Standar Sistem Manajemen Keamanan Informasi di Universitas Negeri Manado

John Reimon Batmetan, Bierhoff Parengkuan, Kenny Tatauhe , Fanny Worotijan.

Pendidikan Teknologi Informasi dan Komunikasi Universitas Negeri Manado, Tondano, 95618

john.reimon@gmail.com, Bierparengkuan@gmail.com

ABSTRAK

Salah satu kunci keberhasilan pengaman sistem informasi adalah adanya visi dan komitmen dari pimpinan top manajemen. Upaya atau inisiatif pengamanan akan percuma tanpa hal ini. Dengan tidak adanya komitmen dari top manajemen, berdampak kepada investasi pengamanan data. Selain itu keberhasilan juga ditentukan seperti proses desain, implementasi, konfigurasi, dan pemakaian. Untuk itu diperlukan standar dan manajemen yang memadai agar kemandirian dapat dilakukan secara memadai pula. Standar kompetensi dapat dilakukan sesuai dengan TKTI jika menggunakan standar Nasional. Standar kompetensi tidak berarti hanya kemampuan menyelesaikan suatu tugas, tetapi dilandasi pula bagaimana serta mengapa tugas itu dikerjakan. Selain itu standar ISO yang merupakan standar internasional dapat diterapkan yaitu menggunakan ISO 17799. Manajemen operasi keamanan harus memenuhi beberapa hal penting yaitu kontrol dan proteksi, monitoring dan auditing, serta pemahaman tentang threat dan vulnerabilitas.

Kata kunci: SKMI, SOP, ISO 17799, keamanan informasi, UNIMA

PENDAHULUAN

Permasalahan keamanan komputer selalu menarik untuk dibahas, hal ini karena perkembangan teknologi informasi yang semakin canggih dan meluas. Semakin canggih teknologi informasi ternyata terkadang tidak diikuti dengan penerapan keamanan yang memadai, sehingga ancaman keamanan selalu menjadi momok bagi penerapan sistem komputer dalam sebuah organisasi atau perusahaan. Salah satu kunci keberhasilan pengaman sistem informasi adalah adanya visi dan komitmen dari pimpinan top manajemen. Upaya atau inisiatif pengamanan akan percuma tanpa hal ini. Dengan tidak adanya komitmen dari top manajemen, berdampak kepada investasi pengamanan data. Pengamanan data tidak dapat tumbuh demikian saja tanpa adanya usaha dan biaya. Pengamanan data elektronik

membutuhkan investasi, tanpa investasi akan sia-sia upaya pengamanan data. Sayangnya hal ini sering diabaikan karena tidak adanya komitmen dari pihak manajemen untuk solusi keamanan.

HASIL DAN PEMBAHASAN

Kesalahan desain terjadi pada tahap desain dimana keamanan seringkali diabaikan atau dipikirkan belakangan (*after thought*). Sebagai contoh ada sebuah sistem informasi yang menganggap bahwa sistem operasi akan aman dan juga jaringan akan aman sehingga tidak ada desain untuk pengamanan data, misalnya dengan menggunakan enkripsi.

Kesalahan implementasi terjadi pada saat desain diimplementasikan menjadi sebuah aplikasi atau sistem. Sistem informasi

diimplementasikan dengan menggunakan software. Sayangnya para pengembang software seringkali tidak memiliki pengetahuan mengenai keamanan sehingga aplikasi yang dikembangkan memiliki banyak lubang keamanan yang dapat dieksploitasi.

Kesalahan konfigurasi terjadi pada tahap operasional. Sistem yang digunakan biasanya harus dikonfigurasi sesuai dengan kebijakan perusahaan. Selain salah konfigurasi, ada juga permasalahan yang disebabkan karena tidak adanya kebijakan prosedural dari pemilik sistem sehingga menyulitkan bagi pengelola untuk melakukan pembatasan.

Kesalahan penggunaan terjadi pada tahap operasional juga. Kadang-kadang karena sistem terlalu kompleks sementara sumber daya yang disediakan sangat terbatas maka dimungkinkan adanya kesalahan dalam penggunaan.

Kesalahan-kesalahan di atas dapat menimbulkan celah lubang keamanan. Celah ini belum tentu menimbulkan masalah, sebab bisa saja memang celah ada akan tetapi tidak terjadi eksploitasi. Namun celah ini merupakan sebuah resiko yang harus dikendalikan dalam sebuah manajemen keamanan.

