Podstawowe zasady bezpieczeństwa informacji w ABC S.A.

(materiał szkoleniowy – proszę o zwrot)

1. Obowiązkiem każdej osoby posiadającej dostęp do **informacji chronionych** w ABC S.A. (zwanej dalej użytkownikiem) jest zapewnienie **bezpieczeństwa** tym **informacjom**, tj. podejmowania takich działań, które zagwarantują przetwarzanej informacji spełnienie wymagań wymienionych w pkt. 2 b) oraz przestrzeganie w codziennej działalności niniejszych podstawowych zasad bezpieczeństwa informacji.

2. Podstawowe pojęcia z zakresu ochrony informacji:

   a) **Informacje chronione** – informacje, których obowiązek ochrony wynika z odnośnych przepisów prawa, w tym dotyczących tajemnicy bankowej, tajemnicy ubezpieczeniowej, tajemnicy zawodowej, informacji poufnych, danych osobowych i tajemnicy przedsiębiorstwa; w ABC przyjęto podział informacji chronionej na cztery grupy:

   - **„Tajemnica ABC”** – informacja której ujawnienie, zniekształcenie lub utrata spowodowałoby znaczną szkodę dla ABC, jej pracowników, klientów lub partnerów biznesowych;
   - **„Do użytku wewnętrznego ABC”** - informacja, która nie została zaklasyfikowane jako „Tajemnica ABC – dane produkcyjne” lub „Tajemnica ABC”, a jej ujawnienie lub utrata mogłyby spowodować szkodę dla ABC, jej pracowników, klientów lub partnerów biznesowych;
   - **informacja jawna** - informacja chroniona, która została w sposób świadomy i uprawniony ujawniona do publicznej wiadomości (informacja z wyłączonym atrybutem poufności).

   b) **Bezpieczeństwo informacji –** łączne zapewnienie poufności, integralności i dostępności informacji oraz rozliczalności jej przetwarzania, przy czym pojęcia te oznaczają odpowiednio:

   - **poufność informacji** – właściwość zapewniająca, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom;
   - **integralność informacji** – właściwość zapewniająca, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
   - **dostępność informacji** – właściwość zapewniająca, że informacja jest dostępna i możliwa do wykorzystania na żądanie, w założonym czasie, przez autoryzowany podmiot.;
   - **rozliczalność** – właściwość zapewniająca, że działania podmiotu w odniesieniu do informacji mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.

   c) **Przetwarzanie informacji** - wykonywanie operacji takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie, przekazywanie, przesyłanie i usuwanie informacji niezależnie od formy przetwarzania (elektroniczna bądź papierowa).

   d) **Socjotechnika** – ogół metod, środków i działań praktycznych zmierzających do wywołania u potencjalnej ofiary, najczęściej drogą manipulacji, pożądanych zachowań mających na celu uzyskanie dostępu do informacji bądź firmy przez osobę do tego nieuprawnioną.

3. Przydzielanie uprawnień do korzystania z systemów teleinformatycznych i systemów ochrony fizycznej realizowane jest w oparciu o zasadę „minimalnych przywilejów”. Każdy użytkownik takiego systemu otrzymuje prawa dostępu wyłącznie do tych zasobów, które są niezbędne do wykonywania powierzonych mu obowiązków. Użytkownik ponosi osobistą odpowiedzialność za wszelkie czynności wykonane z użyciem identyfikatora indywidualnie przydzielonego użytkownikowi w systemie.

4. Jeżeli w trakcie korzystania z zasobów systemu teleinformatycznego i systemów ochrony fizycznej użytkownik stwierdzi, że posiadane przez niego uprawnienia są większe, niż wynikają z zakresu jego obowiązków służbowych, to zobowiązany jest niezwłocznie zgłosić ten fakt do bezpośredniego przełożonego; bezpośredni przełożony takiego pracownika sporządza wniosek o usunięcie nadmiarowych uprawnień w systemie i przekazuje go do realizacji zgodnie z obowiązującą w ABC procedurą nadawania uprawnień w systemach.

