**STANDAR PENEMPATAN APLIKASI BERBASIS WEB & INFRASTRUKTUR**

**{{nama organisasi}}**

**{{logo organisasi}}**

|  |  |
| --- | --- |
| No Dokumen | : 0.1 (Draft) |
| Revisi | : 00 |
| Tanggal Terbit | : |

|  |  |  |
| --- | --- | --- |
| Disusun  oleh : | Diketetahui  oleh: | Disetujui / Disahkan  oleh : |
|  |  |  |
| **NN**  NN | **NN**  NN | **NN**  NN |

**Riwayat Dokumen**

|  |  |  |
| --- | --- | --- |
| **Versi** | **Tanggal** | **Perubahan** |
| 0.1 (Draft) | 28/02/2023 | Rilis draft awal dengan hanya menyalin sepenuhnya konten dari **PEDOMAN TATA KELOLA KEAMANAN APLIKASI BERBASIS WEB - BSSN** |
| … | … | … |
|  |  |  |

1. **TUJUAN**
   1. Untuk memberikan arahan bagi instansi – instansi yang memiliki sistem web statis, web dinamis, web dinamis dengan aplikasi transaksi, serta web dinamis dengan aplikasi transaksi yang membutuhkan tingkat availibility tinggi, sehingga memiliki standar minimum dalam penyediaan infrastruktur pengamanan Aplikasi Berbasis Web.
   2. Untuk memastikan aspek *Confidentiality, Integrity, dan Availibility* aplikasi Aplikasi Berbasis Webinstansi terjaga, baik dalam konteks dikelola sendiri maupun pihak ketiga.
2. **RUANG LINGKUP**

Penempatan dengan model :

* 1. Dalam Data Center yang dimiliki sendiri secara penuh (*Dedicated DC*)
  2. Dalam Data Center Bersama (*Shared Ruang DC*)
  3. Dalam Jaringan Awan (*Cloud Network*)
  4. Dalam Data Center yang dimiliki sendiri secara penuh disertai Jaringan Awan

1. **ISTILAH DAN DEFINISI**

|  |  |  |  |
| --- | --- | --- | --- |
| 1. | Web Statis | : | * Lebih cenderung bersifat informative dimana pengguna/pengunjung hanya dapat melihat – lihat informasi di Aplikasi Berbasis Webtersebut, tidak bisa mengisi data. * Interaksi yang terjadi antara pengguna dan server hanyalah seputar pemrosesan link saja. * Halaman-halaman Aplikasi Berbasis Webtidak memliki database, data dan informasi tidak berubah-ubah kecuali diubah sintaksnya. Dokumen Aplikasi Berbasis Webyang dikirim kepada client akan sama isinya dengan yang ada di web server. * Untuk menambah halaman harus menambah file baru. |
| 2. | Web Dinamis | : | * Pengguna dapat mengupdate informasi Aplikasi Berbasis Weblangsung dari Aplikasi Berbasis Webnya. * Mengubah tampilan Aplikasi Berbasis Webmelalui Content Management System (CMS) * Menggunakan database yang digunakan untuk   menampung banyaknya data, sehingga Aplikasi Berbasis Webtinggal mengambil data dari database. |

|  |  |  |  |
| --- | --- | --- | --- |
| 3. | Web Dinamis dengan Aplikasi Transaksional |  | * Adanya fasilitas akses ke suatu aplikasi untuk konsumsi publik atau internal (internet atau intranet atau menggunakan VPN) * Umumnya terkait dengan data – data yang konfidensial dan   sensitif |
| 4. | Web Dinamis dengan Aplikasi Transaksional dan tingkat availibility | : | Web Dinamis dengan Aplikasi Transaksional dimana dalam momen tertentu atau secara rutin aplikasi itu diakses oleh banyak orang dan sangat intensif, sehingga diminimalisasi  terjadinya downtime. |
| 5. | Proxy | : | Adalah suatu sistem yang memungkinkan kita untuk bisa mengakses jaringan internet menggunakan IP yang berbeda  dengan yang diterima oleh perangkat. |
| 6. | Instansi | : | Kementerian/Lembaga, Instansi pusat atau daerah. |
| 7. | *Password* | : | Kata sandi yang digunakan bersamaan dengan *username* (*sign on/sign in/log-on/log-in*) oleh pemilik yang sah sebelum  melakukan koneksi/akses ke sistem komputer. |
| 8. | *Cloud computing* | : | Adalah penggabungan teknologi komputerisasi dan internet, dimana data mulai dari skala kecil hingga besar tersimpan di server internet, yang memungkinkan kita dapat mengakses  data kita dari berbagai lokasi dan melalui berbagai platform. |
| 9. | Software as a Service |  | Salah satu layanan cloud yang menyediakan lisensi software dan delivery model dimana pengguna dapat memanfaatkan software tersebut dimanapun dengan menggunakan device apapun melalui koneksi internet. Pengguna tidak perlu lagi melakukan install, update, atau menangani masalah pada software yang digunakan karena semua hal tersebut telah dikelola oleh vendor, pengguna hanya tinggal menggunakan layanan yang disediakan.  Contoh: Dropbox, Google Apps, [MTarget,](https://mtarget.co/) Salesforce, Cisco  WebEx. |
| 10. | Platform as a Service |  | Salah satu layanan Cloud yang menyediakan platform untuk dimanfaatkan pengguna dalam membuat aplikasi diatasnya. Pengguna dapat membangun aplikasi, upload aplikasi, testing, dan mengatur konfigurasi. Contoh: Amazon Web Service,  Microsoft Azure, Facebook, dll. |

