Tech Solution Partner Tomasz Kowalski
ul. Marynarki Wojennej 3C/31
33-100 Tarnów
NIP: 6783217048

Tech Solution Partner
TOMASZ KOWALSKI

ZASADY PRACY ZGODNIE Z RODO

I. Polityka czystego biurka

1. Pracujący z danymi osobowymi w formie papierowej należy zabezpieczać je przed kradzieżą lub wglądem osób nieupoważnionych.
2. Nie należy pozostawiać dokumentów zawierających dane osobowe (a także inne istotne dla firmy dane i informacje) podczas swojej nieobecności, w szczególności gdy w obszarze przetwarzania danych osobowych pojawia się osoba nieupoważniona (np. klienci, których dane nie dotyczą, kurier, inne osoby nieupoważnione itp.).
3. Kończąc pracę należy w miarę możliwości schować całą dokumentację papierową zawierającą dane osobowe (a także tą, która zawiera inne istotne dla organizacji dane i informacje) do zamykanych szaf i szuflad, stosując w ten sposób techniczne środki zabezpieczenia przetwarzania danych osobowych.
4. Dokumenty z danymi/ wydruki z danymi osobowymi, które nie są już potrzebne należy niszczyć w niszczarce.
5. Powyższe zapisy mają także zastosowanie odpowiednio do przenośnych fizycznych nośników danych.

II. Polityka czystego ekranu

1. Monitor komputera wyposażony jest we włączający się samoczynnie wygaszacze ekranu. Wznowienie wyświetlenia następuje dopiero po wprowadzeniu odpowiedniego hasła.
2. Ekran laptopa powinien być, w miarę możliwości, ustawiony tak by w momencie pojawienia się osób nieupoważnionych w pomieszczeniu, osoby te nie mogły widzieć treści wyświetlanych na ekranach.

III. Zasady użytkowania sprzętu informatycznego

Zalecenia:

1. Skonfiguruj hasło administracyjne do BIOS-u,
2. Szyfruj dane na dysku, w tym dyskach przenośnych.
3. Wyposaż sprzęt mobilny w oprogramowanie umożliwiające jego nadzór, blokowanie dostępu, czyszczenie zawartości,
4. Aktualizuj oprogramowanie systemów i aplikacji, urządzeń sieciowych i innych (systemy operacyjne/ przeglądarki www / CMS (Wordpress) / Dedykowany CMS / inne). Aktualizacja dokonywana jest zgodnie z zaleceniami producentów oraz opinią rynkową co do bezpieczeństwa i stabilności nowych wersji (np. aktualizacje, service pack-i, łatki)
5. Wprowadza się zakaz korzystania z nośników danych pochodzących od podmiotów zewnętrznych (np. podłączenie znalezionego pendrive do laptopa), z zastrzeżeniem wyjątkowych sytuacji.

Szyfrowanie jest metodą zapewnienia bezpieczeństwa danych.

6. Stosuje się szyfrowanie poczty wychodzącej (SSL) a także szyfrowanie połączeń internetowych z użyciem protokołu SSL (np. bezpłatny certyfikat SSL Let's Encrypt).
7. Stosuje się szyfrowanie dysku oraz nośników zewnętrznych w celu ochrony danych na wypadek np. kradzieży czy innej utraty nośnika.

Naprawa sprzętu

8. Rekomendowane jest korzystanie z serwisu, który dokonuje napraw u klienta.
9. Czynności konserwacyjne i naprawcze wykonywane przez osoby nieposiadające upoważnień do przetwarzania danych (np. specjalistów z firm zewnętrznych) muszą być wykonywane pod nadzorem osób upoważnionych.
10. Wszelkie prace konserwacyjne i naprawcze sprzętu komputerowego oraz uaktualnienia systemu informatycznego wykonywane przez podmiot zewnętrzny, powinny odbywać się na zasadach określonych w szczegółowej umowie z uwzględnieniem klauzuli dotyczącej ochrony danych.
11. W przypadku napraw dokonywanych na zewnątrz (z komputerów należy uprzednio wymontować dyski i wszelkie nośniki, z urządzeń mobilnych karty pamięci, usunąć dane z nośnika z użyciem specjalistycznego oprogramowania, a jeśli to nie jest możliwe- rekomendowane jest przekazywanie do naprawy uszkodzonego sprzętu z danymi zaszyfrowanymi na dysku / karcie pamięci.

