ZAŁĄCZNIK
Do Uchwały Zarządu
Spółdzielni Mieszkaniowej „Aster-Bud" w Warszawie
Nr 1 z dnia 11 września 2024 roku

Procedura ochrony informacji i danych w Spółdzielni Mieszkaniowej „Aster-Bud" w Warszawie

1. Niniejsza Procedura określa zasady bezpieczeństwa informacji i danych w Spółdzielni Mieszkaniowej „Aster-Bud" w Warszawie.
2. Ilekroć w niniejszej Procedurze jest mowa o „informacjach i danych" należy przez to rozumieć wszelkie informacje i dane, w tym dane osobowe utrwalone lub wyrażone w formie pisemnej, dokumentowej lub elektronicznej, dotyczące spraw Spółdzielni Mieszkaniowej „Aster-Bud" a w szczególności: (i) informacje finansowe, organizacyjne, ekonomiczne, prawne, know-how (ii) dotyczące danych kontrahentów Spółdzielni lub członków Spółdzielni; (iii) dotyczące zawarcia, treści oraz wykonania umów zawartych pomiędzy Spółdzielnią i innymi podmiotami w tym dostawcami, współpracownikami i pracownikami Spółdzielni; wszelkie kody, hasła, loginy i podobne dane umożliwiające w szczególności dostęp do systemów informatycznych, poczty elektronicznej, baz danych i stron internetowych Spółdzielni.
3. Pracownicy mogą przetwarzać informacje i dane tylko w celach związanych z wykonywaniem swoich obowiązków służbowych.
4. Pracownik zobowiązany jest dbać o bezpieczeństwo informacji i danych, ich poufność oraz integralność.
5. Pracownik zobowiązany jest natychmiastowo powiadomić Zarząd Spółdzielni o jakimkolwiek incydencie związanym z wyciekiem informacji lub danych, jak również o kradzieży lub zaginięciu powierzonego mu sprzętu.

Praca z danymi w obiegu elektronicznym

6. Instalowanie jakiegokolwiek oprogramowania na komputerach służbowych jest możliwe tylko za zgodą i zgodnie z wytycznymi Zarządu Spółdzielni.
7. Na komputerze służbowym, telefonie służbowym ani na żadnym innym służbowym urządzeniu elektronicznym, nie może być instalowane żadne nielegalne oprogramowanie.
8. Pracownik odpowiada za zabezpieczenie sprzętu służbowego przed dostępem osób trzecich.
9. Pracownik nie może przechowywać żadnych danych ani informacji na innych nośnikach niż udostępnione mu przez Pracodawcę.
10. Zabronione jest używanie prywatnych kont pocztowych oraz prywatnych kont w usługach chmurowych do przetwarzania informacji i danych.
11. Zabronione jest korzystanie ze służbowej poczty elektronicznej przy użyciu prywatnych urządzeń.
12. Pracownik odpowiada za należytą ochronę danych dostępnych na elektronicznych urządzeniach wykorzystywanych do przetwarzania danych służbowych.
13. Hasła do systemów informatycznych nie powinny być zapisywane przez przeglądarkę internetową.
14. Przy wysyłaniu wiadomości e-mail Pracownik zobowiązany jest każdorazowo upewnić się co do poprawności wpisanych adresów mailowych jej adresatów.
15. Pracownik nie może przesyłać treści podejrzanych, naruszających prawa własności intelektualnej, zabronionych prawnie.
16. W przypadku wiadomości zawierających informacje poufne lub o charakterze tajemnicy przedsiębiorstwa konieczne jest szyfrowanie wiadomości.

17. W przypadku identyfikacji wirusa lub nieaktualności oprogramowania antywirusowego konieczne jest natychmiastowe skontaktowanie się z Zarządem Spółdzielni.

Praca z dokumentami papierowymi

18. Wynoszenie dokumentacji papierowej z biura Pracodawcy powinno być ograniczone do niezbędnego minimum i wymaga zgody Pracodawcy w formie dokumentowej.
19. W przypadku konieczności korzystania z dokumentacji papierowej poza biurem Pracodawcy w pierwszej kolejności należy rozważyć wykonanie kopii dokumentacji, na której Pracownik będzie pracował.
20. Drukowanie dokumentów na potrzeby pracy należy ograniczyć do niezbędnego minimum. W przypadku dokumentów zawierających dane osobowe należy w miarę możliwości dokonać anonimizacji danych.
21. Wynoszenie dokumentów lub ich kopii powinno mieć miejsce w zabezpieczonej aktówce i w taki sposób, aby były niewidocznie dla osób trzecich.
22. Pracownik zobowiązany jest do odpowiedniego zabezpieczenia danych w miejscu wykonywania pracy zdalnej - dokumenty i ich kopie powinny być przechowywane w zamykanych na klucz szufladach biurka lub szafach, należy zabezpieczyć dostęp do nich osób nieuprawnionych.
23. Po wykorzystaniu oryginałów dokumentów powinny one zostać niezwłocznie zwrócone do biura Pracodawcy.
24. Po wykorzystaniu kopii dokumentacji powinny one zostać w całości zniszczone przez Pracownika.
25. Po zakończeniu dnia pracy Pracownik powinien bezwzględnie przestrzegać zasady czystego biurka.