|  |  |  |
| --- | --- | --- |
| 11. | Infrastructure as a Service | Salah satu layanan Cloud yang paling fleksibel karena pengguna memiliki kendali penuh terhadap infrastruktur yang digunakan, mulai dari server cloud, jaringan, sistem operasi, hingga penyimpanan/storage. Dalam IaaS, pengguna juga dapat membuat "pusat data virtual" di cloud dan memiliki akses ke seluruh data tanpa harus memiliki hardware sendiri.  DigitalOcean, Linode, Rackspace, Amazon Web Services  (AWS), Cisco Metapod, Microsoft Azure, Google Compute Engine (GCE) |

1. **REFERENSI**
   1. OWASP: Application Security Verification Standard 4.0
2. **STANDAR**
   1. **Gambaran Umum**
      1. Instansi dapat menempatkan Server dan Infrastruktur Pendukungnya dengan berbagai model diantaranya:
         1. Server Web & Infrastruktur Pendukungnya dimiliki sendiri secara penuh (*on - premises*) & termasuk pengelolaannya.
         2. Komputasi Awan berupa:
            * Infrastruktur sebagai Service (*Infrastructures as a Service)*
            * Platform sebagai Service *(Platform as a Service)*
            * Perangkat Lunak sebagai Service *(Software as a Service)*

**Gambar 3.5 Beberapa Model Penempatan Server & Infrastruktur Pendukungnya**

Graphical user interface

Description automatically generated with low confidence

* + 1. Untuk keperluan aplikasi Aplikasi Berbasis Web, tidak direkomendasikan Instansi menggunakan *Software as a Service*, kecuali untuk kondisi yang sangat mendesak. Dan segera mengubahnya kembali ke model yang lain.
  1. **Server Web & Infrastruktur dimiliki sendiri secara penuh (*on – premises*)**
     1. Bentuk penempatan: Dalam Data Center yang dimiliki sendiri secara penuh (*Dedicated DC*)
        1. Peruntukan: Web Dinamis dengan Aplikasi Transaksi non availibility

