NASK

CyberBHP

Bezpieczne Stanowisko Pracy – Twoja Odpowiedzialność!

Odpowiedzialność za bezpieczeństwo danych i informacji to priorytet każdej firmy, a **pracownicy mają istotną rolę do odegrania w minimalizacji ryzyka cyberataków. Jednym ze sposobów jest stosowanie kilku prostych zasad,** które podniosą poziom bezpieczeństwa w organizacji i zmniejszą ryzyko utraty, ujawnienia lub udostępnienia danych. **Zasady te dotyczą: czystego biurka, ekranu, kosza i wydruku.** W każdym tych miejsc przetwarzane są dane osobowe, poufne i wrażliwe informacje, dlatego tak istotne jest przestrzeganie w codziennej pracy zasad, które zwiększą bezpieczeństwo firmy i uchronią ją przed zagrożeniami.

Zasada czystego biurka

Polega na przechowywaniu dokumentów poza zasięgiem wzroku osób postronnych oraz niepozostawianiu dokumentów bez nadzoru podczas naszej nieobecności przy stanowisku pracy.

Zasada ta dotyczy:

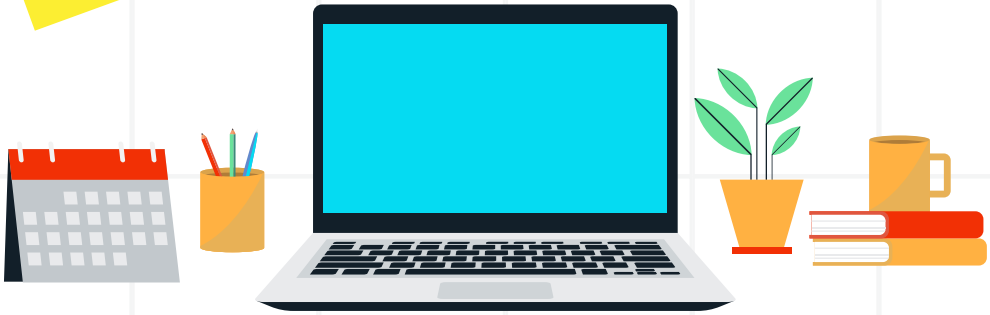
dokumentów papierowych jak np. faktury, umowy, rachunki, wizytówki, odręczne notatki, itp,

dokumentów zapisanych na nośnikach elektronicznych np. płyty CD, USB, dyski zewnętrzne czy pieczątki,

przestrzeni wokół miejsca pracy jak np.: szafki, półki czy tablice korkowe.

Nie umieszczaj i nie przechowuj czy to na biurku, czy przypiętych do tablicy, luźnych kartek, z poufnym numerami telefonów, numerów PIN, itp. a w szczególności danych logowania do komputera.

Usuwaj notatki z tablicy, flipcharta od razu po zakończeniu spotkania, na którym omawiane były kwestie istotne dla firmy, ewentualnie po skończonej pracy.



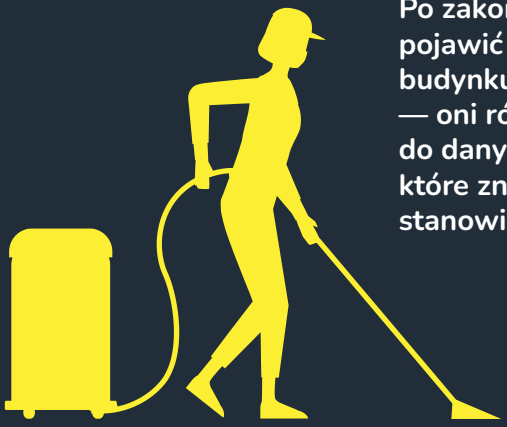
NASK

Jeśli decydujesz się na włączenie kamery internetowej, sprawdź, co znajduje się w tle. Czy nie ma tam żadnych osobistych ani wrażliwych informacji, których nie powinieneś pokazywać w trakcie połączenia. Skorzystaj z programów do obsługi wideokonferencji, które pozwalają na rozmycie lub ustawienie wirtualnego tła, dzięki czemu inni uczestnicy nie widzą tego, co znajduje się z tyłu za Tobą.

Każdorazowo opuszczając stanowisko pracy wszystkie dokumenty i nośniki danych schowaj w miejscu odpowiednio chronionym – np. w kontenerze, szafce na zamek, a klucze do nich zabierz ze sobą albo przekaż odpowiedzialnej za to osobie w firmie, która przechowa go w bezpiecznym, dedykowanym do tego miejscu.

Po zakończonym dniu pracy pozostaw biurko czyste. Nieprzydatne wersje dokumentów papierowych z danymi osobowymi, najpóźniej na koniec dnia pracy zniszcz w sposób uniemożliwiający odczytanie zawartych w nich informacji, np. za pomocą niszczarki.

Pamiętaj:



Po zakończeniu pracy w firmie mogą pojawić się osoby trzecie np. ochrona budynku, serwis sprzątający czy technicy — oni również nie mogą mieć dostępu do danych osobowych, dokumentów które znajdują się w otoczeniu Twojego stanowiska pracy.

