STANDAR KEAMANAN APLIKASI DAN HOSTING BNN

A. Standar Aplikasi

1. Dapat berjalan pada protokol HTTPS dan Minimal TLS 1.2.
2. Aplikasi sudah mengimplementasikan CSP (Content Security Policy) Level 2 sesuai rekomendasi W3C.
3. Aplikasi dapat berjalan sesuai ketentuan (rule) yang diterapkan oleh ModSecurity dan WAF.
4. Mode akses file aplikasi tidak boleh 777 (Full Akses Nobody).
5. Aplikasi tidak dideploy di root server melainkan di home user.
6. File System/framework tidak diperbolehkan didevelopment di public_html (atau terakses di public).
7. User aplikasi tidak boleh menggunakan root/sysadmin akses.
8. User database tidak boleh menggunakan root/setara.
9. Tidak mengaktifikan default user.
10. Membuat kombinasi password min 8 karakter, terdiri dari huruf, angka dan karakter serta tidak boleh sama dgn nama user.

B. Standar Hosting & Pengamanan Aplikasi

1. Aplikasi dapat di hosting melalui layanan hosting BNN, sesuai dengan akses yg akan diberikan.
2. Aplikasi dapat berjalan dengan standar CSP, WAF, dan Mod Security yang ada di Puslitdatin.
3. Aplikasi dapat berjalan pada protokol HTTPS dan jika menggunakan komunikasi IT disarankan menggunakan TLS 1.3.
4. Sebelum dilakukan development, agar dilakukan pemisahan antara file system/framework dengan file aplikasi.
5. Aplikasi bebas dari malware (backdoor, spyware, virus, dll).
6. Menginformasikan thirdparty dan plugin yang digunakan di aplikasi.
7. Menginformasikan arsitektur (koneksi dan integrasi).
8. Menggunakan Framework dan menginformasikan engine (bahasa pemprograman, database, dll) aplikasi.
9. Aplikasi harus menggunakan bahasa pemrograman, database, framework dengan security patch terbaru.
10. Menutup port yang tidak digunakan.
11. Menerapkan standar backup dan pemeliharaan berkala.