Standar Keamanan Komputer

1. Standart Kompetensi Keamanan menurut TKTI.

Standar kompetensi diartikan sebagai suatu ukuran atau patokan tentang pengetahuan, keterampilan, dan sikap kerja yang harus dimiliki oleh seseorang untuk mengerjakan suatu pekerjaan atau tugas sesuai dengan unjuk kerja yang dipersyaratkan oleh Tim Koordinasi Telematika Indonesia (TKTI, 2004). Standar kompetensi tidak berarti hanya kemampuan menyelesaikan suatu tugas, tetapi dilandasi pula bagaimana serta mengapa tugas itu dikerjakan. Berdasarkan jenis kelompok Sumber daya manusia (SDM) pada teknologi informasi dan komunikasi (*information and communication technology* - ICT) berikut kompetensinya, yang

berhubungan dengan keamanan dan pemeliharaan komputer, adalah :

a. unit kompetensi no. 16.

Judul Unit : Mendeskripsikan Kewaspadaan Terhadap Keamanan Informasi

Uraian Unit : Unit kompetensi ini berhubungan dengan pemahaman prinsip keamanan informasi guna meningkatkan kewaspadaan atas keamanan informasi. Berupa :

- Kaidah Umum Keamanan Informasi
- Pemilihan dan Penggunaan Password
- Identifikasi Resiko Keamanan Atas Penggunaan Internet
- Pengelolaan Data/Informasi Secara Aman

b. unit kompetensi no. 17

Judul Unit : Menggunakan Piranti lunak Anti Virus

Uraian Unit : Unit kompetensi ini berkaitan dengan penggunaan piranti lunak anti virus yang umum digunakan dengan tujuan agar dapat melindungi komputer dari berbagai jenis virus standard yang dapat menyebar di komputer kita. Berupa :

- Mengidentifikasi jenis virus
- Mempersiapkan Piranti lunak Anti Virus dijalankan.
- Mengoperasikan piranti lunak anti virus
- Melakukan pencegahan

c. unit kompetensi no. 20

Judul Unit : Melakukan penanganan awal (*Troubleshooting*) atas masalah pada PC

Uraian Unit : Unit kompetensi ini berhubungan dengan pemahaman tentang cara kerja komputer (PC) dan penanganannya apabila komputer tersebut tidak bisa bekerja. Berupa :

- Cara Kerja Komputer
- Instalasi Komponen Komputer
- Penggunaan Alat Bantu Deteksi Masalah

- Diagnosa Masalah dan Penanganan Masalah (*Troubleshoot*)

d. unit kompetensi no. 21

Judul Unit : Mengoperasikan utilitas dasar untuk Backup, Restore, Data Recovery

Uraian Unit : Unit kompetensi ini berkaitan dengan langkah-langkah dasar dalam melakukan pengamanan terhadap data-data elektronik dalam komputer yang dimiliki. Berupa :

- Mengidentifikasi dan mendeskripsikan aspek-aspek pengamanan data
- Melindungi data di komputer dari gangguan
- Melakukan Data Recovery

e. unit kompetensi no. 24

Judul Unit : Mengimplementasikan sistem keamanan dan keselamatan pada pengoperasian komputer

Uraian Unit : Unit kompetensi ini berhubungan dengan penguasaan konsep dasar keamanan sistem komputer yang harus dibuat untuk menjamin keamanan sistem komputer yang digunakan. Berupa

- Mengidentifikasi Ancaman Keamanan
- Standar Pengamanan Komputer Dasar

2. Manajemen Keamanan sesuai ISO 17799

ISO (*International Standard Organisation*) atau Organisasi standar Internasional merupakan badan penetap standar internasional yang terdiri dari wakil-wakil dari badan standar nasional setiap negara. ISO menetapkan standar-standar industrial dan komersial dunia. Standard ISO 17799 adalah merupakan suatu standar sistem manajemen keamanan informasi (*Informasi Security Management system*) yang telah disempurnakan dan diterapkan untuk digunakan oleh perusahaan-perusahaan di dalam mengamankan data atau informasi yang dimilikinya. Dengan adanya standar ISO 17799 maka kita akan dapat mengukur apakah sistem

keamanan informasi yang kita terapkan sudah efektif dan memberikan jaminan keamanan terhadap konsumen.

