablokowaniu niezbędny okaże się wgląd do poczty elektronicznej lub folderu

użytkownika, należy postępować zgodnie z punktem 6. Nadawcy wysyłający wiadomości na zablokowany adres zostaną automatycznie poinformowani o tym, że adres odbiorcy już nie działa. Po uzgodnieniu z przełożonym w wyjątkowych przypadkach może zostać włączona funkcja automatycznej odpowiedzi zawierającej zastępczy adres poczty elektronicznej AFG. Należy zwrócić uwagę, aby nie można było wywnioskować sposobu zakończenia stosunku pracy.

30 dni od ostatniego efektywnego dnia pracy, jednakże najpóźniej wraz z upływem okresu wypowiedzenia, następuje skasowanie konta użytkownika.

6. Wgląd do konta użytkownika współpracownika

Jeżeli pomimo podjęcia środków zgodnie z punktem 5.1 lub w przypadku nieprzewidywalnych nieobecności wystąpi konieczność wglądu do skrzynki poczty elektronicznej współpracownika, należy najpierw skontaktować się z tym pracownikiem i uzyskać od niego zgodę na wgląd. Jeżeli współpracownik odmówi udzielenia zgody lub skontaktowanie się z nim będzie niemożliwe, przełożony ma obowiązek złożyć pisemny wniosek do właściwego działu kadr (por. załącznik). Zgoda zostanie wydana tylko wówczas, jeżeli AFG ma istotny interes (np. pilne, służbowe powody), nie można czekać na powrót współpracownika i podjęte zostały wszelkie środki, aby uniknąć wglądu. Automatyczne przekierowanie wszystkich wiadomości jest dozwolone tylko w wyjątkowych przypadkach.

W przypadku uzyskania zgody na wgląd należy poinformować dział informatyczny, który zresetuje hasło. W procedurze wglądu uczestniczy przełożony i pracownik działu kadr (zasada czterech oczu). Nieobecny współpracownik zostanie o tym fakcie poinformowany najpóźniej w dniu powrotu do pracy.

Wgląd pod względem czasowym i treściowym należy ograniczyć do danych podanych we wniosku. Dozwolony jest wgląd tylko w służbowe wiadomości elektroniczne. Wiadomości oznaczonych jako prywatne nie wolno otwierać, przeglądać, przenosić, kopiować, przesyłać dalej i/lub kasować (por. także punkt 3). Przełożony przekierowuje potrzebne wiadomości elektroniczne do siebie samego. Ponadto należy włączyć funkcję automatycznej odpowiedzi ze wskazaniem osoby do kontaktu w pilnych sprawach.

Postanowienia te obowiązują w analogiczny sposób w przypadku odejścia współpracownika z pracy oraz wglądu do folderu użytkownika.

7. Podejrzenie o popełnieniu czynu karalnego

Jeżeli po analizie protokołów lub na podstawie innych wskazówek zostanie stwierdzony bądź podejrzewany będzie czyn karalny, zostaną zabezpieczone odpowiednie protokoły. AFG zastrzega sobie prawo do złożenia doniesienia o przestępstwie przeciwko danej osobie. Jeżeli niezbędny okaże się wgląd w korespondencję elektroniczną, dane itp., należy podjąć te kroki tylko po uzyskaniu wcześniejszej zgody podejrzanego współpracownika. W przypadku gdy uzyskanie wcześniejszej zgody jest niemożliwe lub w sytuacji odmowy jej udzielenia, sprawę należy co do zasady przekazać właściwym organom śledczym. W wyjątkowych przypadkach AFG może samodzielnie dokonać wglądu, gdy usprawiedliwiają to istotny interes i konkretna sytuacje związane z podejrzeniem. Wgląd przebiega zgodnie z wymienionym wyżej punktem 6.

AFG zobowiązuje się do poufnego traktowania wyniku dochodzenia przeciwko osobom trzecim, w szczególności także innym współpracownikom.

8. Informacje

Informacji związanych z niniejszymi wytycznymi udziela Head of Legal & Compliance.

AFG
Building the Difference

9. Wejście w życie

Niniejsze wytyczne wchodzą w życie w trybie natychmiastowym.

Arbon, 29 sierpnia 2013 r.

AFG Arbonia-Forster-Holding AG

Daniel Frutig
Chief Executive Officer

Andrea Wickart
Head of Legal & Compliance
Sekretarka Generalna

AFG
Building the Difference

Załącznik: Formularz wniosku o prawo do wglądu do konta użytkownika współpracownika

Konkretny współpracownik	
Nazwisko:	Spółka:
Stanowisko:	
Przedmiot wglądu	
□ Wiadomości elektroniczne	□ Pliki
Przyczyna wglądu	
□ planowana nieobecność	data przewidywanego powrotu:
□ nieprzewidywana nieobecność	
□ współpracownik już odszedł z pracy	Data odejścia z pracy:
□ Podejrzenie o popełnieniu czynu karalnego	Konkretne powody podejrzenia:
Wgląd jest pilnie niezbędny ze względu na	
Zakres wglądu (możliwie jak najbardziej szczegółowo)	
Niezbędne są wiadomości elektroniczne lub dane na następujące tematy:	Wgląd ma dotyczyć wiadomości elektronicznych lub danych w następującym okresie:
Próby skontaktowania się z danym współpracownikiem	
□ Tak, próba uzyskania wcześniejszej zgody została podjęta z następującym skutkiem:	□ Nie, próba uzyskania wcześniejszej zgody nie została podjęta, ponieważ:
Alternatywy	
Podjęto następujące środki, aby uniknąć wglądu:	
□ szukano danych w katalogu ogólnym (stacja dysków G: /wspólnym koncie poczty elektronicznej).	□ spytano innych członków zespołu nieobecnej osoby o potrzebne pliki/wiadomości elektroniczne.
□ Pozostałe:	
Miejscowość/data	**Podpis**