5. Każdy użytkownik systemu teleinformatycznego zobowiązany jest:
   a) rozpoczynać pracę w systemie logując (rejestrując) się do niego wyłącznie za pomocą przydzielonego na podstawie imiennego wniosku osobistego identyfikatora i uwierzytelniając się metodą przyjętą w danym systemie, np. poprzez podanie hasła, użycie indywidualnej karty mikroprocesorowej, użycie odcisku palca itp.; zabrania się logowania do systemu z użyciem identyfikatorów innych osób;
   b) opuszczając stanowisko pracy zablokować stację roboczą w ten sposób, aby nie mogła z niej skorzystać inna osoba (np. w systemie Windows: Ctrl+Alt+Del „Zablokuj komputer”, lub poprzez wyrejestrowanie się z systemu);
   c) po zakończeniu pracy zamknąć używane przez niego szafy i pomieszczenia, w których przechowuje dokumentację i nośniki informacji, wyrejestrować się z systemu oraz wyłączyć stację roboczą.
6. Każdy pracownik posiada indywidualną kartę mikroprocesorową niezbędną do korzystania z elektronicznego systemu kontroli dostępu do pomieszczeń ABC, pełniącą jednocześnie funkcję imiennego identyfikatora pracownika. Korzystanie z kluczy ma miejsce wyłącznie w przypadku gdy pomieszczenie nie zostało objęte systemem kontroli dostępu. Pracownik, który stwierdził brak lub zniszczenie klucza, powiadamia o tym Administratora Obiektu oraz Administratora Bezpieczeństwa Fizycznego. Zabrania się:
   a) dorabiania kluczy do pomieszczeń i budynków bez zgody Dyrektora Centrum Administracji oraz poinformowania Administratora Bezpieczeństwa Fizycznego,
   b) udostępniania kluczy osobom nieupoważnionym,
   c) pozostawiania kluczy bez dozoru.
7. Identyfikator należy nosić w widocznym miejscu, w sposób umożliwiający odczytanie zawartych na nim informacji. W przypadku zauważenia osoby bez identyfikatora lub bez towarzyszącej osoby nadzorującej, lub zauważenia osoby posługującej się cudzym identyfikatorem, pracownik ABC obowiązany jest do niezwłocznego zgłoszenia tego faktu do komórki bezpieczeństwa ABC (bezpieczeństwo@abc.pl).
8. Użytkownik ponosi osobistą odpowiedzialność za wszelkie czynności wykonane z użyciem swojego identyfikatora i kodu dostępu (jeśli kod taki został użytkownikowi przydzielony w systemie kontroli dostępu).
9. Zabronione jest:
   a) dokonywanie prób sprawdzania, testowania i omijania zabezpieczeń systemu ochrony fizycznej,
   b) udzielanie informacji osobom nieuprawnionym o wykorzystywanym przez ABC systemie ochrony fizycznej,
   c) korzystanie z identyfikatora innej osoby,
   d) pozostawianie identyfikatora bez nadzoru,
   e) udostępnianie identyfikatora osobom trzecim,
   f) ingerowanie w strukturę identyfikatora (np. zginanie, łamanie, przecinanie czy dziurawienie),
   g) samodzielne dokonywanie zmian na wydanym identyfikatorze (podmienianie zdjęcia, zmienianie opisów itp.),
   h) dokonywanie modyfikacji danych zapisanych w identyfikatorze oraz dokonywanie prób przełamania jego zabezpieczeń chyba, że należy to do obowiązków służbowych danego pracownika,
   i) wpuszczanie do pomieszczeń ABC osób nieuprawnionych za pomocą swojego identyfikatora,
   j) wchodzenie i wychodzenie do/z pomieszczeń bez użycia własnego identyfikatora (np. korzystając z otwarcia drzwi przez inną osobę).