1. Persyaratan fisik minimal
   * Menggunakan sistem akses fisik dan prasyaratnya
2. Persyaratan perangkat minimal
   * Menggunakan UTM/NGFW dan prasyaratnya
   * Menggunakan Sistem Proteksi 0-hari dan persyaratannya
   * Menggunakan FIM dan prasyaratnya
   * Menggunakan SIEM dan prasyaratnya
   * Menggunakan NBA dan prasyaratnya
   * Menggunakan koneksi-aman untuk pihak ketiga
   * Bila menggunakan sistem server virtual harus menggunakan firewall virtual dan prasyaratnya
   * Menggunakan koneksi-aman/proxi-aman untuk akses lebih dari laman awal
     + 1. Peruntukan: Web Dinamis & Statik
3. Persyaratan fisik minimal:
   * Menggunakan sistem akses fisik dan prasyaratnya
4. Persyaratan perangkat minimal:
   * Menggunakan UTM/NGFW dan prasyaratnya
   * Menggunakan FIM dan prasyaratnya
   * Menggunakan koneksi aman untuk pihak-ketiga
     1. Bentuk penempatan: Sewa Rak dalam Data Center Bersama
        1. Peruntukan: Web Dinamik dengan Aplikasi Transaksi Non Availibility
5. Persyaratan fisik minimal:
   * Data Center bersama menggunakan sistem akses fisik dan prasyaratnya
6. Persyaratan perangkat minimal:
   * Menggunakan UTM/NGFW dan prasyaratnya
   * Menggunakan Sistem Proteksi 0-hari dan persyaratannya
   * Menggunakan FIM dan prasyaratnya
   * Menggunakan SIEM dan prasyaratnya
   * Menggunakan NBA dan prasyaratnya
   * Menggunakan koneksi-aman untuk pihak ketiga
   * Bila menggunakan sistem server virtual harus menggunakan firewall virtual dan prasyaratnya
   * Menggunakan koneksi-aman/proxi-aman untuk akses lebih dari laman awal
     + 1. Peruntukan: Web Statik dan Web Dinamis
7. Persyaratan fisik minimal:
   * Data Center bersama menggunakan sistem akses fisik dan prasyaratnya
8. Persyaratan perangkat minimal:
   * Menggunakan UTM/NGFW dan prasyaratnya
   * Menggunakan FIM dan prasyaratnya
   * Menggunakan koneksi-aman untuk pihak ketiga
     1. Bentuk penempatan: Kolokasi server dalam Data Center Bersama
        1. Peruntukan: Web Dinamis dengan Transaksi Aplikasi
9. Persyaratan fisik minimal:
   * Data Center bersama menggunakan sistem akses fisik dan prasyaratnya
10. Persyaratan perangkat minimal:
    * Bila menggunakan sistem server-virtual harus menggunakan firewall-virtual dan prasyaratnya
    * Menggunakan FIM dan prasyaratnya
    * Menggunakan Sistem Pengecoh dengan prasyaratnya
    * Menggunakan koneksi-aman/proxi-aman untuk akses
      + 1. Peruntukan: Web Statik dan Web Dinamis
11. Persyaratan fisik minimal:
    * Datacenter bersama menggunakan sistem akses fisik dan prasyaratnya
12. Persyaratan perangkat minimal:
    * Bila menggunakan sistem server-virtual harus menggunakan firewall-virtual dan prasyaratnya
    * Menggunakan eksternal FIM dan prasyaratnya
    * Menggunakan koneksi-aman/proxi-aman untuk akses
13. **Server Web Berbasis Awan (Cloud Based)**
14. Bentuk Servis: Hosting/Platform sebagai Servis (*Platform as a Service/PaaS*)
    1. Peruntukan: Web dengan Transaksi Aplikasi
       1. Persyaratan servis minimal:
          * Menyewa firewall-virtual dan prasyaratnya
          * Menggunakan eksternal FIM dan prasyaratnya
          * Menggunakan Sistem Pengecoh dengan prasyaratnya
          * Menggunakan koneksi-aman/proxi-aman untuk akses
    2. Peruntukan: Web Statik dan Web Dinamis
       1. Persyaratan servis minimal:
          * Menyewa firewall-virtual dan prasyaratnya
          * Menggunakan eksternal FIM dan prasyaratnya
          * Menggunakan koneksi-aman/proxi-aman untuk akses
15. Bentuk servis: Platform sebagai Servis (Platform as a Service/PaaS)
    1. Peruntukan: Tidak disarankan untuk digunakan Web dengan transaksi ataupun Web Dinamis
    2. Peruntukan: Web Statik
       1. Persyaratan servis minimal:
          * Menggunakan eksternal FIM dan prasyaratnya
          * Menggunakan koneksi-aman/proxi-aman untuk akses
16. Bentuk servis: Perangkat Lunak sebagai Servis (*Software as a Service/SaaS*)
    1. Peruntukan: Tidak disarankan untuk digunakan Web dengan transaksi, Web Dinamis, ataupun Web Statik
17. **Kombinasi Server Web yang dimiliki sendiri secara penuh + redundansi atau servis Server Web berbasis Awan**
