Zawarte w poniższej broszurze informacje mają na celu przedstawienie podstawowych zasad dotyczących ochrony danych osobowych i ich bezpieczeństwa w miejscu pracy. Każdy pracownik, który ma do czynienia z danymi osobowymi, powinien szczególnie zwrócić na to uwagę, ponieważ nie przestrzeganie tych zasad zwiększa ryzyko ich kradzieży, zniszczenia czy też całkowitej utraty, a co za tym idzie poważnych konsekwencji zarówno dla pracodawcy jak i pracownika. Warto też pamiętać, że to te codzienne, podstawowe czynności wykonywane przez wszystkich pracowników mają ogromny wpływ na poziom bezpieczeństwa całej organizacji.

Ważne: poniższe zasady chronią nie tylko przed osobami z zewnątrz, ale również przed pracownikami z wewnątrz organizacji, którzy nie powinni mieć dostępu do danych zasobów.

Zasada „czystego biurka"- polega na zachowaniu porządku w przestrzeni swojego miejsca pracy:

- kiedy opuszczasz swoje miejsce pracy nie pozostawiaj żadnych dokumentów bez kontroli, najlepiej włóż je do szafy/szuflady, itp.
- zamykaj szafy z dokumentacją, najlepiej na klucz,
- dokumentację z nieaktualnymi danymi trwale usuwaj,
- zasada ta obejmuje wszystkie dokumenty w postaci papierowej (faktury, umowy, wizytówki, odręczne notatki), jak i te, które znajdują się na nośnikach elektronicznych (dyski zewnętrzne, pendrivy, itp.), ale też np. pieczątki.

Zasada „czystego wydruku"

Zbieraj dokumenty z urządzeń drukujących niezwłocznie po ich wydrukowaniu, podobnie w przypadku urządzeń wielofunkcyjnych gdzie możemy dokonać skserowania/zeskanowania dokumentu

Zasada „czystego ekranu" – zwraca uwagę na wzmożoną czujność oraz odpowiednie ustawienie, ale pamiętaj też o:

- korzystaniu tylko i wyłącznie ze swojego konta w systemie teleinformatycznym a po zakończonej pracy nie zapomnij się wylogować,
- ustawieniu wyświetlacza monitora tak, aby nikt postronny/nieupoważniony nie mógł zobaczyć co na nim wyświetlasz,
- dbaniu o „silne" hasła i nie udostępnianiu ich nikomu,
- okresowo zmienianiu hasła dostępu do komputera, poczty elektronicznej, itp.

Dodatkowo ważne w środowisku służbowym jest też, aby:

- zgłaszać przełożonemu wszelkie nieprawidłowości wynikające z pracy urządzeń takich jak komputer, laptop, telefon, itp.
- nie wyrzucać dokumentacji papierowej do kosza, a zniszczyć bezpiecznie w np. niszczarce lub specjalnym pojemniku do utylizacji dokumentów,
- nie logować się do kont korzystając z publicznych sieci Wi-Fi.

Wysyłając wiadomości zawierające dane osobowe zastosuj jedną z poniższych metod ochrony danych:

- anonimizację – usuń dane osobowe,
- pseudonimizację - część informacji wyślij mailem, a pozostałe dane przekaż innym kanałem komunikacji np. telefonicznie lub poprzez sms,
- szyfrowanie - dane osobowe umieść w osobnym pliku, a następnie zaszyfruj dokument. Zaszyfrowany plik załącz do wiadomości, a hasło do pliku prześlij innym kanałem komunikacji.

Do szyfrowania możesz skorzystać z dedykowanego programu, np. 7-Zip. W tym celu kliknij prawym przyciskiem myszy na plik lub katalog, który chcesz zaszyfrować i wybierz opcję "7-Zip", następnie kliknij "Dodaj do archiwum" i w polu "Szyfrowanie" wpisz wybrane przez siebie silne hasło. Szyfrowane potwierdź przyciskiem "Ok". Po zakończeniu procesu otrzymasz zaszyfrowany plik o rozszerzeniu .7z, który możesz bezpiecznie przesłać jak normalny załącznik.

Dbaj o silne hasła

Aby utworzyć **silne hasło**, zastosuj kilka podstawowych zasad:

1. Hasło powinno składać się z co najmniej 8 znaków,
2. Hasło powinno zawierać kombinację małych i wielkich liter, cyfr oraz znaków specjalnych,
3. Należy unikać używania słów ze słownika,
4. Korzystaj z różnych haseł do komunikatorów, poczty elektronicznej i serwisów społecznościowych. Najlepiej, aby nie miały one nic wspólnego z Twoimi imieniem i nazwiskiem, datą urodzin, itp.,
5. Uaktywnij dwuskładnikowe uwierzytelnianie i stosuj unikalną kombinację haseł, w celu uzyskania dostępu do systemu/urządzenia.