10. W obiektach zajmowanych przez ABC ustala się podział pomieszczeń na obszary chronione, charakteryzujące się różnymi poziomami wymagań bezpieczeństwa:
    a) administracyjny – obejmujący stanowisko recepcji oraz sale konferencyjne,
    b) bezpieczny – pomieszczenia, w których odbywa się przetwarzanie informacji chronionych.
11. W ABC S.A. obowiązuje zakaz wprowadzania osób trzecich na teren firmy do pomieszczeń znajdujących się poza administracyjnym. Goście powinni być przyjmowani wyłącznie w salach konferencyjnych.
12. W przypadku uzasadnionej konieczności wprowadzenia gościa na obszar bezpieczny (np. serwis), po uzyskaniu zgody pracownika bezpieczeństwa firmy ABC, osoba wprowadzająca zobowiązana jest dokonać wpisu w „Rejestrze wejść” oraz osobiście nadzorować pobyt gościa w obszarze bezpiecznym.
13. Pracownicy powinni szczególnie zwracać uwagę na obce osoby na terenie firmy, zwłaszcza, gdy pozostają one bez opieki innego pracownika firmy i bezzwłocznie zgłaszać takie przypadki pracownikom komórki bezpieczeństwa ABC.
14. Pracownicy zobowiązani są do używania wyłącznie sprzętu komputerowego i oprogramowania, zatwierdzonego do użytkowania w ABC S.A. Zabrania się podłączania do systemu teleinformatycznego wykorzystywanego przez ABC i używania jakichkolwiek urządzeń nie posiadających autoryzacji, w tym między innymi prywatnych środków do przetwarzania informacji, takich jak laptopy czy urządzenia komunikacji mobilnej.
15. Systemy przetwarzania informacji (m.in. informatyczne, telekomunikacyjne) mogą być wykorzystywane tylko w celach służbowych.
16. Efekty pracy pracownika, w tym oprogramowanie i dokumentacja wytworzone na użytek ABC S.A., stanowią własność Spółki i nie mogą być wynoszone lub przekazywane poza teren firmy. W odniesieniu do służbowych komputerów przenośnych przyjmuje się jako zasadę, że przydzielenie pracownikowi służbowego komputera przenośnego jest jednoznaczne z udzieleniem mu zgody na wynoszenie takiego komputera i przetwarzanie na nim informacji chronionej poza terenem firmy, o ile komputer taki spełnia wymagania, o których mowa w pkt. 47.
17. W celu zapewnienia przetwarzanym w Spółce informacjom odpowiedniej ochrony, prowadzony jest monitoring działań w systemach teleinformatycznych oraz na obszarze ABC S.A. tym samym ABC SA zastrzega sobie prawo kontroli wszystkich danych przechowywanych lub przekazywanych za pomocą w/w systemów.
18. Po zakończeniu pracy nie wolno zostawiać niezabezpieczonych dokumentów zawierających informacje chronione inne niż „informacja jawna”. Należy stosować zasadę „czystego biurka” w odniesieniu do dokumentów i wymiennych nośników informacji oraz zasadę „czystego ekranu” (np. zablokowanie stacji) w odniesieniu do urządzeń przetwarzania informacji, a także zadbać o odpowiednie ustawienie monitora, tak aby informacje chronione inne niż „informacja jawna” wyświetlane na ekranie komputera nie były dostępne osobom nieuprawnionym.
19. Wymagane jest zabezpieczenie poufności informacji metodami kryptograficznymi (np. przy użyciu programu PGP lub standardu S/MIME poczty elektronicznej) w przypadkach:
    a) przesyłania poprzez Internet, w tym pocztą elektroniczną, informacji chronionych oznaczonych klauzulą inną niż „informacja jawna”;
    b) przekazywania na nośnikach elektronicznych poza siedzibę Spółki informacji chronionych oznaczonych klauzulą inną niż „informacja jawna”.
20. Poczta elektroniczna ABC służy do celów służbowych. Informacje przesyłane za pośrednictwem systemów teleinformatycznych użytkowanych przez ABC (w tym do i z Internetu) nie stanowią własności prywatnej pracownika.
21. Zabronione jest:
    a) wysyłanie na konta prywatne dokumentów służbowych,
    b) wykorzystywanie systemu poczty elektronicznej do działań mogących zaszkodzić lub szkodzących wizerunkowi ABC,
    c) otwieranie przesyłek z nieznanych źródeł,

d) otwieranie załączników z plikami samorozpakowującymi się bądź wykonalnymi typu bat, exe, com, itp, bez sprawdzenia oprogramowaniem antywirusowym,

e) ukrywanie lub dokonywanie zmian tożsamości nadawcy poczty elektronicznej,

f) nieautoryzowane czytanie, usuwanie, kopiowanie lub zmienianie zawartości skrzynek pocztowych innego użytkownika,

g) otwieranie wiadomości elektronicznych oraz odpowiadanie na niezamawiane informacje handlowe lub tzw. „łańcuszki” oraz na inne formy wymiany danych określane jako spam,

h) posługiwanie się adresem służbowym poczty elektronicznej w celu rejestrowania się w serwisach internetowych niedotyczących obowiązków służbowych,

i) wykorzystywanie poczty elektronicznej do reklamy prywatnych towarów lub usług, działalności handlowo-usługowej innej niż wynikającej z potrzeb ABC oraz do poszukiwania innego zatrudnienia.

