**PROSEDUR PENANGANAN INSIDEN TEKNOLOGI INFORMASI**

|  |  |
| --- | --- |
| **Document Number** | **MAP/IS/04-ITS/SOP/05.0** |
| **Effective Date** |  |
| **Version Number** | **1.0** |
| **Document Owner** | **System – Information and Policy Directorate** |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Approval List (Sign & Name)**   |  |  | | --- | --- | |  |  | | **Ari Tjahjanto** | **Imam Rofii** | | ***Information & Policy Director*** | ***System Infrastructure & Application Manager*** | |  |  | |  |  | |  |  | |  |  | |  |  | |  |  | |  |  | |  |  | |  |  | | **Document History**   |  |  | | --- | --- | | V 1.0 – August 2017 - Nurul Akbar | Initial Document  First Version of sign off | | V 1.23 – September 2017 – Nurul Akbar | Revision | |  |  | |  |  | |
| **Reference**   |  | | --- | |  | | **Level of Confidentiality**  FS\_H  FS\_C  FS\_I  FS\_P | |

**LEMBAR PERSETUJUAN KARYAWAN TERKAIT**

|  |  |  |  |
| --- | --- | --- | --- |
| **No** | **Review Oleh** | **Detail** | **Tanda Tangan** |
| 1 | Dea Rendra Kirana |  |  |
| *Business Compliance Manager* |
| 2 | Edith Fernando |  |  |
| *System Infrastructure Team Leader* |
| 3 | Dadang Setiawan |  |  |
| *System Application Team Leader* |
| 4 | Yulianto Hadi Wibowo |  |  |
| *Risk Management Specialist* |
| 5 | Ahmad Iman Sudrajat |  |  |
| *Business Process Specialist* |
| 6 | Bong Suripno |  |  |
| *Network Analyst* |

**LEMBAR PARAF PENYUSUN:**

|  |  |
| --- | --- |
| **Disusun Oleh:** | |
| Nurul Akbar |  |
| *Information Security* |
| Uswatun Aulia |  |
| *Data Center Analyst* |

**DAFTAR ISI**

[1. TUJUAN 4](#_Toc494879103)

[2. RUANG LINGKUP 4](#_Toc494879104)

[3. *MILESTONE* UTAMA 6](#_Toc494879105)

[4. DEFINISI DAN ISTILAH 6](#_Toc494879106)

[5. *FLOW* DUKUNGAN PENANGANAN INSIDEN 8](#_Toc494879107)

[6. DOKUMEN PENDUKUNG 10](#_Toc494879108)

# **TUJUAN**

Prosedur penanganan insiden pengguna layanan Teknologi Informasi dan Komunikasi (TIK) adalah metode *troubleshooting* untuk *Internal Network System* seperti Server, Interkoneksi Jaringan, Internet, Konektivitas VPN milik perusahaan, *Cyber Attack to Internal Network*, dan sebagainya. Proses ini melibatkan pakar perusahaan di bidang *IT Infrastructure and Security*. Proses ini diterapkan untuk semua masalah terkait jaringan dan infrastruktur (hal ini termasuk perangkat kantor: *laptop* / *printer*, dll).

Dokumen ini menguraikan pedoman untuk menentukan urutan aktivitas, pihak-pihak yang terlibat dan bertanggung jawab, dalam konteks bagaimana mengelola penanganan insiden terhadap penggunaan fasilitas berbasis teknologi informasi di Jaringan Internal perusahaan.

Prosedur ini akan disempurnakan secara berkesinambungan dan dapat berubah sewaktu bisnis berkembang dan mungkin dipengaruhi oleh perubahan teknologi.

# **RUANG LINGKUP**

Prosedur ini mencakuppenanganan insiden pengguna TIK.

|  |  |
| --- | --- |
| **Titik Awal** | Tanggal pelaporan insiden |
| **Titik Akhir** | Tanggal insiden di selesaikan |
| **Ruang Lingkup Layanan** | * Laporan insiden * Area yang terkena dampak * Daftar insiden internal * Pencatatan permintaan penanganan insiden * Memberikan dukungan atau resolusi insiden * Eskalasi pelaporan insiden |
| ***Input*** | Laporan permintaan penanganan insiden |
| ***Output*** | Laporan hasil penyelesaian insiden |