Sebelum diperkenalkan ISO 17799, pada tahun 1995, *Britania Standard Institut* (BSI) meluncurkan standard pertama mengenai manajemen informasi di seluruh dunia, yaitu “B 7799”, Bagian Pertama: Kode Praktek untuk Manajemen Keamanan

Informasi, yang didasarkan pada Infrastruktur pokok B 7799. Kemudian pada tanggal 1 Desember, 2000, ISO 17799 standard mengenai manajemen informasi baru diterbitkan.

Pemakaian standar ISO 17799 meliputi kebutuhan akan hal-hal sebagai berikut :

- Dokumen kebijakan keamanan informasi
- Adanya Tanggung jawab keamanan informasi
- Adanya program pendidikan dan pelatihan keamanan informasi untuk semua pemakai (*user*)
- Mengembangkan suatu sistem untuk pelaporan peristiwa keamanan
- Memperkenalkan teknik pengendalian virus
- Mengembangkan suatu rencana kesinambungan bisnis
- Mengendalikan pengkopian perangkat lunak kepemilikan
- Surat pengantar arsip organisatoris untuk mengikuti kebutuhan perlindungan data,
- Menetapkan prosedur dalam mentaati kebijakan keamanan.

Sedangkan Kebijakan pengendalian atau kontrol menurut standar ISO 17799 meliputi : kebijakan keamanan, organisasi keamanan, penggolongan dan pengendalian asset, keamanan personil, keamanan fisik dan kendali lingkungan, pengembangan dan manajemen jaringan komputer, sistem akses kendali, pemeliharaan sistem, perencanaan kesinambungan bisnis, dan pemenuhan. Guna meminimalkan resiko ancaman keamanan yang merugikan bisnis, maka masalah tersebut harus ditangani dengan menggunakan suatu tindakan

pencegahan (*preventive action*) tanpa harus menunggu dalam keadaan darurat dalam melakukan tindakan keamanan. Dalam rangka pro aktif terhadap kebutuhan keamanan, arsitektur keamanan meliputi tiga unsur pokok:

Kebijakan perusahaan yaitu keterlibatan manajemen dalam alokasi sumber daya dan suatu visi yang strategis dan permasalahan global dalam keamanan, Perilaku individu (pelatihan karyawan, dan adanya proses komunikasi).

Dalam standar ISO 17799, sistem manajemen keamanan informasi yang efektif dan efisien akan memberikan petunjuk bagi perusahaan atau organisasi untuk:

- Secara konstan memperbaharui (*update*) atas adanya ancaman baru serta mengambil tindakan dengan pertimbangan yang sistematis.
- Melakukan penanganan kecelakaan dan kerugian dengan tindakan pencegahan dan peningkatan keamanan sistem yang berkelanjutan.
- Mengetahui ketika kebijakan dan prosedur tidak cukup mampu diterapkan dalam usaha pencegahan ancaman keamanan.
- Menerapkan kebijakan dan prosedur tentang pentingnya manajemen keamanan, dengan mengikuti "prosedur praktek terbaik" dan manajemen resiko yang baik.

Dengan mengenali nilai manajemen keamanan informasi yang strategis ini, maka dapat ditawarkan suatu rencana inovasi sertifikasi, berdasar pada rencana sertifikasi BS7799-2:1999 dan petunjuk ISO17799. Dimana isi dari ISO-17799 meliputi : 10 Ketentuan Pengendalian (*control clauses*), 36 Tujuan Pengendalian (*control objectives*), dan, 127 Kendali (*controls*). Kendali / Kontrol tersebut diuraikan pada tingkat tinggi, tanpa memasukkan masalah teknologi secara detail, dalam rangka membiarkan perusahaan / organisasi masing-masing secara total bebas untuk memilih kendali itu yang terdekat ke

situasi cultural/technological dan kebutuhan sendiri.

Fungsi Keamanan Dalam Organisasi

Setiap personal (staff) keamanan TI harus mengerti dan mengimplementasi kontrol manajemen, operasional dan teknis. Implementasi penuh terhadap semua jenis kontrol membutuhkan staff keamanan TI dengan berbagai keahlian. Pada suatu saat tim keamanan tersebut bias bertindak sebagai spesialis pengadaan barang yang meninjau sebuah spesifikasi dari system upgrade atau kemudian bertindak sebagai pengajar dalam kelas IT security awareness.