22. Pracownik zobowiązany jest do przestrzegania zakazu prowadzenia rozmów, podczas których może dochodzić do wymiany informacji chronionych innych niż „informacja jawna”, jeśli rozmowy te odbywają się w miejscach publicznych lub takich, które nie gwarantują zachowania poufności rozmów.

23. Pracownik zobowiązany jest do przestrzegania zakazu wysyłania wiadomości (SMS, MMS) zawierających informacje chronione inne niż „informacja jawna”.

24. Drukarki i urządzenia kserograficzne nie mogą być pozostawione bez nadzoru podczas drukowania (kopiowania) dokumentów zawierających informacje chronione inne niż „informacja jawna”.

25. W sytuacji wystąpienia niewłaściwej pracy drukarki, faksu lub urządzenia kserograficznego (np. błędy transmisji, zacięcie papieru itp.) użytkownik zobowiązany jest do usunięcia z podręcznej pamięci urządzenia (o ile udostępnia ono użytkownikowi taką funkcjonalność) pozostawionej tam informacji chronionej innej niż „informacja jawna”, uniemożliwiając w ten sposób nieuprawnione jej odzyskanie.

26. Zabronione jest pozostawianie wiadomości zawierających informacje chronione inne niż „informacja jawna” w skrzynkach poczty głosowej.

27. W przypadku korzystania z trybu skróconego wybierania numeru w urządzeniach faksowych, przed zaakceptowaniem wysłania, użytkownik zobowiązany jest upewnić się, że nie doszło do umyślnej zmiany wybieranego numeru.

28. Jeśli istnieje możliwość techniczna, to należy korzystać z blokad urządzeń kserograficznych, drukarek lub faksów.

29. Pracownik zobowiązany jest do zabezpieczenia oryginałów i kopii dokumentów zawierających informacje chronione inne niż „informacja jawna”, które zostały pozostawione w pobliżu urządzeń kserograficznych, faksów lub drukarek.

30. Zabronione jest wykonywanie bez zgody ABI zdjęć oraz wideofilmowanie pomieszczeń lub ich części zajmowanych przez ABC, które ujawniałoby informacje chronione inne niż „informacja jawna”, zastosowane środki bezpieczeństwa systemów teleinformatycznych i systemów ochrony fizycznej.

31. Pracownik ma obowiązek zniszczyć, w sposób uniemożliwiający odtworzenie, wszelkie tradycyjne nośniki informacji (np. dokumenty papierowe) oraz zewnętrzne nośniki elektroniczne (np. dyskietki, płyty CD/DVD) zawierające informacje chronione inne niż „informacja jawna”, niezwłocznie po podjęciu decyzji o ich zbędności lub uzyskaniu wiarygodnej informacji o podjęciu takiej decyzji przez uprawnioną osobę. Nośniki takie należy zniszczyć w specjalnie do tego celu przeznaczonych urządzeniach (niszczarki papieru, niszczarki nośników elektronicznych).

32. Inne niż wymienione w pkt. 31 nośniki uszkodzone, wycofywane z eksploatacji lub przeznaczone do ponownego użycia, użytkownik przekazuje komórce wskazanej przez komórkę bezpieczeństwa ABC bezpieczeństwo@abc.pl

33. Należy unikać gromadzenia ważnych danych na dysku lokalnym komputera użytkownika. Powinny one być zapisywane na dyskach serwera (np. **\\abc_store\users\login**). Wyjątkiem od tej reguły jest brak możliwości technicznych, ale wówczas należy takie przypadki zgłaszać komórce bezpieczeństwa ABC. Celem przechowywania danych na serwerze jest zarówno zmniejszenie rozproszenia danych, jak i ochrona przed ich utratą przez automatyczne wykonywanie kopii zapasowych.

34. Każdy użytkownik posiada własny, unikalny identyfikator w systemie teleinformatycznym, który wraz z mechanizmem uwierzytelniania (np. hasło, czytnik z kartą mikroprocesorową, token itp.) umożliwia dostęp do systemu.

