Checklist Kesiapan Menggunakan Gen-AI dengan Aman

Gunakan checklist ini untuk pemeriksaan awal Gen-AI dalam cybersecurity di perusahaan Anda.

- [ ] **1. Tujuan penggunaan Gen-AI sudah ditentukan**
  Tugas apa saja yang boleh dibantu AI, dan oleh tim mana

- [ ] **2. Data yang boleh diproses sudah diklasifikasikan**
  Pisahkan data publik, internal, rahasia, dan data pribadi

- [ ] **3. Platform AI telah diperiksa dan disetujui**
  Hanya akun dan layanan resmi perusahaan yang dipakai

- [ ] **4. Hak akses telah dibatasi**
  AI dan pengguna hanya mengakses data serta sistem yang diperlukan

- [ ] **5. Aktivitas pengguna dicatat**
  Log penggunaan disimpan dan bisa ditinjau

- [ ] **6. API dan integrasi telah diuji**
  Uji keamanan sebelum AI terhubung ke sistem internal

- [ ] **7. Hasil AI wajib melalui verifikasi**
  Analisis dan rekomendasi AI diperiksa analis sebelum dipakai

- [ ] **8. Tindakan berisiko memerlukan persetujuan manusia**
  Blokir akun, matikan layanan, atau ubah sistem produksi

- [ ] **9. Karyawan memahami data yang tidak boleh dimasukkan**
  Data pribadi, kata sandi, API key, kode internal, dokumen rahasia

- [ ] **10. Prosedur penanganan insiden AI sudah tersedia**
  Langkah jelas jika data sensitif telanjur masuk ke platform AI

Catatan: _____