**PROSEDUR MANAJEMEN PIHAK KETIGA**

**DI {{nama oraganisasi}}**

**{{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. Memberikan referensi dan panduan umum bagi aktivitas pengelolaan pihak ketiga dalam Aplikasi Berbasis Web, agar dapat meminimalkan risiko keamanan yang mungkin terjadi dalam sebuah Aplikasi Berbasis Web.
   2. Memastikan bahwa setiap petugas/tim yang terlibat dalam kegiatan ini, tanggap dalam melakukan langkah- langkah untuk meminimalkan risiko keamanan atas suatu sistem Aplikasi Berbasis Web.
   3. Memastikan Aplikasi Berbasis We beserta datanya menjadi lebih aman dari kemungkinan berbagai tindakan yang tidak sah (unauthorized action).
   4. Memastikan kegiatan pengelolaan pihak ketiga dalam Aplikasi Berbasis Web berjalan dengan baik dan efektif.
   5. Memastikan adanya dokumentasi dari setiap kegiatan dalam aktivitas pengelolaan pihak ketiga dalam Aplikasi Berbasis Web.
2. **RUANG LINGKUP:**

Prosedur ini mencakup pengelolaan Aplikasi Berbasis Web oleh pihak ketiga yang lebih dititikberatkan pada aspek keamanan Aplikasi Berbasis Webdan memberikan batasan umum terhadap tanggungjawab terhadap keamanan Aplikasi Berbasis Webdari pihak-pihak yang terlibat.

1. **REFERENSI:**
   1. OWASP Testing Guide version 4.0
   2. Kebijakan Keamanan Informasi
   3. OWASP Top 10 - 2017: The Ten Most Critical Web Application Security Risks
2. **DEFINISI/ SINGKATAN:**
   1. Web hosting adalah layanan (service) yang memungkinkan suatu organisasi dan individu untuk menampilkan Aplikasi Berbasis Web atau halaman web, sehingga bisa diakses oleh pengguna dari Internet.
   2. TIK (Teknologi Informasi dan Komunikasi) adalah istilah dalam sistem komputer yang meliputi perangkat keras (hardware), perangkat lunak (software), jaringan data dan suara, aplikasi sistem informasi dan database, dan lain sebagainya.
   3. Pengguna (User) adalah akun yang digunakan untuk mengakses suatu aplikasi atau sistem TIK.
   4. Hak akses adalah hak akses suatu akun Pengguna terhadap suatu aplikasi atau sistem TIK (misal: read, write, delete, upload, download, dll).
   5. Vulnerability (Kerentanan) adalah suatu kelemahan berkaitan dengan keamanan sistem komputer (Aplikasi Berbasis Web), yang dapat dieksploitasi oleh suatu sumber ancaman (threat source), untuk melakukan suatu tindakan yang tidak sah (unauthorized action) dalam sistem komputer (Aplikasi Berbasis Web) tersebut.
   6. Exploit (Eksploitasi) adalah cara di mana suatu kerentanan dapat dimanfaatkan untuk melakukan aktivitas yang berbahaya (malicious activity) oleh peretas. Eksploitasi adalah langkah selanjutnya dari si penyerang setelah menemukan sebuah kerentanan dalam sistem komputer (Aplikasi Berbasis Web).
   7. Vulnerability Scanning adalah pemindaian terhadap suatu sistem komputer berbasis jaringan (misal: Aplikasi Berbasis Web) dengan menggunakan suatu program komputer yang dirancang untuk mencari berbagai kelemahan atau kerentanan yang terdapat dalam sistem komputer tersebut.
   8. Penetration Testing adalah simulasi serangan siber yang secara resmi dilakukan pada suatu sistem komputer (Aplikasi Berbasis Web) untuk mengevaluasi keamanan sistemnya. Pengujian ini dilakukan dengan mengeksploitasi kelemahan atau kerentanan sistem komputer yang teridentifikasi, khususnya terhadap potensi pihak yang tidak berwenang untuk bisa mendapatkan akses ke fitur dan data sistem komputer.
3. **PENANGGUNGJAWAB:**
   1. Koordinator Keamanan Aplikasi Berbasis Web, adalah individu dalam organisasi yang bertindak sebagai Penanggungjawab atas koordinator keamanan pada sistem Aplikasi Berbasis Web di organisasi.
   2. Pengelola Aplikasi Berbasis Web Pihak Ketiga, adalah pihak lain di luar Instansi yang bertindak sebagai Penanggungjawab atas pelaksanaan kegiatan web hosting pada sistem Aplikasi Berbasis Web.
   3. Pengembang Aplikasi Web, adalah Penanggungjawab atas pengembangan, pemeliharaan dan semua hal teknis yang berkaitan dengan software aplikasi web dan database.
4. **LANGKAH – LANGKAH:**
5. **Aktivitas Persiapan**