Dalam kenyataannya diberbagai organisasi dengan beragam tugas dari tim keamanan TI sering dihadapkan pada kekurangan sumberdaya atau prioritas beban kerja untuk menyelesaikan hanya tugas-tugas yang penting. Fungsi-fungsi yang dibahas dibawah ini mengandung jumlah staff yang dibutuhkan untuk menyelesaikan fungsi tersebut dalam tingkat yang minimal. Tingkat ini dihitung dalam bentuk prosentasi dari 1 staff per tahun.

a. Audit.

Auditor bertanggungjawab dalam memeriksa sistem untuk melihat apakah sistem tersebut telah memenuhi kebutuhan keamanan TI. termasuk sistem dan kebijakan organisasi, dan apakah kontrol keamanan TI telah dijalankan dengan benar.

b. Physical Security

Pada banyak organisasi, bagian keamanan fisik ini pada umumnya adalah staff keamanan berupa satuan pengamanan (satpam). Bagian keamanan fisik biasanya bertanggungjawab untuk mengembangkan dan menjalankan kontrol keamanan fisik yang baik, dengan konsultasi dengan manajemen keamanan komputer. program dan manajer fungsional, dan yang pihak lain yang diperlukan.

c. *Disaster Recovery/Contingency Planning*

Staff keamanan TI harus memiliki disaster recovery/contingency planning team. Tim ini bertanggungjawab pada aktifitas contingency planning organisasi tersebut dan bekerjasama dengan bagian keamanan fisik, telekomunikasi, IRM, pengadaan barang dan pegawai lainnya.

d. *Pengadaan (Procurement)*

Bagian pengadaan bertanggungjawab untuk memastikan pengadaan barang dalam organisasi telah ditinjau oleh petugas yang berwenang.

e. *Pelatihan*

Pelatihan mengenai keamanan TI termasuk dalam kebutuhan keamanan TI. Staff keamanan TI memiliki salah satu tanggung jawab utama untuk memberikan pelatihan kepada user, operator, dan manajer mengenai keamanan komputer.

f. *Sumberdaya Manusia (Personalia)*

Bagian personalia dan staff keamanan TI harus bekerjasama dalam melakukan investigasi terhadap latar belakang dan, prosedur pemberhentian kerja dari seorang pegawai yang hendak mengundurkan diri.

g. *Risk Management/Planning*

Beberapa organisasi memiliki staff yang bertugas mempelajari berbagai tipe resiko yang mungkin dihadapi oleh organisasi. Staff keamanan TI harus mengembangkan proses untuk mengenali resiko yang ada dalam siklus hidup organisasi. Ketika sebuah kelemahan (vulnerabilities) terdeteksi, tim keamanan harus menganalisa resiko dan jumlah sumberdaya yang dibutuhkan untuk menurunkan resiko (mitigate the risk).

h. *Building Operations*

Bagian pemeliharaan gedung bertanggungjawab dalam memastikan bahwa setiap fasilitas keamanan gedung, daya listrik dan kontrol lingkungan gedung, aman digunakan selama masa operasional organisasi.

i. *System Management/System Administrators*

Pegawai ini adalah manajer dan teknisi yang merancang dan mengoperasikan suatu sistem, jaringan komputer dan LAN dari organisasi. Mereka bertanggungjawab dalam mengimplementasikan keamanan teknis dan harus paham terhadap teknologi pengamanan TI yang berhubungan dengan sistem mereka. Mereka juga perlu memastikan kontinuitas dari layanan mereka dalam memenuhi kebutuhan manajer fungsional, serta menganalisa kelemahan yang ada pada sistem.

j. *Telekomunikasi*

Bagian telekomunikasi bertanggungjawab untuk menyediakan layanan telekomunikasi termasuk telekomunikasi suara, data, video dan layanan faks.

k. *Help Desk*

Apakah bagian Help Desk menangani atau tidak menangani setiap insiden, ia harus dapat mengenali gangguan keamanan dan meneruskan panggilan tersebut kepada pihak yang berwenang dalam organisasi untuk direpson. Tim keamanan TI harus bekerjasama dengan manajemen help desk untuk memastikan prosedur yang ada telah dijalankan dalam menangani insiden yang berhubungan dengan keamanan TI.

l. *Maintenance of Security Program*

Program keamanan membutuhkan beberapa aktifitas tambahan yang tidak tercantum dalam fungsi-fungsi diatas. Untuk setiap area fungsi harus memiliki dokumen penuntun bagi staff dan tim keamanan TI. Dokumen tersebut harus diteliti, ditulis, ditinjau dan diawasi secara berkala.