Berikut ini adalah ruang lingkup insiden pengguna Teknologi Informasi dan Komunikasi FiberStar:

|  |  |  |
| --- | --- | --- |
| **Kategori insiden** | **Deskripsi** | |
| 1. *Internet* | Permasalahan koneksi dari internal perusahaan ke *Internet*. |
| 1. Perangkat jaringan | Gangguan koneksi internal (LAN & WIFI). |
| 1. *VPN gateway* | Permasalahan terkait dengan *VPN gateway Cisco AnyConnect*. |
| 1. Serangan siber dan keamanan informasi | Indikasi serangan siber dari external ke internal (contoh: *DDOS, malware, virus, spam, phishing,* dll.) |
| 1. Sistem tiket | Gangguan terhadap sistem tiket perusahaan. |
| 1. *Notebook* | Permasalahan yang berkaitan dengan *laptop* perusahaan (contoh: *blue screen, hanging, bootloop,* lambat, mati total, dsb.) |
| 1. Perubahan dan penghapusan *domain* | Permasalahan yang berkaitan dengan *domain* (contoh: *permission issue, group policy issue, domain issue*, dsb.) |
| 1. *Email issue* | Permasalahan yang berkaitan dengan *email* (contoh: salah penamaan *email,* masalah *authentication, mailing group issue,* dsb.) |
| 1. *File sharing & quota* | Permasalahan dengan file sharing (contoh: *user’s permission & privilege*, *full capacity* dalam *file sharing*, dsb.) |
| 1. Modifikasi & penghapusan *Application / Software* | Permasalahan yang berkaitan dengan aplikasi atau perangkat lunak untuk *Notebook* perusahaan. |
| 1. Modifikasi & penghapusan *ext. phone* | Permasalahan yang berkaitan dengan sistem *telephony* perusahaan*.* |
| 1. *Printer* | Permasalahan yang berkaitan dengan mesin *printer* perusahaan. |
| 1. *Video Conference* | Permasalahan yang berkaitan dengan *sistem video conference* perusahaan. |
| **Keterangan**: Kategori insiden tidak dibatasi oleh daftar ini. Segala sesuatu yang termasuk dalam ruang lingkup departemen sistem infrastruktur dan aplikasi yang **sudah *exist* (bukan *new request*)** dapat menjadi pertimbangan untuk menjadi layanan atau insiden dari departemen sistem infrastruktur dan aplikasi. | |

# ***MILESTONE* UTAMA**

1. Pelaporan dan pencatatan permintaan penanganan insiden
2. Memberikan resolusi insiden tahap awal
3. Mengkoordinasikan resolusi lanjutan
4. Konfirmasi atas penanganan yang telah diberikan

# **DEFINISI DAN ISTILAH**

|  |  |  |
| --- | --- | --- |
| **NO** | **SIMBOL / KATA** | **KETERANGAN** |
| 1 |  | Proses mulai. |
| 2 |  | Proses atau aktifitas. |
| 3 |  | *Decision.* |
| 4 |  | Alur ke proses berikutnya. |
| 5 |  | Proses berakhir. |
| 6 | **Unit Kerja Sistem Infrastruktur dan Aplikasi** | Departemen Sistem Infrastruktur dan Aplikasi Perusahaan. |
| 7 | **Unit Kerja** | Unit-unit kerja dalam lingkungan perusahaan yang meliputi divisi, satuan, unit dan cabang. |
| 8 | **Perusahaan** | PT. Mega Akses Persada. |
| 9 | **Kepala Bagian Sistem Infrastruktur dan Aplikasi** | Karyawan perusahaan yang mengelola unit kerja bagian sistem infrastruktur dan aplikasi |
| 10 | **Pengguna akhir TIK** | Pengguna TI yang mencakup karyawan perusahaan (*end user*). |
| 11 | ***1st level support*** | Karyawan perusahaan yang mencakup *service desk unit* dalam departemen sistem. |
| 12 | ***2nd level support*** | Karyawan perusahaan mencakup tim aplikasi, infrastruktur dan keamanan informasi. |
| 13 | ***3rd level support*** | Entitas yang mencakup individu atau tim yang lebih khusus seperti Spesialis Jaringan, Spesialis Server, dsb. Individu ini bisa merupakan principal dari suatu sistem atau perangkat. |
| 14 | ***Management lead*** | Karyawan perusahaan yang mencakup karyawan diluar departemen sistem yang ditunjuk untuk menjalankan proses *problem management.* |
| 15 | ***Log*** | Log adalah rekaman/*record* dari suatu proses. |
| 16 | ***Process Problem Management*** | Process Problem Management adalah sebuah proses terkait dengan pengelolaan masalah di level manajemen. |

# ***FLOW* DUKUNGAN PENANGANAN INSIDEN**





# **DOKUMEN PENDUKUNG**

* *IT Service Request Form*
* *Incident handling acceptance*