1. Określ jasne i skuteczne zasady polityki poufności i zobowiąż każdego pracownika do ich przestrzegania.
2. Zrób szkolenie dla nowych pracowników . Zapoznaj ich z polityką poufności oraz zasadami przetwarzania danych osobowych. W jasny i prosty sposób przedstaw obowiązki każdemu, kto będzie miał dostęp do danych osobowych.
3. Rób szkolenia przypominające o tych zasadach.
4. Poinformuj osoby, których dane przetwarzasz, o tym po co gromadzisz dane i co z nimi robisz. Opracuj przejrzyste informacje w tym zakresie zgodnie z wymogami prawnymi.
5. Poinformuj zainteresowanych do czego wykorzystywane będą ich dane.
6. Informacje o osobach przechowuj tylko przez taki czas, przez jaki jest to niezbędne.
7. Odpowiedzialność za zgodne z prawem przetwarzanie danych osobowych oraz bezpieczeństwo danych spoczywa na administratorze, czyli organizacji takiej jak np. uczelnia. Administrator odpowiada również za przetwarzanie, które powierza innemu podmiotowi. Powinien zwracać szczególną uwagę kogo upoważnia do dostępu do danych i co się dzieje z danymi na każdym etapie ich przetwarzania.
8. Nadzoruj i monitoruj procedury związane z bezpiecznym przetwarzaniem danych osobowych.
9. Zadbaj o bezpieczeństwo biura – zabezpiecz dokumenty, ogranicz do nich dostęp.
   Kieruj się zasadą czystego biurka – nie pozostawiaj zapisanych haseł, dokumentów, danych na biurku.
10. Zobowiąż pracowników do niepozostawiania dokumentów z danymi osobowymi bez nadzoru oraz ich nieudostępniania osobom do tego nieupoważnionym, bądź nieuprawnionym.
11. Nie ujawniaj danych osobowych poza organizacją, w której pracujesz. Uważaj gdzie i z kim o nich rozmawiasz. Unikaj takich rozmów w miejscach publicznych, podczas spotkań towarzyskich oraz przez telefon.
12. Gdy pracujesz nad dokumentami zawierającymi dane osobowe unikaj miejsc publicznych, np. komunikacji miejskiej, galerii handlowych, dworców itp.
13. Zadbaj o przeszkolenie pracowników pracujących zdalnie w zakresie szyfrowania wiadomości e-mail, nie pozostawiania komputera i nośników danych bez kontroli.
14. Używaj silnych haseł zabezpieczających komputer i nośniki danych, tak aby chronić informacje na nich zawarte przed dostaniem się w niepowołane ręce.
15. Zaszyfruj wszystkie urządzenia przenośne – laptopy, pendrive’y, dyski zewnętrzne.
16. Systematycznie czyść pliki cookies, zapamiętane hasła oraz nazwy użytkowników.
17. Nie proś o dane, których nie potrzebujesz.
18. Dokumenty, które nie są już potrzebne, a zawierają dane osobowe, zniszcz przed wyrzuceniem, w sposób uniemożliwiający ich odtworzenie.