IV. Procedura korzystania z telefonów

1. Należy unikać prowadzenia rozmów telefonicznych w miejscach publicznych, w czasie których wypowiada się informacje dot. danych osobowych, mogących w jakikolwiek sposób zidentyfikować osobę, o której się mówi.
2. Podczas korzystania z poczty e-mail za pośrednictwem telefonu/komputera należy wyłączyć opcję autozapamiętywania hasła do tej poczty.
3. Nie należy korzystać z otwartych sieci wi-fi, w szczególności w celu logowania się z hotspot na pocztę e-mail czy do chmury lub do innych miejsc, w których znajduje się dane osobowe objęte ochroną.
4. Telefon powinien zostać zabezpieczony silnym kodem, tj. np. nie będącym ciągiem cyfr/datą urodzenia, nie przyjmujący znaku w postaci kwadratu, prostokąta, trójkąta czy też liter C, M, W, U. Telefon powinien być zabezpieczony przy użyciu metody/znaku/hasła, która utrudni użycie telefonu przez nieupoważnione osoby.
5. Telefon powinien być zaszyfrowany.
6. Telefon powinien mieć zainstalowane oprogramowanie antywirusowe .
7. Instalując aplikacje na telefonie należy sprawdzać czy pochodzą z wiarygodnego źródła oraz jaki zakres informacji chcą uzyskać (Informacja ta wyświetla się przy instalowaniu; instalowanie najczęściej nie rozpoczyna się zanim nie wyrazi się zgody na dostęp do ww. informacji) .

V. Polityka haseł

Hasło to podstawowa bariera chroniąca zarówno dane osobowe we wszelkiego rodzaju programach, systemach, aplikacjach.

1. Dostęp do systemu/ konta/aplikacji powinien być możliwy wyłącznie co najmniej po wprowadzeniu właściwego identyfikatora i właściwego hasła.
2. Nie można używać w serwisach internetowych takich samych lub podobnych haseł jak w systemie komputerowym firmy. Do każdej aplikacji/ konta/ systemu powinno być stworzone inne hasło.
3. Hasła nie mogą być łatwe do odgadnięcia.
4. Nie twórz haseł, które:
   - będą odnosiły się do właściciela konta, tzn. będą zawierały w sobie np. imię, nazwisko, daty urodzenia, inne ważne daty, PESEL, imiona dzieci, nazwę firmy, numerów rejestracyjnych auta itp.
   - będą składały się z prostego ciągu znaków typu QWERTY (ciąg znaków z klawiatury), 12345 czy 11111 lub odnosiły się do innych popularnych haseł typu STARWARS, ADMIN itp.,

- nie twórz haseł w oparciu o jeden, nawet skomplikowany wzór. W ten sposób „wykradniecie" jednego hasła i wygenerowanie kolejnych przez inne osoby nadal będzie prostym zadaniem. Przykład błędnego tworzenia haseł: E089$09080KIRFT543 i kolejne hasła powstające w oparciu o poprzednie wzbogacone o kilka cyfr typu E089$09080KIRFT543123.

5. Zaleca się korzystanie z Managera haseł (np. Program KeePass), dzięki któremu możliwe jest bezpieczne generowanie, przechowywanie i wprowadzanie haseł na stronach www, do poszczególnych kont itp.
6. Należy zachowywać hasła w poufności, nawet po utracie przez nie ważności lub zmianie.
7. Zmiana hasła powinna następować nie rzadziej niż co 90 dni;
8. Należy zmieniać hasło zawsze gdy zachodzi podejrzenie, że ktoś mógł uzyskać informacje o haśle.
9. Użytkownicy są odpowiedzialni za zachowanie poufności swoich haseł. Hasła nie powinny być ujawnianie innym osobom. Nie należy zapisywać haseł na kartkach i w notesach, nie naklejać na monitorze komputera, nie trzymać pod klawiaturą, itp.
10. W systemach umożliwiających zapamiętanie nazwy użytkownika lub jego hasła nie należy korzystać z tego ułatwienia.

Dwukrotne uwierzytelnianie

11. Do miejsc ważnych z punktu widzenia prowadzenia działalności, a także do miejsc takich jak prywatna skrzynka e-mailowa, na której znajduje się istotne informacje powinno stosować się co najmniej dwukrotne uwierzytelnianie.
12. Możliwości uwierzytelniania dwuskładnikowego można sprawdzić na stronie WWW: https://twofactorauth.org

VI. Ochrona antywirusowa

1. Podstawowym sposobem zabezpieczenia przed ww. oprogramowanie jest zastosowanie, na wszystkich stacjach roboczych, serwerach, komputerach przenośnych oprogramowania antywirusowego. Stosowany jest firewall programowy.
2. Oprogramowanie antywirusowe jest cykliczne i automatycznie aktualizowane. Zaleca się okresowe monitorowanie czy aktualizacja ta przebiega bez zakłóceń.
3. Oprogramowanie, o którym mowa w pkt 2, sprawuje ciągły nadzór (ciągła praca w tle) nad pracą systemu i jego zasobami oraz serwerami i stacjami roboczymi.

