

Rola i zadania koordynatora bezpieczeństwa w sieci w Centrum Kształcenia Ustawicznego w Kutnie

Koordynator bezpieczeństwa w sieci odpowiada za techniczne i organizacyjne przygotowanie Placówki do zapewnienia bezpiecznych warunków korzystania przez słuchaczy z sieci teleinformatycznych, w tym Internetu, na terenie Centrum Kształcenia Ustawicznego.

Koordynator bezpieczeństwa w sieci:

1. posiada odpowiednie kompetencje techniczne i potrafi wprowadzić zabezpieczenia informatyczne chroniące przed nielegalnymi i szkodliwymi treściami;
2. zna zagrożenia technologiczne i społeczne oraz wie, jak małoletni wykorzystują Internet i technologie;
3. potrafi wprowadzić rozwiązania, które zablokują nielegalne i szkodliwe treści;
4. doskonali się zawodowo samodzielnie lub uczestniczy w różnych zewnętrznych formach doskonalenia zawodowego w obszarze reagowania na incydenty, na przykład na przemoc z użyciem technologii;
5. potrafi wykorzystywać rozwiązania online w edukacji;
6. zna zasady prostej i efektywnej komunikacji – potrafi dostosować język i formę informacji do potrzeb odbiorcy.

Zadania koordynatora bezpieczeństwa w sieci

1. opracowuje regulamin pracowni komputerowych, zasady korzystania z urządzeń placówki, internetu/sieci wifi i zapoznaje słuchaczy oraz pracowników;
2. blokuje tylko treści niebezpieczne dla małoletnich; edukuje słuchaczy w zakresie bezpiecznego korzystania z internetu – zna zasady bezpiecznego korzystania z internetu i je propaguje, opracowuje i udostępnia słuchaczom i ich rodzicom/opiekunom prawnym informacje dotyczące zagrożeń internetowych i metod ich eliminacji;
3. na bieżąco informuje wszystkie osoby korzystające z internetu w placówce o zmianach w zasadach bezpieczeństwa i wytycznych; zakres tych zasad i sposób ich przedstawienia musi być dostosowany do wieku i potrzeb słuchaczy i innych użytkowników – dotyczy też różnych urządzeń, np. laptopów, tabletów, drukarek,

skanerów, kamer internetowych, monitorów) i sposobów ich wykorzystywania, w tym w ramach ewentualnej nauki zdalnej;

4. stosuje programy antywirusowe, tryby bezpiecznego wyszukiwania, monitoruje aktywność użytkowników;
5. zabezpiecza sieć silnymi hasłami;
6. regularnie aktualizuje oprogramowanie routera – jeśli to możliwe, przy pomocy automatycznej aktualizacji;
7. sprawdza systematycznie (np. co miesiąc), czy na urządzeniach placówki nie znajdują się nielegalne, szkodliwe i nieodpowiednie dla treści dla słuchaczy;
8. monitoruje korzystanie przez słuchaczy z urządzeń należących do placówki, które są podłączone do internetu wyłącznie przez sieć Centrum, nie dopuszcza do sytuacji, aby słuchacze podłączyli urządzenia do innych sieci, na przykład publicznych sieci wifi albo osobistych hotspotów;
9. informuje słuchaczy o bezpiecznych zasadach korzystania przez słuchaczy z prywatnego internetu na prywatnych urządzeniach w Placówce, promuje dobre praktyki i bezpieczne zachowania;
10. monitoruje dostęp do internetu dla pracowników Placówki (każdy użytkownik ma własne konto i hasło użytkownika potrzebne do wykonywania zadań, słuchacze nie mają do nich dostępu);
11. sprawdza urządzenia należące do Placówki i zabezpiecza je przed kradzieżą, zniszczeniem, sprawdza aktualne oznakowanie urządzeń, aktualizuje systemy operacyjne.