# Tabel 4.12 Aktivitas Persiapan Manajemen Pihak Ketiga

|  |  |  |
| --- | --- | --- |
| **LANGKAH** | **AKTIVITAS** | **AKTOR** |
| 1 | Menentukan prasyarat keamanan untuk Aplikasi Berbasis Webyang akan dikelola dan lingkup tanggungjawab dalam keamanan pengelolaan Aplikasi Berbasis Web   * Berdasarkan jenis aplikasi web, tingkat kritikalitas dan sensitivitas data, yang mengacu pada “Kebijakan Keamanan Informasi ”. * Berdasarkan skema web hosting yang akan digunakan.   + Shared Hosting   + Managed Hosting (VPS, Dedicated Server, Cloud) | Koordinator Keamanan Aplikasi Berbasis Web |
| 2 | Memilih Pihak Ketiga Pengelola Aplikasi Berbasis Web, dalam hal ini adalah perusahaan penyedia layanan web hosting (web hosting provider):   * Sesuai dengan skema web hosting dan yang memenuhi prasyarat keamanan Aplikasi Berbasis Web * Membuat kesepakatan layanan dan lingkup tanggungjawab terkait keamanan Aplikasi Berbasis Web | Koordinator Keamanan Aplikasi Berbasis Web |
| 3 | Membentuk dan mengkoordinasikan “Tim Penanggungjawab Pengelolaan dan Keamanan Aplikasi Berbasis Web”, terdiri dari:   * Pihak Instansi:   + Koordinator Keamanan Aplikasi Berbasis Web   + Pengembang Aplikasi Web * Pihak Ketiga:   + Pengelola Aplikasi Berbasis Web   Serta menentukan metode komunikasi, koordinasi, dan pelaporan | Koordinator Keamanan Aplikasi Berbasis Web |

|  |  |  |
| --- | --- | --- |
| 4 | Menyusun rencana kerja pengelolaan Aplikasi Berbasis Webdalam hal keamanan sesuai lingkup tanggungjawab setiap pihak.   * Instansi: bertanggungjawab atas keamanan Aplikasi Berbasis Web, diantaranya yang berkaitan dengan: software aplikasi web, kode program, struktur file ownership, file permissions, middleware, database, dan sebagainya.. * Pihak Ketiga: bertanggungjawab atas keamanan Aplikasi Berbasis Web, diantaranya yang berkaitan dengan: akses fisik, hardware (fisik atau virtual), sistem operasi, infrastruktur jaringan, dan sebagainya. | Tim Penanggungjawab Pengelolaan dan Keamanan Aplikasi Berbasis Web |

1. **Diagram Alir Aktivitas Persiapan**

**Gambar 4.13 Diagram Alir Aktivitas Persiapan Manajemen Pihak Ketiga**

**Pengelola Aplikasi Berbasis Web**

**(Pihak Ketiga)**

**Koordinator Keamanan Aplikasi Berbasis Web**

**Pengembang Aplikasi Web**

Spesifikasi Website

Menentukan prasyarat dan lingkup tanggungjawab

Memilih Pihak Ketiga Pengelola Website

Susunan Tim Penanggung Jawab

Membentuk “Tim Penanggung Jawab Pengelolaan & Keamanan Website”