VII. Zabezpieczenie dokumentacji papierowej zawierającej dane osobowe

1. Pracujący z danymi osobowymi są zobowiązani do stosowania tzw. „Polityki czystego biurka". Polega ona na zabezpieczaniu przed kradzieżą lub wglądem osób nieupoważnionych do dokumentów oraz nośników (np. chowanie do szaf, biurek).
2. Pracujący z danymi osobowymi zobowiązani są do niszczenia dokumentów i wydruków, które utraciły przydatność i nie objęte są obowiązkiem ich przechowywania i archiwizowania. Usuwanie tych dokumentów następuje w niszczarkach.
3. Zabrania się pozostawiania dokumentów z danymi osobowymi poza zabezpieczonymi pomieszczeniami.

VIII. Zasady korzystania z poczty elektronicznej

1. W przypadku przesyłania danych osobowych poza organizację należy ocenić czy zasadne byłoby w określonym przypadku wysłanie pliku zaszyfrowanego/ spakowanego (np. programem 7 zip, winzipem, winrarem) i zahasłowane, gdzie hasło powinno być przesłane do odbiorcy telefonicznie SMS, lub kolejną wiadomością e-mail.
2. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy.
3. Należy zwracać uwagę na przypadki podejrzanych e-maili (np. wiadomości z fakturami od podmiotów, od których Administrator nie spodziewał się faktury, wezwania z Urzędów z błędami).
4. Podczas wysyłania maili do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości – UDW". Zabronione jest rozsyłanie maili do wielu adresatów z użyciem opcji „Do wiadomości"
5. Użytkownicy powinni okresowo kasować niepotrzebne maile.

IX. Kopie zapasowe

Tworzenie kopii zapasowych to jeden ze środków technicznych pozwalających na zapewnienie dostępności danych osobowych w celu ochrony danych np. przed ich utratą.

1. Kopie zapasowe tworzy się na bieżąco.
2. W szczególności należy wykonywać następujące kopie bezpieczeństwa:

   1) przed dokonaniem zmian w konfiguracji systemów lub oprogramowania,

   2) przed dokonaniem zmian w programach (np. zmiana wersji).

4. Zasady dot. tworzenia kopii zapasowych.
   Zaleca się stosowanie metody 3-2-1 rekomendowanej przez US-CERT[1]
   1) 3 egzemplarze, tzn. 1 oryginał + 2 kopie danych zapisanych na różnych nośnikach,
   2) 2 różne formaty - np. jeśli dane pierwotne są przechowywane w formie papierowej, warto je np. zeskanować i przechowywać w formie elektronicznej np. w chmurze, na skrzynce pocztowej, nośnikach zewnętrznych.
      UWAGA! W przypadku zapisywania kopii zapasowych na nośnikach zewnętrznych należy pamiętać o ich zaszyfrowaniu.
   3) 1 kopia poza firmą (w tym m.in. w chmurze): zmniejsza ryzyko utraty danych na wypadek zdarzeń związanych bezpośrednio z firmą.

5. W celu zapewnienia poprawności wykonywanych kopii bezpieczeństwa należy co najmniej raz na kwartał poddać testowi cyklicznie wybraną kopię. Próba polega na odtworzeniu danych w warunkach testowych i sprawdzeniu, czy jest możliwość odczytania danych.
6. Nośniki zawierające nieaktualne kopie danych, likwiduje się. W przypadku nośników jednorazowych, takich jak płyty CD-R, DVD-R, likwidacja polega na ich fizycznym zniszczeniu w taki sposób, by nie można było odczytać ich zawartości. Nośniki wielorazowego użytku, takie jak dyski twarde, pendrive, płyty CD-RW, DVD-RW, można wykorzystać ponownie do celów przechowywania kopii bezpieczeństwa po uprzednim usunięciu ich zawartości.
7. Nośniki wielorazowego użytku nienadające się do ponownego użycia należy zniszczyć fizycznie.

[1] United States Computer Emergency Readiness Team