Manajemen Operasi Keamanan

Dalam penggunaan teknologi informasi di setiap institusi, terutama yang mengutamakan teknologi informasi dalam proses bisnisnya membutuhkan suatu operasional yang optimal untuk dapat mendukung bisnis yang berjalan. Bila berbicara tentang operasional, maka banyak hal yang bisa dilibatkan mulai dari *hardware*,

software, prosedur dan sumber daya manusianya sendiri untuk bisa melaksanakan operasional itu. Ketergantungan dari setiap komponen di atas sangatlah menentukan keberhasilan operasional yang dilakukan tetapi dengan keberhasilan operasional dengan teknologi yang canggih pun tanpa melibatkan faktor keamanan semuanya menjadi kurang berarti karena informasi atau data apapun yang dihasilkan dari teknologi tanpa adanya keamanan bisa menjadi bencana bila tidak memperhatikan *confidentiality*, *integrity* dan *availability* pada umumnya dan keamanan pada khususnya sehingga setiap informasi yang dimiliki benar-benar diperlakukan sebagai asset yang berharga bagi institusi.

Untuk menjamin keamanan operasional tidak hanya bicara teknologi pelindungnya, tetapi kebijakan yang jelas dalam melakukan keamanan operasional adalah sangat penting untuk dapat dijalankan dengan baik karena ancaman yang paling tinggi pada prakteknya adalah dari sumber daya internal sendiri. Hal ini adalah ancaman yang sebenarnya sangat mengancam dan sulit untuk diperkirakan, karena internal sumber daya sudah ada di dalam sistem itu sendiri. Dalam rangka meminimalisasi ancaman ini maka kebijakan untuk keamanan operasional harus dibuat dengan sedetail mungkin memperkirakan hal-hal yang dapat menjadi ancaman, dan melakukan prosedur – prosedur keamanan dengan konsekwen. Jadi tanpa kebijakan dan prosedur yang baik maka tidak hanya ancaman dari luar yang menakutkan tetapi juga lebih menakutkan ancaman dari dalam. Untuk itu setiap divisi teknologi informasi harus punya kebijakan untuk *corporate user* dalam menggunakan sumber daya teknologi informasi yang dipunyai.

Dalam pembahasan ini akan dijelaskan setidaknya terdapat 3 hal besar yang harus dapat dipahami :

1. *Control and Protection*. Berisi pemahaman tentang pengaturan dan proteksi dalam kegiatan operasional untuk dapat mencapai tingkat keamanan operasional yang optimal ada beberapa hal yang harus diperhatikan diantaranya adalah *preventive control*,

corrective control *detective control*, *deterrent control*, *application control*, *transaction control* dan *separation and rotation of duties* lebih menekankan kepada *confidentiality* (kerahasiaan) dan *integrity* atau keutuhan data. Semua hal di atas lebih memfokuskan juga pada prosedur pengawasan yang optimal dalam melakukan berbagai hal mulai dari pencegahan hingga rotasi tugas yang baik dan bila tidak dilakukan dengan benar akan menjadi ancaman dan membuka lebar pintu keamanan.

2. *Monitoring and Auditing*. Setelah dilakukan pengaturan dan proteksi yang baik maka tidak bisa hanya berhenti untuk bisa melakukan proteksi tetapi tetap diperlukan monitoring and auditing untuk bisa mengetahui dan menjamin sejauh mana keamanan yang sudah dicapai, faktor yang harus diperhatikan adalah *Change management*, *Escalation management*, *Record retention*, *Due dilligince*, dan *Logging monitoring*. Dengan melakukan hal-hal diatas yang lebih bersifat prosedur maka pengawasan keamanan dapat lebih ditingkatkan.

3. *Threat and Vulnerabilities*. Berisi pemahaman tentang jenis ancaman dan kelemahan yang dapat mengancam operasional keamanan yang sudah dilakukan. Untuk *threat* dan *vulnerability* beberapa hal yang akan dibahas adalah *Accidental Loss*, *Inappropriate Activities*, *Illegal computer operations*, *Account maintenance*, *Data Scavenging Attacks*, *IPL/rebooting*, dan *Network highjacking*.