Susunan Tim Penanggung Jawab

Menyusun Rencana Kerja Pengelolaan & Keamanan Website

Rencana Kerja Pengelolaan & Keamanan Website

Rencana Kerja Pengelolaan & Keamanan Website

Rencana Kerja Pengelolaan & Keamanan Website

1. **Aktivitas Pelaksanaan**

# Tabel 4.13 Aktivitas Pelaksanaan Manajemen Pihak Ketiga

|  |  |  |  |
| --- | --- | --- | --- |
| **LANGKAH** | | **AKTIVITAS** | **AKTOR** |
| 1 | | Mempersiapkan hardware dan infrastruktur untuk pengelolaan Aplikasi Berbasis Web. Pastikan bahwa prasyarat keamanan pengelolaan Aplikasi Berbasis Webtelah dipenuhi dan diimplementasikan. | Pengelola Aplikasi Berbasis Web  (Pihak Ketiga) |
| 2 | | Melakukan implementasi Aplikasi Berbasis Web pada perangkat server yang telah dipersiapkan. Pastikan bahwa semua hal teknis yang menyangkut keamanan Aplikasi Berbasis Webtelah dipenuhi dan dikerjakan. | Tim Teknis (Web Developer) |
| 3 | | Melakukan pemeliharaan hardware dan infrastruktur, sekaligus menjalankan prosedur back-up secara rutin. | Pengelola Aplikasi Berbasis Web  (Pihak Ketiga) |
| 4 | | Melaksanakan kegiatan monitoring atau pengujian secara berkala terhadap keamanan Aplikasi Berbasis Websesuai tanggungjawabnya, namun tidak selalu terbatas pada lingkup tanggungjawab yang telah ditetapkan. | * Pengelola Aplikasi Berbasis Web   (Pihak Ketiga)   * Pengembang Aplikasi Web |
| 5 | | Jika dalam kegiatan monitoring atau pengujian terdeteksi suatu masalah keamanan, maka melakukan pemeriksaan dan validasi terhadap masalah keamanan yang terdeteksi untuk menentukan langkah selanjutnya, | * Pengelola Aplikasi Berbasis Web   (Pihak Ketiga)   * Pengembang Aplikasi Web |
|  | 5.1 | Memilah dan mengklasifikasikan masalah keamanan tersebut terkait dengan tingkat potensi ancaman (risiko keamanan), |
| 5.2 | Melaporkan masalah keamanan tersebut kepada “Koordinator Keamanan Aplikasi Berbasis Web”, bila masalah keamanan tersebut berada di luar wewenangnya untuk bisa langsung melakukan tindak lanjut. |

|  |  |  |  |
| --- | --- | --- | --- |
|  | 5.3 | “Koordinator Keamanan Aplikasi Berbasis Web” selanjutnya menyampaikan masalah keamanan tersebut ke pihak yang berwenang untuk ditindaklanjuti. | Koordinator Keamanan Aplikasi Berbasis Web |
| 6 | | Melakukan langkah tindak lanjut (perbaikan) terhadap masalah keamanan sesuai dengan tanggungjawab dan wewenangnya. | * Pengelola Aplikasi Berbasis Web   (Pihak Ketiga)   * Pengembang Aplikasi Web |
| 7 | | Membuat dokumentasi dan membuat laporan kegiatan pengelolaan Aplikasi Berbasis Web(dalam hal keamanan) secara periodik untuk diserahkan kepada “Koordinator Keamanan Aplikasi Berbasis Web” | * Pengelola Aplikasi Berbasis Web   (Pihak Ketiga)   * Pengembang Aplikasi Web |

1. **Diagram Alir Aktivitas Pelaksanaan**

**Gambar 4.14 Diagram Alir Aktivitas Pelaksanaan Manajemen Pihak Ketiga**



|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Pengelola Aplikasi Berbasis Web (Pihak Ketiga)** | **Koordinator Keamanan Aplikasi Berbasis Web** | | | | | | **Pengembang Aplikasi Web** |
| Mempersiapkan perangkat server dan infrastruktur  Melakukan Pemeliharaan Melakukan Implementasi  & Prosedur Backup Website  Melakukan Monitoring Melakukan Pengujian  Keamanan Website Berkala Keamanan  Website    Masalah Masalah  Tidak Keamanan? Tidak Keamanan?  Ya  Ya  Melakukan Melakukan  Penilaian & Klasifikasi Penilaian & Klasifikasi  Masalah Keamanan Informasi Masalah Keamanan  Masalah  Tidak  Berwenang? Berwenang?  Ya  Ya  Melakukan Tindak Lanjut Informasi Melakukan Tindak Lanjut (Perbaikan) Masalah (Perbaikan) | | | | | | | |
|  | | |  | | | Membuat Dokumentasi  dan Pelaporan Berkala | |
| Membuat Dokumentasi dan Pelaporan Berkala | |  | Laporan Pengelolaan &  Keamanan Website | |  |
|  |  |  |  | |
|  | |  |  | | |
|  | | | | | | | |