ALTEM • Bezpieczeństwo • Technologie • Edukacja

Checklista audytu IT szkoły

Krótka lista kontrolna dla dyrekcji i administratora przed rozpoczęciem audytu lub modernizacji.

1. Konta i tożsamość

- ☐ Czy istnieje aktualna lista kont nauczycieli, pracowników i uczniów?
- ☐ Czy konta byłych pracowników i absolwentów są regularnie wyłączane?
- ☐ Czy konta administracyjne są oddzielone od codziennych kont użytkowników?
- ☐ Czy dla administratorów i osób z dostępem do danych stosowane jest MFA/2FA?

2. Sieć i Wi-Fi

- ☐ Czy znana jest aktualna topologia sieci i lista urządzeń aktywnych?
- ☐ Czy sieć administracyjna, nauczycielska, uczniowska i gościnna są logicznie odseparowane?
- ☐ Czy punkty dostępowe, przełączniki i urządzenia brzegowe mają aktualne oprogramowanie?
- ☐ Czy dostęp do paneli zarządzania jest ograniczony i chroniony silnym uwierzytelnianiem?

3. Komputery i urządzenia

- ☐ Czy szkoła ma aktualną inwentaryzację sprzętu wraz z odpowiedzialnością za urządzenia?
- ☐ Czy systemy i przeglądarki otrzymują aktualizacje bezpieczeństwa?
- ☐ Czy oprogramowanie antywirusowe/EDR i szyfrowanie są stosowane adekwatnie do ryzyka?
- ☐ Czy sprzęt pozyskany w ramach programów KPO/UE jest ujęty oddzielnie od sprzętu wymagającego stałej obsługi?

4. Kopie zapasowe i odtwarzanie

- ☐ Czy wykonywane są kopie danych krytycznych i konfiguracji?
- ☐ Czy co najmniej jedna kopia jest odseparowana od systemu produkcyjnego?

- ☐ Czy odtwarzanie było testowane w praktyce, a nie tylko deklarowane?

5. Poczta i domeny

- ☐ Czy domena ma poprawne SPF, DKIM i DMARC?
- ☐ Czy poczta jest chroniona przed phishingiem i podszywaniem się pod szkołę?
- ☐ Czy istnieje procedura zgłoszenia podejrzanej wiadomości lub przejęcia konta?

Ta checklista nie zastępuje formalnego audytu bezpieczeństwa. Służy do zebrania informacji i ustalenia priorytetów przed dalszymi działaniami.