KESIMPULAN

Penerapan sistem keamanan dalam sebuah organisasi yang ideal tentunya harus memenuhi persyaratan standarisasi sesuai dengan ketentuan yang berlaku pada standar sistem keamanan baik itu TKTi dan ISO. Namun begitu mengingat

keterbatasan sumber daya pada beberapa organisasi atau perusahaan kecil dan menengah, maka standar tersebut beberapa bagian diantaranya dapat digabungkan. Namun begitu prinsip keamanan harus tetap memenuhi aspek-aspek yang menjadi persyaratan keamanan yaitu *confidentiality*, *integrity* dan *availability*. Untuk mencapai aspek tersebut maka perlu diperhatikan beberapa hal yang penting yaitu adanya kontrol dan proteksi, monitoring dan auditing, serta pemahaman tentang *threat* dan *vulnerabilitas*.

DAFTAR PUSTAKA

- [1]. Depkominfo, 2006, "*Pedoman Praktis manajemen Keamanan Informasi untuk Pimpinan Organisasi, 10 Rekomendasi Terbaik Manajemen Keamanan Informasi*", Direktorat Sistem Informasi, Perangkat Lunak Dan Konten Direktorat Jenderal Aplikasi Telematika Departemen Komunikasi Dan Informatika
- [2]. Budi Raharjo, 2005, "*Keamanan Sistem Informasi Berbasis Internet*", PT Insan Infonesia - Bandung & PT INDOCISC – Jakarta Internet
- [3]. Gary Stoneburner, dkk, 2004, "*Computer Security: Engineering Principles For Information Technology Security (Baseline for Achieving Security), Revision A*", NIST. 4. <http://www.wikipedia.org>
- [4]. [http://amutiara.files.wordpress.com/2007/01 /sp800-86.pdf](http://amutiara.files.wordpress.com/2007/01/sp800-86.pdf)
- [5]. IEEE 802.11 Working Group. <http://grouper.ieee.org/groups/802/11/ind ex. html>.
- [6]. NIST Special Pub. 800-86:, 2005, "*Guide to Computer and Network Data Analysis: Applying Forensic Techniques to Incident Response (Draft)*", <http://csrc.nist.gov/publications/drafts/DraftSP800-86.pdf>.
- [8]. J. R. Batmetan Suyoto, J. D. C. L. Soares, "An Empirical Investigation on Customer Behavior to Adopt Mobile Commerce among the Y Generation in Indonesia", Sriwijaya International Conference On Engineering, Science & Technology [SICEST 2016], 2016
- [9]. J.R. Batmetan, "Algoritma Ant Colony Optimization (ACO) untuk Pemilihan Jalur Tercepat Evakuasi Bencana Gunung Lokon Sulawesi Utara", Jurnal Teknologi Informasi-AITI, 2016, vol.13, no.2, pp 31-48
- [10]. L. Madeso, D. R. Kabo, J. R. Batmetan, "Rancang Bangun Sistem Pakar Penentuan Status Gizi Pada Balita Menggunakan Metode Forward Chaining", E-Jurnal UNSRIT, vol.2
- [11]. J. R. Batmetan, V. R. Palilingan, "Higher Education Students' Behaviour to Adopt Mobile Learning", IOP Conference Series: Materials Science and Engineering, 2018, vol. 306, Issue 1, pp. 012110 (2018)
- [12]. V. R. Palilingan, J. R. Batmetan, "Incident Management in Academic Information System using ITIL Framework", IOP Conference Series: Materials Science and Engineering, 2018, vol. 306, Issue 1, pp. 012110 (2018)
- [13]. J. R. Batmetan, A. J. Santoso, Pranowo, "A Multiple-Objective Ant Colony Algorithm for Optimizing Disaster Relief Logistics", Advanced Science Letters, 2017, vol.23, no.3, pp. 2344-2347
- [14]. M. L. Tompodung, F. Supit, J. R. Batmetan, "Rancang Bangun Aplikasi Sensus Penduduk Berbasis Android", Buletin Sariputra, 2017, vol.7, pp. 57-61
- [15]. J. R. Batmetan, "Optimasi Strategi Smart Environment Dalam Mitigasi Bencana Menggunakan Multi-Objective Aco (Mo-Aco) Algorithm", Pasca Sarjana Magister Teknik Informatika Universitas Atma Jaya Yogyakarta, 2016