

„ZATWIERDZAM”

REKTOR
Zachodniopomorskiego Uniwersytetu
Technologicznego w Szczecinie

dr hab. inż. Jacek Wróbel, prof. ZUT



Zatwierdzam i wprowadzam do użytku służbowego:

Wytyczne

w zakresie niszczenia nośników danych osobowych w
Zachodniopomorskim Uniwersytecie Technologicznym
w Szczecinie

Inspektor Ochrony Danych

INSPEKTOR OCHRONY DANYCH
Zachodniopomorskim Uniwersytecie Technologicznym
w Szczecinie

mgr Artur Kurek

Szczecin - 2020 r.

1. Wytyczne określają zalecenie IOD w zakresie sposobu i trybu niszczenia nośnika danych osobowych w jednostkach organizacyjnych ZUT.
2. Ilekroć w wytycznych jest mowa o:
nośniku danych osobowych - należy przez to rozumieć materiał lub urządzenie służące do zapisywania, przechowywania i odczytywania danych w postaci cyfrowej lub tradycyjnej.
3. Niszczeniu poddaje się nośnik danych, w przypadku stwierdzenia:
 - 1) wady lub uszkodzenia nośnika danych osobowych wynikającego z eksploatacji, których naprawa byłaby nieopłacalna,
 - 2) braku przydatności do dalszego użytkowania nośnika danych osobowych ze względu na zły stan techniczny,
 - 3) technicznej dezaktualizacji lub braku możliwości zastosowania nośnika danych osobowych,
 - 4) braku możliwości dalszego wykorzystania nośnika danych osobowych z uwagi na konieczność zapewnienia ochrony informacji.
4. Kwalifikacji do zniszczenia oraz czynności zniszczenia nośnika danych dokonuje komisja powoływana przez kierownika jednostki organizacyjnej ZUT.
5. Proces kwalifikacji nośnika danych osobowych do zniszczenia komisja dokumentuje w protokole oceny technicznej.
6. Zniszczenie nośnika danych osobowych w postaci dysku twardego, dysku SSD lub pamięci półprzewodnikowej pendrive komisja dokonuje zgodnie z wytycznymi Dyrektora UCI .
7. Niszczenia nośnika danych osobowych komisja dokonuje przy użyciu właściwych urządzeń, w sposób uniemożliwiający odzyskanie lub odczytanie danych z nośnika danych.
8. Niszczenie nośnika danych osobowych polega na jego zniszczeniu fizycznym.
9. W zależności od rodzaju materiału, z jakiego został wykonany nośnik danych, jego zniszczenie fizyczne polega na:
 - 1) ścięciu lub,
 - 2) spaleniu lub,
 - 3) zmiżdżeniu.
10. Ścięcie nośnika danych osobowych, komisja dokonuje przy użyciu niszczarki, która powinna ścinać nośnik danych osobowych lub jego elementy na ścinki o maksymalnej szerokości 5 mm.
11. Spalenie nośnika danych, polega na całkowitym spopieleniu nośnika przez komisję.
12. Zmiżdżenia nośnika danych osobowych, komisja dokonuje poprzez jego zniekształcenie w sposób uniemożliwiający odzyskanie lub odczytanie danych.
13. Zniszczenie nośnika danych osobowych w postaci magnetoptycznego dysku twardego poprzedza jego rozmagnesowanie przy użyciu demagnetyzera.

14. Zniszczenie nośnika danych osobowych w postaci dysku twardego, dysku SSD lub pamięci półprzewodnikowej pendrive odbywa się przy użyciu właściwych urządzeń.
15. Z komisijnego zniszczenia nośnika danych komisja sporządza, w egzemplarzu pojedynczym, protokół zniszczenia.
16. Protokół zniszczenia, w szczególności powinien zawierać:
 - 1) sygnaturę literowo-cyfrową, pod którą zarejestrowano nośnik danych w ewidencji,
 - 2) producenta nośnika danych,
 - 3) model,
 - 4) pojemność,
 - 5) numer seryjny.
17. Protokół zniszczenia jest podstawą do dokonania zmian w ewidencji, w której zarejestrowany był nośnik danych.
18. Utylizacja odpadów powstałych w wyniku zniszczenia cyfrowego nośnika danych jest dokonywana zgodnie z procedurą opracowaną przez Dyrektora UCI.