18. Bagian penempatan: Dalam Data Center yang dimiliki sendiri secara penuh
    1. Peruntukan: Web dengan transaksi
       1. Persyaratan fisik minimal:
          * Menggunakan sistem akses fisik dan prasyaratnya
       2. Persyaratan perangkat minimal:
          * Menggunakan UTM/NGFW dan prasyaratnya
          * Menggunakan Sistem Proteksi 0-hari dan persyaratannya
          * Menggunakan FIM dan prasyaratnya
          * Menggunakan SIEM dan prasyaratnya
          * Menggunakan NBA dan prasyaratnya
          * Menggunakan koneksi-aman untuk pihak-ketiga
          * Bila menggunakan sistem server-virtual harus menggunakan firewall-virtual dan prasyaratnya
          * Menggunakan koneksi-aman/proxi-aman untuk akses lebih dari laman-awal
    2. Peruntukan: Web Statik dan Web Dinamis
       1. Persyaratan fisik minimal:
          * Menggunakan sistem akses fisik dan prasyaratnya
       2. Persyaratan perangkat minimal:
          * Menggunakan UTM/NGFW dan prasyaratnya
          * Menggunakan FIM dan prasyaratnya
          * Menggunakan koneksi-aman untuk pihak-ketiga
19. Bagian penempatan: Sewa Rak dalam Data Center Bersama
    1. Peruntukan: Web dengan transaksi
20. Persyaratan fisik minimal:
    * Datacenter bersama menggunakan sistem akses fisik dan prasyaratnya
21. Persyaratan perangkat minimal:
    * Menggunakan UTM/NGFW dan prasyaratnya
    * Menggunakan Sistem Proteksi 0-hari dan persyaratannya
    * Menggunakan FIM dan prasyaratnya
    * Menggunakan SIEM dan prasyaratnya
    * Menggunakan NBA dan prasyaratnya
    * Menggunakan koneksi-aman untuk pihak-ketiga
    * Bila menggunakan sistem server-virtual harus menggunakan firewall-virtual dan prasyaratnya
    * Menggunakan koneksi-aman/proxi-aman untuk akses lebih dari laman-awal
    1. Peruntukan: Web Statik dan Web Dinamis
22. Persyaratan fisik minimal:
    * Datacenter bersama menggunakan sistem akses fisik dan prasyaratnya
23. Persyaratan perangkat minimal:
    * Menggunakan UTM/NGFW dan prasyaratnya
    * Menggunakan FIM dan prasyaratnya
    * Menggunakan koneksi-aman untuk pihak-ketiga
24. Bagian penempatan: Kolokasi server dalam Data Center Bersama
    1. Peruntukan: Web dengan transaksi
25. Persyaratan fisik minimal:
    * Datacenter bersama menggunakan sistem akses fisik dan prasyaratnya
26. Persyaratan perangkat minimal:
    * Bila menggunakan sistem server-virtual harus menggunakan firewall-virtual dan prasyaratnya
    * Menggunakan FIM dan prasyaratnya
    * Menggunakan Sistem Pengecoh dengan prasyaratnya
    * Menggunakan koneksi-aman/proxi-aman untuk akses
    1. Peruntukan: Web Statik dan Web Dinamis
27. Persyaratan fisik minimal:
    * Datacenter bersama menggunakan sistem akses fisik dan prasyaratnya
28. Persyaratan perangkat minimal:
    * Bila menggunakan sistem server-virtual harus menggunakan firewall-virtual dan prasyaratnya
    * Menggunakan eksternal FIM dan prasyaratnya
    * Menggunakan koneksi-aman/proxi-aman untuk akses
29. Bagian servis: Infrastruktur sebagai Servis (*Infrastructure as a Service/IaaS*)
    1. Peruntukan: Web dengan transaksi aplikasi
30. Persyaratan servis minimal:
    * Menyewa firewall-virtual dan prasyaratnya
    * Menggunakan eksternal FIM dan prasyaratnya
    * Menggunakan Sistem Pengecoh dengan prasyaratnya
    * Menggunakan koneksi-aman/proxi-aman untuk akses
    1. Peruntukan: Web Statik dan Web Dinamis
31. Persyaratan servis minimal:
    * Menyewa firewall-virtual dan prasyaratnya
    * Menggunakan eksternal FIM dan prasyaratnya
    * Menggunakan koneksi-aman/proxi-aman untuk akses
32. Bagian Servis: Platform sebagai Servis (*Platform as a Service/PaaS*)
    1. Peruntukan: Tidak disarankan untuk digunakan sebagai redundansi Web dengan transaksi ataupun Web Dinamis
    2. Peruntukan: Web Statik
33. Persyaratan servis minimal:
    * Menggunakan eksternal FIM dan prasyaratnya
    * Menggunakan koneksi-aman/proxi-aman untuk akses
34. Bagian servis: Perangkat Lunak sebagai Servis (*Software as a Service/SaaS*)

Peruntukan: Perangkat Lunak sebagai Servis (*Software as a Service/SaaS)* tidak bisa digunakan sebagai redundansi