3) Hasła powinny być często zmieniane, na przykład co 30 dni, ADO może, w uzasadnionych sytuacjach polecić dokonanie zmiany hasła przez użytkownika np. po każdym incydencie lub podejrzeniu naruszenia bezpieczeństwa.
4) Należy unikać ponownego lub cyklicznego używania starych haseł.
5) Zabrania się użytkownikom systemu udostępniania swojego identyfikatora i hasła innym osobom oraz korzystania przez osoby upoważnione do przetwarzania danych osobowych z identyfikatora lub hasła innego użytkownika.
6) Pracownicy są odpowiedzialni za zachowanie w poufności swoich haseł.
7) Użytkownik nie powinien przechowywać haseł w widocznych miejscach, nie powinien umieszczać haseł w żadnych automatycznych procesach logowania (skryptach, makrach lub pod klawiszami funkcyjnymi) oraz zapisywać haseł w przeglądarkach internetowych.
8) Użytkownik wprowadza swoje hasło w sposób uniemożliwiający innym osobom jego poznanie.
9) W sytuacji, gdy zachodzi podejrzenie, że hasło mogła poznać osoba nieuprawniona, użytkownik natychmiast dokonuje zmiany hasła.
10) Hasła użytkownika utrzymuje się w tajemnicy również po upływie ich ważności.
11) Administrator Systemu Informatycznego oraz Specjalista ds. odo przeprowadzają okresowe sprawdzanie, usuwanie lub blokowanie zbędnych identyfikatorów użytkowników oraz kont w systemach za które są odpowiedzialni.

5. Hasło administratora systemu informatycznego
   Hasła użytkowników uprzywilejowanych (tzn. użytkowników posiadających uprawnienia na poziomie administratorów systemów informatycznych) są zabezpieczone u Administratora danych na wypadek sytuacji awaryjnych, szczególnie w przypadku nieobecności administratora systemu.
6. Zastosowano urządzenia typu UPS chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania.
20. Zastosowano środki kryptograficznej ochrony danych dla danych osobowych przekazywanych drogą teletransmisji.
21. Dostęp do środków teletransmisji zabezpieczono za pomocą mechanizmów uwierzytelnienia.
22. Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity.
    a. Poniesienie odpowiedzialności wynikających z art. 52 kodeksu pracy,
    b. Poniesienie odpowiedzialności wynikających z art. 363 § 1. kodeksu cywilnego.

C. PRACA ZDALNA.

1. O możliwości podjęcia pracy zdalnej przez pracownika decyduje Administrator.
2. Użytkownik może zgłosić Administratorowi chęć podjęcia pracy zdalnej.
3. Warunki i zasady pracy zdalnej, w tym zakres i harmonogram wykonywanej pracy określa pracodawca.
4. W przypadku podjęcia pracy zdalnej pracownika obowiązują zasady pracy zdalnej określone w niniejszej Polityce.
5. Jeżeli użytkownik nie ma możliwości świadczenia pracy zdalnej z zapewnieniem właściwych zabezpieczeń, w szczególności ze względu na siłę wyższą (np. brak prądu lub Internetu), niezwłocznie zgłasza to Administratorowi i postępuje zgodnie z jego instrukcjami.
6. Złamanie zasad określonych w Polityce lub postanowień i zaleceń Administratora może stanowić naruszenie obowiązków pracowniczych.
7. Użytkownik musi zapewnić właściwe warunki umożliwiające mu skuteczną pracę zdalną z zachowaniem właściwego poziomu bezpieczeństwa informacji.
8. Niedozwolone jest podejmowanie pracy zdalnej w miejscach publicznych, jak kawiarnie, restauracje, galerie handlowe, gdzie osoby postronne mogłyby usłyszeć fragmenty służbowych rozmów lub zapoznać się z fragmentami wykonywanej pracy.