UNIWERSYTECKI
SZPITAL KLINICZNY
W OPOLU

# Cyberbezpieczeństwo (http://www.usk.opole.pl/szpital/cyberbezpieczenstwo)

Uniwersytecki Szpital Kliniczny w Opolu, jako operator usługi kluczowej, zgodnie z Ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U z 2018 r, poz. 1560) wdrożył i eksploatuje system zarządzania bezpieczeństwem informacji zgodnie z międzynarodowym standardem ISO/IEC 27001.

Szpital analizuje ryzyka z zakresu bezpieczeństwa informacji, ochrony danych osobowych i cyberbezpieczeństwa.

Dla lokalizacji szpitala ustalono zasady ochrony pomieszczeń istotnych z punktu widzenia bezpieczeństwa procesu świadczenia usługi kluczowej. Ochronę fizyczną zapewniają w szczególności systemy kontroli dostępu (zamki mechaniczne i elektroniczne), system monitoringu wizyjnego, identyfikację pracowników oraz system przeciwpożarowy.

Ze względu na krytyczność systemów informacyjnych, urządzeń i narzędzi wspomagających proces utrzymania pacjenta przy życiu, Szpital został wyposażony w redundantne zabezpieczenia na wypadek zakłóceń lub utraty zasilania.

Szpital wdrożył system zarządzania bezpieczeństwem informacji i restrykcyjnie egzekwuje stosowanie wewnętrznych procedur i instrukcji. Każdy pracownik jest świadomy zapisów procedur systemowych oraz swoich obowiązków w tym zakresie. W odniesieniu do zagrożeń wynikających z braku przestrzegania zapisów w zakresie bezpiecznego przetwarzania informacji Szpital podejmuje działania uświadamiające zagrożenia, informując pracowników o wszelakich próbach ataków środowisk przestępczych na zasoby informacyjne Szpitala.

Szpital korzysta z usług zaufanych dostawców Internetu celem zmniejszenia prawdopodobieństwa błędów po stronie dostawcy, które mogłyby wpłynąć na ciągłość usług szpitala, utratę komunikacji lub bezpieczeństwa przesyłanych informacji.

---