

Perawatan website dan latihan pemulihan

Susun rutinitas pemeriksaan dan cadangan yang dapat dipulihkan, dengan tanggung jawab yang jelas saat terjadi gangguan.

EVALUASI & PERAWATAN

Untuk siapa panduan ini?

Pemilik website, operasional, dan pengembang yang perlu menyepakati cakupan perawatan.

Hasil yang disiapkan

Jadwal perawatan, catatan backup, dan rencana penanganan gangguan.

Bahan awal

- Daftar layanan, lisensi, dan masa berlaku
- Akses operasional sesuai peran
- Cadangan serta lingkungan untuk latihan restore

Isi Playbook

01 Persiapan / 02 Langkah kerja / 03 Contoh latihan

04 Titik review / 05 Lembar kerja / 06 Checklist & rujukan

Panduan kerja terbuka, bukan sertifikasi atau jaminan hasil. Contoh di dalamnya adalah latihan editorial, bukan dokumentasi klien.

Kerjakan dalam urutan yang jelas.

01 Petakan sistem yang harus tetap tersedia

Catat domain, sertifikat, hosting, CMS, database, formulir, dan integrasi penting. Beri pemilik serta kontak eskalasi untuk setiap sistem. Bedakan pekerjaan yang ditangani penyedia hosting, vendor, dan tim internal. Masa berlaku layanan serta aturan pembaruan perlu jelas; jangan menganggap semuanya otomatis termasuk paket.

Output: Inventaris dependensi dan pembagian tanggung jawab.

02 Jadwalkan pemeriksaan berdasarkan dampak

Periksa fungsi kontak, masa berlaku domain dan sertifikat, perubahan akses, serta pembaruan komponen. Patch perlu mengikuti risiko dan kompatibilitas; uji perubahan yang berpengaruh di lingkungan yang sesuai. Catat pemeriksaan yang dilakukan beserta temuan. Sertifikat HTTPS membantu perlindungan koneksi, tetapi bukan bukti seluruh sistem aman.

Output: Jadwal pemeriksaan dengan bukti dan tindakan.

03 Tentukan data cadangan dan batas kehilangan

Identifikasi file, konfigurasi, database, dan dokumen yang dibutuhkan untuk memulihkan layanan. Sepakati frekuensi, retensi, lokasi, dan pihak yang punya akses. Tentukan berapa kehilangan data dan waktu pemulihan yang dapat diterima bisnis sebagai target perencanaan, bukan janji tanpa pengujian. Lindungi cadangan dari akses yang tidak perlu.

Output: Spesifikasi backup dan target pemulihan yang disepakati.

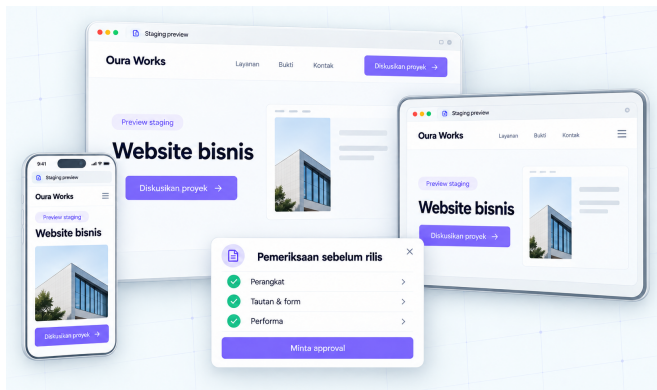
04 Latih pemulihan dan evaluasi gangguan

Lakukan restore di lingkungan uji yang terlindungi. Periksa halaman, media, formulir, dan integrasi; catat waktu serta pekerjaan manual yang diperlukan. Saat gangguan nyata, tentukan siapa memutuskan pemulihan dan memberi informasi ke tim bisnis. Setelah layanan pulih, dokumentasikan penyebab yang diketahui serta perbaikan berikutnya.

Output: Hasil latihan restore dan urutan eskalasi.

Hubungkan langkah dengan keputusan.

Latihan website dengan katalog dan inquiry: cadangan perlu memulihkan isi katalog serta konfigurasi formulir, bukan hanya file halaman yang tampak di browser.



Ilustrasi alur kerja; data dan label adalah contoh, bukan hasil klien.

Area	Pemeriksaan / latihan	Bukti yang dicatat
Domain & sertifikat	Masa berlaku serta penanggung jawab	Tanggal dan tindakan pembaruan
Formulir	Pengiriman uji dan penerimaan	Status alur sukses dan gagal
Backup	Cakupan, lokasi, retensi, akses	Log cadangan yang dapat diperiksa
Restore	Pemulihan di lingkungan uji	Fungsi yang pulih dan kendala

04 / HINDARI SALAH LANGKAH

Menjual SSL sebagai proteksi total

Keamanan melibatkan akses, aplikasi, konfigurasi, dan kebiasaan operasional, bukan sertifikat saja.

Mencadangkan tanpa pernah mencoba restore

Latihan membantu menemukan data atau langkah manual yang belum tercakup.

Susun rencana Anda.

Isi kondisi, keputusan, atau pertanyaan yang perlu dikonfirmasi. Jangan menuliskan password, token, atau data pribadi pelanggan.

01 Sistem serta pemilik

02 Rutinitas pemeriksaan

03 Data dan konfigurasi yang dicadangkan

04 Frekuensi, retensi, dan akses

05 Target pemulihan serta skenario latihan

06 Kontak eskalasi dan urutan tindakan

06 / CHECKLIST SEBELUM DISERAHKAN

- ☐ Sistem penting mempunyai pemilik
- ☐ Cakupan perawatan disepakati
- ☐ Cadangan mencakup data yang diperlukan
- ☐ Restore diuji di lingkungan terlindungi
- ☐ Eskalasi dan tindak lanjut dicatat

Periksa batas dan sumbernya.

Apakah backup harus setiap hari?

Tentukan dari frekuensi perubahan dan toleransi kehilangan data. Tidak ada jadwal tunggal yang cocok untuk semua website.

Apakah panduan ini menjamin website bebas gangguan?

Tidak. Tujuannya meningkatkan kesiapan dan kejelasan tindakan; risiko tetap perlu ditinjau sesuai sistem Anda.

Rujukan publik

[CISA: pengujian cadangan dan pemulihan](#)

<https://www.cisa.gov/stopransomware/ransomware-guide>

[CISA: autentikasi multifaktor](#)

<https://www.cisa.gov/audiences/small-and-medium-businesses/secure-your-business/require-multifactor-authentication>

Batas penggunaan

Rujukan diperiksa pada 2 Oktober 2026. Langkah, contoh, dan lembar kerja merupakan rumusan editorial Oura dengan bantuan AI dan rujukan publik. Sesuaikan keputusan dengan kondisi bisnis dan periksa hal teknis bersama pihak yang berwenang. Panduan ini bukan kontrak, sertifikasi, atau jaminan hasil.

[Baca versi interaktif Playbook](#)