CHECKLIST – Emergency modul (on-prem Bakaláři)

Určeno pro ICT správce školy. Platí pro školy provozující systém Bakaláři na vlastním serveru (IIS).
Zaškrtněte po ověření.

1) **Server a operační systém**
   ☐ Server běží na podporovaném OS dle technických podmínek Bakalářů (nápověda → Správa systému → Podporované operační systémy).
   ☐ Server je pravidelně aktualizovaný (bezpečnostní aktualizace OS).
   ☐ Server má dostatečnou kapacitu pro stabilní provoz (CPU/RAM/disk).

2) **IIS a aplikační komponenty**
   ☐ Webová aplikace Bakaláři je v IIS publikovaná a běží bez chyb – jsou nainstalované požadované runtime komponenty (.NET / .NET Framework) dle verze Bakalářů.

3) **HTTPS, TLS a certifikát**
   ☐ Je nasazen platný certifikát odpovídající veřejnému názvu (FQDN).
   ☐ Server podporuje minimální podporovanou verzi TLS dle aktuálních technických podmínek (min. TLS 1.2).

4) **DNS a veřejná dostupnost**
   ☐ Je nastavené veřejné FQDN (doménové jméno) a správný DNS záznam (A/AAAA).
   ☐ Pokud je server za NAT nebo je publikován přes reverzní proxy / load balancer, je nastaveno směrování služby pro TCP/443 (HTTPS) na webový server Bakalářů (IIS).

5) **Firewall – odchozí komunikace (OUTBOUND)**
   ☐ Ze serveru Bakalářů s webovou aplikací je povolena **odchozí** komunikace (HTTPS) pro potřeby služby.

6) **Firewall – příchozí komunikace (INBOUND)**
   ☐ Na firewallu je povolen příchozí provoz z internetu na server – centrální služby Emergency modulu na Azure od Microsoft.

7) **Funkčnost modulu Emergency**
   ☐ Modul Emergency je v systému aktivní.
   ☐ Uživatelé mají aktuální funkční mobilní aplikaci Bakaláři a povolené notifikace.
   ☐ Proběhl test: vyhlášení události (admin/krizový tým) + doručení notifikací + potvrzení bezpečí.

Rychlá diagnostika při potížích (když něco nefunguje)

☐ Ověřeno, že certifikát má kompletní řetězec a odpovídá doméně (bez varování v prohlížeči).
☐ Ověřeno, že firewall / WAF / IDS/IPS neblokuje HTTPS provoz aplikace.