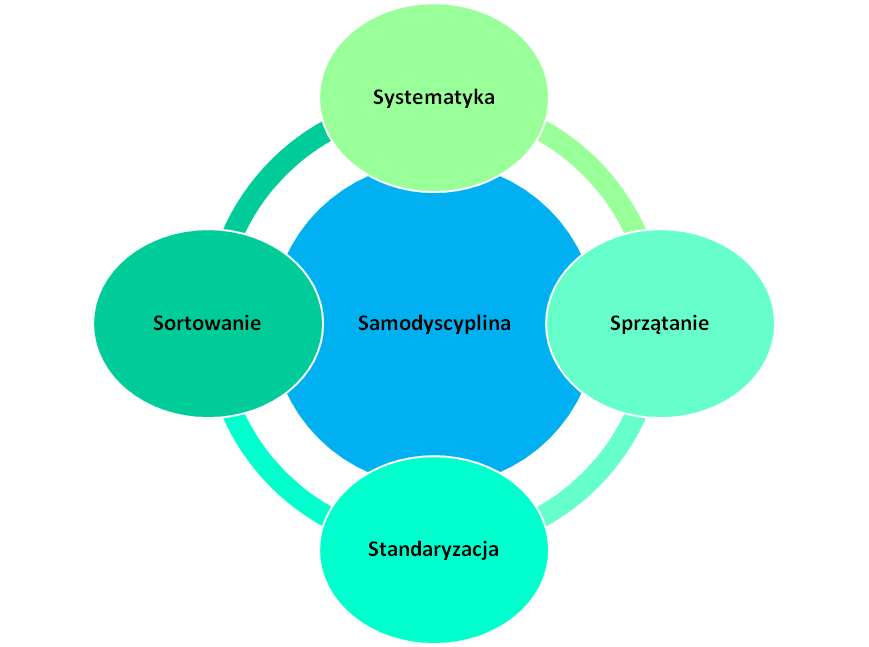
**POLITYKA CZYSTEGO BIURKA I EKRANU (CBE)**



**Zasady 5-S:**

Model postępowania zgodnie z Polityką CBE wyznacza hasłowo **5 zasad „S”**, odnoszonych do bezpieczeństwa informacji i ochrony danych:

1. **Sortowanie**

Wyeliminowanie ze środowiska pracy zbędnych elementów, takich jak dokumenty, materiały, notatki i nośniki danych, które nie są konieczne do wykonywania bieżących zadań.

Pozostawia się tylko dane przydatne, tylko w niezbędnej ilości, i tylko na czas, w którym istnieje potrzeba ich wykorzystania. Dane zbędne niszczy się w należyty sposób, natomiast dane, które na dany moment nie są przydatne, zabezpiecza się i umieszcza w miejscu ich przechowywania.

1. **Systematyka**

Organizacja elementów środowiska pracy oraz ich oznaczenie w sposób umożliwiający łatwość ich identyfikacji, odnalezienia, użycia i odłożenia na miejsce, czytelne także dla innych osób mających uprawniony interes w dostępie do nich. Umożliwienie wizualnej kontroli danych, ich statusu, sposobu wykorzystania oraz stanu prowadzonych z ich użyciem prac.

1. **Sprzątanie**

Stałe i rutynowe porządkowanie środowiska pracy, umożliwiające bieżące identyfikowanie źródeł potencjalnych problemów i anomalii.

1. **Standaryzacja**

Wypracowanie ustalonych sposobów i modeli wykonywania czynności w zakresie pozostałych kroków, utrwalanie dobrych praktyk.

Wkomponowanie dbałości o jednolitość czynności przetwarzanych danych, sposobów ich wykorzystywania i zabezpieczenia w rutynę bieżących czynności operacyjnych.

1. **Samodyscyplina**

Wyrobienie potrzeby wewnętrznej dbałości o bezpieczeństwo informacji, a także utrzymanie nawyków i przyzwyczajeń ułatwiających pracę zgodnie z przyjętymi standardami.

Osiągnięcie efektu w postaci utrzymywania „czystego biurka” oraz utrzymywania wypracowanego efektywnego systemu pracy z danymi i dokumentami zgodnie z wymogami ochrony danych i dobrymi praktykami w tym zakresie.

**POLITYKA CZYSTEGO BIURKA I EKRANU (CBE)**

Na koniec dnia pracy, a także na czas nieobecności, wszystkie dokumenty w formie papierowej zabezpiecza się poprzez umieszczenie w przeznaczonych na nie miejscach (teczki, segregatory, szuflady, szafki, organizatory).

Unika się pozostawiania dokumentów widocznych na stanowisku pracy. Informacje o charakterze wrażliwym i poufnym przechowuje się w zamknięciu.

1. **Ekrany**

Monitory ekranowe na czas nieobecności użytkownika przy stanowisku zabezpiecza się blokadą.

1. **Stanowiska komputerowe**

Unika się pozostawiania stacji roboczych i systemów w trybach oszczędzania energii, wstrzymania, uśpienia itp. na koniec dnia pracy. Preferowanym sposobem zakończenia pracy jest ich pełne zamknięcie. Laptopy i inne urządzenia przenośne fizycznie zabezpiecza się przed niepowołanym dostępem.

1. **Środki dostępu**

Fizycznych i logicznych środków dostępu (hasła komputerowe, klucze, karty elektroniczne) nie przechowuje się w miejscach publicznie dostępnych, jak blaty biurek czy zasobniki na przybory biurowe i nie pozostawia bez nadzoru.

Haseł nie przechowuje się w systemach teleinformatycznych w formie niezabezpieczonej kryptograficznie. Nie udostępnia się ich innym osobom i nie zapisuje w formie papierowej w sposób dostępny dla osób trzecich – w szczególności nie zapisuje się ich na kartach post-it i nie umieszcza na elementach stacji roboczych.

1. **Drukowanie**

Wydruki podejmuje się z drukarek bezpośrednio po ich wydrukowaniu. Wydruków nie pozostawia się na drukarce.

1. **Nośniki danych**

Elektroniczne nośniki danych, jak pamięci SD, nośniki optyczne, urządzenia typu pendrive itp., traktuje się jako wrażliwe i przechowuje w zamknięciu.

1. **Niszczenie**

Przedarcie i wyrzucenie wydruku do kosza na odpadki nie stanowi bezpiecznego niszczenia dokumentu. Preferowaną metodą usuwania dokumentacji papierowej jest niszczarka bądź umieszczenie w bezpiecznym pojemniku na dokumentację do zniszczenia.