UNIWERSYTET MEDYCZNY
IM. PIASTÓW ŚLĄSKICH WE WROCŁAWIU

INSPEKTORAT SPRAW OBRONNYCH I OCHRONY INFORMACJI NIEJAWNYCH

Pełnomocnik ds. Ochrony Informacji Niejawnych Administrator Bezpieczeństwa Informacji

RC/ODO -140-7/04/16

Szanowni Państwo.

W obecnym okresie, w którym ranga informacji nabrała szczególnego znaczenia, nasilają się działania zmierzające do pozyskiwania jej, często w dyskusyjnych celach.
Stąd szczególnego znaczenia nabierają działania chroniące te informacje, których nieuprawnione pozyskanie i wykorzystanie mogą mieć istotny wpływ także na szeroko rozumiane interesy Uczelni.
W związku z powyższym przypominam Państwu o konieczności przestrzegania podstawowych zasad bezpieczeństwa informacji, które stanowią załącznik do pisma J.M. Rektora nr RC/ODO-014-2/05/10 z dnia 18.05.2010 r.
Informuję jednocześnie, że wspomniane zasady bezpieczeństwa informacji znajdują się na stronie Inspektoratu Spraw Obronnych i Ochrony Informacji Niejawnych UM we Wrocławiu.

Z wyrazami szacunku

Pełnomocnik ds. Ochrony Informacji Niejawnych
Administrator Bezpieczeństwa Informacji

Szanowni Państwo.

Przypominam wszystkim pracownikom Uczelni o konieczności konsekwentnego przestrzegania następujących, podstawowych zasad bezpieczeństwa informacji pozyskiwanych w procesie realizacji obowiązków służbowych:

1. **Zasada indywidualnych kont w systemie.**

   Każdy pracownik zobowiązany jest do pracy w systemach teleinformatycznych na przypisanych jemu kontach. Zabronione jest udostępnianie kont osobom trzecim.

2. **Zasada poufności haseł i kodów dostępu.**

   Każdy pracownik zobowiązany jest do zachowania poufności i nie przekazywania osobom nieuprawnionym udostępnionych jemu haseł. Zasada ta w szczególności dotyczy osobistych haseł dostępu pracownika do systemów teleinformatycznych i stref chronionych.

3. **Zasada zamkniętego pomieszczenia.**

   Niedopuszczalne jest pozostawianie niezabezpieczonego pomieszczenia służbowego, zarówno w godzinach pracy, jak i po jej zakończeniu, jeśli nie pozostaje w nim osoba uprawniona. Zasada nie dotyczy pomieszczeń ogólnie dostępnych. Po zakończeniu dnia pracy, ostatnia wychodząca z pomieszczenia osoba jest zobowiązana zamknąć wszystkie okna i drzwi oraz zgodnie z obowiązującymi ustaleniami, zabezpieczyć klucze do pomieszczenia.

4. **Zasada nadzorowania dokumentów.**

   Po godzinach pracy wszystkie dokumenty zawierające informacje istotne z punktu widzenia interesów Spółki powinny być przechowywane w zamkniętych szafach lub szufladach, zabezpieczonych przed dostępem do osób nieuprawnionych.

5. **Zasada czystego biurka.**

   Należy unikać pozostawionych bez nadzoru dokumentów na biurku. Po zakończeniu pracy należy uprzątnąć biurko z dokumentów papierowych oraz innych nośników informacji (płyt CD, DVD, itp.).

6. **Zasada czystej tablicy.**

   Po zakończeniu zajęć, spotkań, dyskusji itp. należy uprzątnąć wszystkie materiały oraz oczyścić tablice.

7. **Zasada czystego ekranu.**

Każdy komputer musi mieć ustawiony wygaszasz ekranu po podaniu hasła lub wyłączający się automatycznie po określonym czasie bezczynności użytkownika. Dodatkowo przed pozostawieniem włączonego komputera bez opieki użytkownicy powinni zablokować go (włączając wygaszasz ekranu) lub w przypadku dłuższej nieobecności wylogować się z systemu.

8. **Zasada czystego pulpitu.**

Na pulpicie komputera mogą znajdować się jedynie ikony standardowego oprogramowania i aplikacji służbowych oraz skróty folderów pod warunkiem, że w nazwie nie zawierają informacji o realizowanych projektach lub klientach.

9. **Zasada czystych drukarek.**

Informacje drukowane powinny być zabierane z drukarek niezwłocznie po wydrukowaniu. W przypadku nieudanej próby drukowania, użytkownik powinien skontaktować się z serwisantem odpowiedzialnym za poprawne funkcjonowanie urządzenia. Samodzielnie lub według instrukcji serwisanta usunąć informację z pamięci drukarki.

10. **Zasada czystego kosza.**

Dokumenty papierowe z wyjątkiem materiałów promocyjnych, marketingowych i informacyjnych powinny być niszczone w sposób uniemożliwiający ich odczytanie, (najlepiej w niszczarce), umieszczane w specjalnie przeznaczonych do tego pojemnikach itp.

11. **Zasada odpowiedzialności za zasoby.**

Każdy użytkownik odpowiada za udostępnione jemu zasoby (komputery, oprogramowanie, systemy, konta itp.) Zasoby te przeznaczone są do realizacji celów służbowych. Wykorzystanie ich do celów prywatnych możliwe jest jedynie w ograniczonym wewnętrznymi przepisami zakresie. Nieuprawnione instalowanie nielegalnego oprogramowania jest bezwzględnie zabronione.