35. Pierwsze logowanie (rejestracja) użytkownika w systemie teleinformatycznym lub systemie kontroli dostępu fizycznego odbywa się przy użyciu tymczasowego – odpowiednio – hasła lub kodu dostępu, definiowanego przez administratora systemu podczas tworzenia konta użytkownika w systemie. Takie tymczasowe hasło/kod jest przeznaczone wyłącznie do jednorazowego użycia - użytkownik zobowiązany jest do niezwłocznej zmiany hasła/kodu tymczasowego na nowe, tylko jemu znane, spełniające wymagania, o których mowa poniżej

36. Należy używać haseł o właściwej i zalecanej jakości, tj.:

    a) o długości co najmniej 8 znaków,

    b) zawierające wielkie i małe litery oraz cyfry i znaki specjalne (np. @#$%^&:’’<>?),

    c) nie opartych na prostych skojarzeniach, łatwych do odgadnięcia lub wywnioskowania z informacji dotyczących danej osoby (np. imiona, numery telefonów, daty urodzenia itp,), ale jednocześnie łatwe do zapamiętania,

    d) nie zawierające identyfikatora użytkownika,

    e) zmieniane nie rzadziej, niż co 30 dni.

37. Użytkownikom zabrania się ujawniania lub udostępniania hasła/kodu innym osobom lub pozostawiania hasła/kodu w miejscu umożliwiającym jego poznanie/przejęcie. W przypadku wykorzystania hasła/kodu przez inną osobę, osoba, która nie zabezpieczyła należycie własnego hasła/kodu ponosi pełną odpowiedzialność za wszystkie działania wykonane z wykorzystaniem tego hasła/kodu.

38. Jeżeli zachodzi podejrzenie ujawnienia hasła/kodu, to użytkownik ma obowiązek niezwłocznie zmienić hasło/kod oraz powiadomić bezpośredniego przełożonego i ABI.

39. Zabronione jest:

    a) zapisywanie haseł/kodów w sposób jawny i umieszczania ich w miejscach dostępnych dla innych osób (np. na papierze, w pliku, na urządzeniu przenośnym etc.),

    b) wykorzystywanie haseł/kodów innych użytkowników,

    c) przeprowadzanie prób łamania haseł/kodów,

    d) powtarzanie haseł/kodów lub „cykliczne” używanie starych haseł/kodów,

    e) wprowadzanie haseł/kodów do jakichkolwiek zautomatyzowanych procesów logowania się do systemu lub aplikacji za wyjątkiem kont technicznych,

    f) korzystania z takiego samego hasła/kodu w celach służbowych i niezwiązanych z działalnością służbową,

    g) stosowanie haseł/kodów w postaci sekwencji kolejnych znaków na klawiaturze,

40. Każdy użytkownik korzystający z kluczy kryptograficznych jest zobowiązany do ich użytkowania i przechowywania w sposób uniemożliwiający utratę lub dostęp osób nieuprawnionych.

41. Użytkownikom zabrania się samodzielnego instalowania i wprowadzania zmian do oprogramowania, sprzętu komputerowego oraz podłączania do sieci komputerowej. Potrzeby tego rodzaju należy zgłaszać do Helpdesk (za pośrednictwem systemu Bugzilla – grupa **HelpDesk**). Wyjątek od tej reguły stanowią pracownicy, dla których w/w działania stanowią zakres obowiązków służbowych (w szczególności administratorzy systemów).

42. Wszelkie nieprawidłowości związane z funkcjonowaniem sprzętu teleinformatycznego oraz systemów teleinformatycznych, w tym także przypadki wykrycia wirusa, użytkownik zobowiązany jest zgłaszać do Helpdesk za pośrednictwem systemu Bugzilla (grupa **HelpDesk**); w przypadku braku dostępu do systemu Bugzilla dopuszcza się dwa inne kanały zgłaszania: e-mail **helpdesk@abc.pl** oraz całodobowy **tel. (22) 555 5555** (lub numer wewnętrzny: **5555**).

