DOKUMENT WEWNĘTRZNY

Wykaz zabezpieczeń stosowanych w Akademii Łomżyńskiej

1. Zabezpieczenia organizacyjne:
    a. Upoważnienia wystawiane pracownikom i współpracownikom: Dostęp do systemów informatycznych udzielany jest użytkownikom na podstawie wystawionych upoważnień na wniosek przełożonego lub Działu Spraw Osobowych
    b. Szkolenia pracowników w zakresie bezpieczeństwa IT.
2. Zabezpieczania fizyczne
    a. Ograniczony dostęp do pomieszczeń biurowych: pomieszczenia zamykane na klucz, stosowanie systemu kontroli dostępu,
    b. Ograniczanie dostępu do pomieszczeń serwerowni: dostęp ograniczony do pracowników Działu Systemów Komputerowych, stosowanie systemu kontroli dostępu.
3. Zabezpieczenia techniczne:
    a. Systemy chłodzenia w serwerowni: pomieszczenia serwerowni są stale klimatyzowane wraz z monitorowaniem temperatury,
    b. Systemy zasilania awaryjnego UPS: urządzenia serwerowe oraz urządzenia sieciowe głównych punktów dystrybucyjnych i serwerowni zasilane są z urządzeń podtrzymujących zasilanie.
4. Zabezpieczenia informatyczne:
    a. Indywidualne konta użytkowników: Każdy użytkownik posiada indywidualne konto do systemu i aplikacji,
    b. Ochrona antywirusowa: Komputery użytkowane w obszarze przetwarzania danych posiadają zainstalowane i aktualizowane oprogramowanie antywirusowe,
    c. Filtrowanie ruchu sieciowego na styku sieci lokalnej i Internetu: Wymiana danych między siecią lokalną Uczelni oraz Internetem kontrolowana jest z użyciem urządzenia UTM,
    d. Segmentowanie sieci: separowanie obszarów sieci lokalnej przez zastosowanie wirtualnych sieci LAN w celu ograniczenia dostępu do zasobów administracji z sieci dydaktycznej,
    e. Szyfrowanie transmisji danych: Stosowanie protokołów szyfrujących transmisję w sieciach publicznych (np. stosowanie protokołów https, ssh itp),
    f. Praca zdalna za pomocą VPN i RDP: Praca zdalna zabezpieczana jest technologią VPN (Virtual Private Network), aplikacje uruchamiane są na komputerach zainstalowanych w obszarze przetwarzania danych z wykorzystaniem usługi pulpitu zdalnego RDP,
    g. Stosowanie nadmiarowych urządzeń: stosowanie serwerów wyposażonych w 2 niezależne zasilacze oraz systemy pamięci masowych RAID, stosowanie serwerów zwirtualizowanych oraz połączonych w klaster, stosowanie w głównych węzłach sieci urządzeń transmisji danych połączonych w klaster wysokiej dostępności HA

h. Kopie bezpieczeństwa: Stosowanie systemów wykonywania kopii zapasowych systemów serwerowych oraz stacji roboczych w najistotniejszych jednostkach organizacyjnych.