NASK

Zasada czystego ekranu

Polega na uniemożliwieniu osobom nieupoważnionym dostępu do zawartości Twojego komputera.

Komputer czy laptop ustaw w taki sposób, aby uniemożliwić osobom postronnym, w tym także innym pracownikom wgląd w informacje wyświetlane na ekranie Twojego urządzenia lub co bardziej niebezpieczne, utrwalenie wpisywanych lub przeglądanych przez Ciebie treści np. przez zrobienie zdjęcia albo zapiski.

Stosuj filtr prywatyzujący, zwłaszcza gdy pracujesz zdalnie lub w otwartej przestrzeni.

Blokuj komputer za każdym razem, gdy od niego odchodzisz (windows + L).

Skonfiguruj automatyczny wygaszacz ekranu, który po upłynięciu kilkuminutowego czasu bezczynności blokuje dostęp do danych, a ponowny dostęp do komputera jest możliwy dopiero po wpisaniu spersonalizowanego hasła dostępu.

Jeśli chcesz udostępnić ekran komputera podczas wideokonferencji, pamiętaj, aby zamknąć wszystkie inne aplikacje i ukryć poufne pliki z pulpitu. Wyłącz także powiadomienia z aplikacji, unikniesz w ten sposób przypadkowego upublicznienia poufnych lub wstydliwych informacji. Zamiast udostępniać cały ekran komputera, zastanów się nad udostępnianiem tylko tej aplikacji, którą chcesz pokazać.

NASK

Po zakończeniu pracy w danym dniu, wyloguj się z systemu.

Przestrzeganie zasady „czystego ekranu” zapobiega obserwowaniu treści na ekranie przez osoby postronne i nieautoryzowanemu dostępowi nich. Komputery pozostawione bez nadzoru to możliwość wprowadzenia, modyfikowania lub usuwania danych w sposób nieautoryzowany. Wszystkie te sytuacje mogą mieć dla Ciebie albo firmy poważne konsekwencje, nawet prawne.

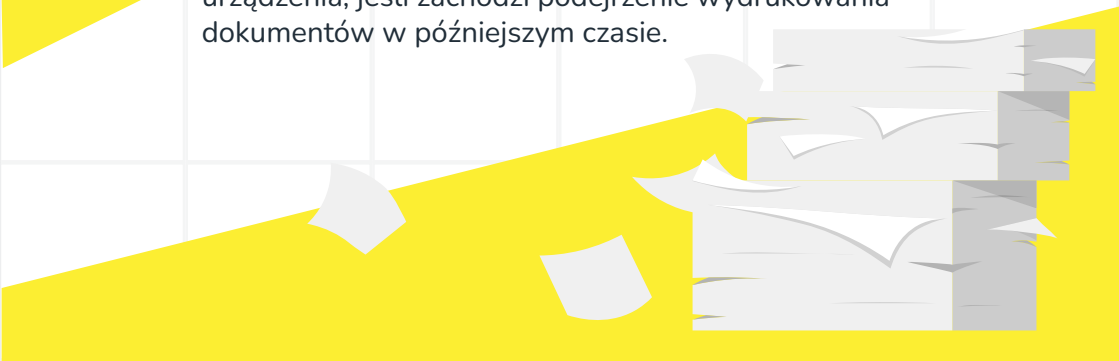
Zasada czystego wydruku

Polega na zabieraniu z urządzeń drukujących dokumentów zaraz po ich wydrukowaniu / skserowaniu / zeskanowaniu. Procedura ta jest szczególnie istotna w przypadku wielkopowierzchniowych pomieszczeń czy współdzielenia biur z innymi firmami.

Nie pozostawiaj urządzenia w trakcie drukowania/skanowania/kopiowania bez nadzoru, jeżeli materiały znajdujące się w urządzeniu zawierają dane osobowe i od razu zabierz je z drukarki.

Pamiętaj, aby po użyciu skanera usunąć plik z folderu sieciowego.

W przypadku braku wydruku, nieudanego wydruku lub pomyłki skontaktuj się z osobą odpowiedzialną za eksploatację urządzenia, jeśli zachodzi podejrzenie wydrukowania dokumentów w późniejszym czasie.



Zasada czystego kosza

Polega na niszczeniu dokumentów, na których znajdują się poufne informacje, w taki sposób, aby ich odczytanie było niemożliwe.

Wyjątek stanowią materiały promocyjne, marketingowe czy informacyjne.

Wszystkie dokumenty archiwalne, wersje robocze lub dokumenty, które już nie są Ci potrzebne należy zniszczyć w specjalnych niszczarkach. Pozwoli to uniknąć sytuacji, w której po odejściu od stanowiska pracy, osoba nieupoważniona uzyska łatwy dostęp do dokumentów.

Twoja świadomość i ostrożność są kluczowe dla ochrony bezpieczeństwa w miejscu pracy.

Omówione zasady nie wymagają dużego wysiłku, a jedynie systematyki. Stosując je działasz odpowiedzialnie i przyczyniasz się do zminimalizowania ryzyka naruszenia danych i ochrony firmy przed zagrożeniami.