43. W przypadku zaobserwowania incydentu bezpieczeństwa informacji innego, niż określone w pkt. 42 pracownik zobowiązany jest niezwłocznie zgłosić to bezpośredniemu przełożonemu oraz komórce bezpieczeństwa ABC (**bezpieczeństwo@abc.pl**) lub ABI, a w przypadkach pilnych, poza godzinami pracy oraz gdy skuteczny kontakt ze wskazanymi wyżej osobami nie jest możliwy – telefonicznie do Helpdesk, całodobowo **tel.: (22) 555 5555** (lub numer wewnętrzny: **5555**). Za incydent bezpieczeństwa informacji, o którym mowa w niniejszym punkcie uznaje się w szczególności:

a) utratę, ujawnienie lub podejrzenie utraty lub ujawnienia informacji chronionych innych niż „informacja jawna” (np. danych osobowych);
b) kradzież sprzętu,
c) naruszenie zabezpieczenia systemów teleinformatycznych przetwarzających informacje chronione;
d) taki stan urządzenia, zawartość zbioru informacji chronionych, ujawnione metody pracy, sposób działania oprogramowania lub jakość komunikacji w sieci teleinformatycznej, który może wskazywać na naruszenie bezpieczeństwa informacji,
e) naruszenie lub wadliwe funkcjonowanie zabezpieczeń fizycznych w pomieszczeniach,
f) utratę identyfikatora wykorzystywanego w systemie kontroli dostępu,
g) naruszenie bezpieczeństwa klucza kryptograficznego.

44. Użytkownikom zabrania się:

a) testowania oraz podejmowania prób poznania i łamania zabezpieczeń systemów teleinformatycznych bez pisemnej zgody ABI;
b) ujawniania informacji odnoszących się do funkcjonowania systemów teleinformatycznych ABC, w szczególności dotyczących zidentyfikowanych podatności, awarii, incydentów bezpieczeństwa informacji, o ile uprawniony organ państwowy nie zwolni użytkownika z zachowania tajemnicy,
c) przechowywania i uruchamiania plików multimedialnych nie związanych z celami służbowymi;
d) korzystania z danych uzyskanych z sieci zewnętrznych (tj. spoza sieci komputerowej Spółki), zanim te dane nie zostaną sprawdzone przez oprogramowanie antywirusowe;
e) nieautoryzowanego, tj. nie wynikającego z zakresu obowiązków służbowych, dokonywania napraw systemów teleinformatycznych,
f) umożliwiania dostępu do systemów teleinformatycznych osobom nieupoważnionym,
g) korzystania z konta innego użytkownika, chyba że część lub całość zasobów związanych z tym kontem są udostępniane,
h) nieautoryzowanego niszczenia danych gromadzonych w systemach teleinformatycznych, w szczególności takiego, którego celem jest umyślne działanie na szkodę Spółki (np. zamiar ukrycia dowodów, działanie złośliwe) lub takiego, które jest skutkiem niezachowania należytej staranności (np. nieupewnienie się, że niszczone dane są zbędne).
i) kopiowania oprogramowania oraz danych będących w posiadaniu ABC dla celów prywatnych,
j) świadomego wprowadzania błędnych danych do systemów teleinformatycznych,
k) korzystanie ze stron internetowych o treściach pornograficznych, erotycznych, rasistowskich, użytkowanych przez grupy przestępcze i terrorystyczne,
l) wykorzystywania materiałów zawierających logo ABC w celach prywatnych,
m) pobierania z sieci, kopiowania, przechowywania lub rozprowadzania oprogramowania, utworów muzycznych lub wideo oraz innych plików, których używanie może powodować naruszenie praw autorskich lub powodować naruszenie bezpieczeństwa systemu teleinformatycznego.

45. Użytkownik ponosi finansowe i prawne konsekwencje posiadania nieautoryzowanego oprogramowania w przypisanym mu komputerze lub zasobach sieciowych.

46. Użytkownicy systemów informatycznych mają obowiązek stosować się do wymagań określonych przez ABI oraz poszczególnych Administratorów Systemów (AS).

47. Komputery przenośne oraz wymienne nośniki informacji, na których znajdują się informacje chronione inne niż „informacja jawna”, nie mogą być pozostawione bez zabezpieczenia fizycznego (m.in. zamknięcie pomieszczenia, zamknięcie komputera w szafie) i logicznego (wyłączenie, zawieszenie sesji lub wylogowanie z systemu). Ponadto we wszystkich komputerach przenośnych stosuje się – jako zabezpieczenie bezwzględnie wymagane – szyfrowanie dysków lokalnych wykonane zgodnie z obowiązującą w ABC procedurą.

48. Użytkownik jest zobowiązany nie pozostawiać w napędach wymiennych nośników zawierających informacje chronione inne niż „informacja jawna”.

49. Udzielenie informacji związanych z działalnością firmy osobom nieupoważnionym, niezidentyfikowanym, a zwłaszcza informacji o charakterze strategicznym np. o toczących się projektach (zagrożenie wyłudzenia informacji poprzez stosowanie **socjotechniki**) stanowi rażące naruszenie obowiązków pracowniczych.

50. W celu ochrony przed potencjalnym atakiem socjotechnicznym, wszyscy użytkownicy zobowiązani są do postępowania zgodnie z poniższymi zaleceniami:

    a) nieoczekiwane maile od nieznanych nadawców, zwłaszcza zawierające różnego rodzaju załączniki, odsyłacze/linki itp. należy kasować, najlepiej przed przeczytaniem;

    b) nie należy używać odsyłaczy w wiadomościach e-mail w celu załadowania strony internetowej, najlepiej samodzielnie wpisywać adres URL do przeglądarki internetowej;

    c) nie wolno używać nieznanych wymiennych nośników informacji (np. dyskietek, płyt CD/DVD, pendrive'ów), czy otwierać dokumentów elektronicznych pochodzących z nieznanego źródła oraz instalować niewiadomego pochodzenia programów (w przypadku wątpliwości kontaktować się z komórką bezpieczeństwa ABC);

    d) należy zawsze mieć kontrolę nad posiadanymi i udostępnianymi informacjami oraz być świadomym stopnia uwierzytelnienia (zaufania, pewności) swoich rozmówców, a w razie jakichkolwiek wątpliwości uwierzytelniać te osoby wykorzystując przełożonych lub inne znane obu stronom zaufane osoby, natomiast w sytuacjach niejasnych odmówić udzielenia informacji i poprosić o kontakt z Recepcją (mail: recepcja@abc.pl; tel.: **(22) 555 5500**);

    e) każdą nieznaną sobie osobę, zarówno dzwoniącą do firmy, jak i pojawiającą się osobiście, pracownik zobowiązany jest zidentyfikować na wszystkie dostępne sposoby (np. prośba o okazanie dokumentu tożsamości ze zdjęciem, kontakt ze znanymi obu stronom zaufanymi osobami), jednocześnie nie należy wykonywać żadnych próśb czy poleceń gościa/rozmówcy, dopóki nie będziemy pewni jego tożsamości;

    f) należy regularnie i dokładnie niszczyć wszelkiego rodzaju zbędną dokumentację i inne niepotrzebne materiały drukowane, przeznaczone do użytku wewnętrznego, mogące zawierać informacje chronione inne niż „informacja jawna”.

51. Pracownik jest zobowiązany zapoznać się z dokumentami wewnętrznymi ABC dotyczącymi bezpieczeństwa informacji obowiązującymi na jego stanowisku pracy. Pracownik jest również zobowiązany zapoznawać się ze wszystkimi uaktualnieniami tychże dokumentów ogłaszanymi w sposób zwyczajowo przyjęty w ABC.

52. Nieprzestrzeganie **zasad określonych w dokumentach wewnętrznych ABC dotyczących bezpieczeństwa informacji stanowi ciężkie naruszenie podstawowych obowiązków pracowniczych i podlega odpowiedzialności dyscyplinarnej określonej w Regulaminie pracy.**

53. Jeżeli **skutkiem działania jest ujawnienie informacji osobie nieuprawnionej, pracownik może zostać pociągnięty do odpowiedzialności karnej wynikającej ze stosownych przepisów prawa**

54. Jeżeli **skutkiem działania jest szkoda dla ABC, pracownik ponosi odpowiedzialność materialną na warunkach określonych w przepisach kodeksu pracy oraz prawa cywilnego.**

……
imię i nazwisko Pracownika

……
komórka organizacyjna

Oświadczenie

Oświadczam, że zapoznałem/am się, rozumiem i przyjmuję do wiadomości i stosowania wszystkie zasady określone w dokumencie „Podstawowe zasady bezpieczeństwa informacji w ABC”, stanowiącym Załącznik nr 34 do dokumentu XXX_ABC „Zasady ochrony informacji”.

Niniejsze oświadczenie zostało sporządzone w dwóch jednobrzmiących egzemplarzach – jeden dla ABC S.A.[1] oraz jeden dla osoby przyjmującej do wiadomości i stosowania powyższe zasady zapewnienia bezpieczeństwa informacji w ABC S.A.

……
data i podpis Pracownika

……
data i podpis osoby przyjmującej oświadczenie Pracownika