ANALISIS DAN PERANCANGAN *SECURITY POLICY, PRIVILLAGE MANAGEMENT* MENGGUNAKAN *DOMAIN CONTROLLER ACTIVE DIRECTORY*

Ahmad Sa'di[1)], Melwin Syafrizal[2)]

[1)] PT. MSV PICTURES
[2)]STMIK AMIKOM YOGYAKARTA
Jl. Ring Road Utara Condong Catur Depok Sleman Yogyakarta
Email: [1]sandworks3@gmail.com[1)], melwin@amikom.ac.id[2)]

Abstrak

Data pembuatan film The Legend of Ajisaka yang dimiliki oleh PT. MSV PICTURES maupun data proyek-proyek film lain yang dikerjakan bersama-sama sesuai job description masing-masing departemen, di bagi dalam satu jaringan dan belum memiliki security policy untuk melindungi data-data tersebut. Belum ada access control terhadap karyawan atau user ketika mengoperasikan komputer, akses file atau terutama saat kirim file ke direktori PC sendiri atau server.

Pemanfaatkan Domain Controller Active Directory adalah upaya untuk membuat sebuah kebijakan agar optimalisasi security policy terhadap hak akses data berdasarkan departemen organisasi kerja, akan memberikan otoritas tinggi pada tiap Lead Departement, dan mengupayakan terciptanya kontrol dan prosedural ketika menggunakan komputer pada mode administrator.

***Kata kunci**: Security policy, Manajemen akses, Domain controller, Active Directory*

1. Pendahuluan

Data merupakan aset penting yang sangat berharga bagi kelangsungan hidup suatu organisasi atau bisnis[1]. Keamanan data secara tidak langsung dapat memastikan kontinuitas bisnis, mengurangi resiko, mengoptimalkan *return on investment* dan mencari kesempatan bisnis[2]. Semakin banyak informasi perusahaan yang disimpan, dikelola dan di-*sharing* maka semakin besar pula resiko terjadinya kerusakan atau hilangnya data[3].

Survei yang dilakukan oleh InfoWatch Analytical Center, menyebutkan, dari 410 perusahaan antara 2 Januari dan 2 Maret 2007 terjadi pencurian data sebesar (78%), ancaman yang terjadi dari pelanggaran keamanan internal maupun eksternal menghasilkan, (45%) terjadi di eksternal dan (55%) terjadi di interternal[4]. Hasil survei tersebut memperlihatkan bahwa pencurian data berada pada posisi pertama (78%) dan pelanggaran keamanan (ancaman) yang paling berisiko yaitu: dari faktor internal (55%).

Menanggulangi pencurian data dan serangan dari internal, diperlukan tindakan aturan dari *system* maupun prosedur dari manajemen supaya kejadian pencurian data dan serangan dari internal dapat ditangani[5].

Tujuan dari penelitian ini adalah memberikan solusi penerapan manajemen akses data, *security policy* terhadap user, memastikan bahwa dokumen hanya dapat diakses oleh pengguna yang berwenang dan user melakukan tindakan sesuai prosedurnya masing-masing. Penelitian ini menggunakan obyek studi kasus di PT. Mataram Surya Visi Pictures.

2. Pembahasan

Penelitian ini menggunakan dua metode: 1. Penelitian empiris (studi kasus, studi lapangan, dan studi laboratorium), dan 2. Penelitian analitis (memecahkan masalah yang ada guna mendapatkan solusi isu *security policy*).

Teknik pengumpulan data sbb:

1. Survei (dengan memeriksa kondisi dan kualitas hardware jaringan serta alur jaringan)
2. Analisa dan evaluasi implementasi share data antar departemen yang telah dilakukan.
3. Analisa dan evaluasi proses pembuatan film animasi dari *concept art* sampai dengan projek final.
4. Identifikasi dan evaluasi kemungkinan resiko yang mungkin muncul saat implementasi *security policy* dan hak akses terhadap data.
5. Studi literatur untuk mencari dan menemukan referensi yang benar dalam implementasi *security policy* hak akses terhadap data.
6. Dokumentasi

2.1 Analisis Masalah

Agar mendapatkan solusi yang tepat, perlu diadakan analisis masalah dari sistem yang berjalan saat ini.
Beberapa dari masalah-masalah tersebut :

1. **User dan Komputer Client**
   a. Belum ada tingkatan privillage user di setiap user computer .
   b. User tidak ada kendali dalam menginstall aplikasi, keadaan seperti ini dapat memicu terserang virus maupun malware.
   c. Interface network tidak ada control, keadaan ini memicu penggantian IP address dan terjadi

duplikasi IP address. Akibatnya diskonek terhadap akses jaringan.

d. Beberapa komputer tidak ada otoritas user logon ketika mengakses komputer.
e. Tidak ada kontrol mode administrator.

2. **Keadaan User Mengakses File ke Data Center**

Share folder yang diterjadi ditiap departemen belum ada otoritas file, artinya mempunyai hak akses satu sama lain sama. Misal, leader dan member departemen Production diizinkan melihat semua isi folder dari pekerjaannya tetapi yang berhak mendelete file hanya leader production, anggota hanya bisa *read* dan *write*. Departemen production otoritas terhadap file pekerjaan departemen lain hanya read atau list folder, tidak diizikankan mendelete file atau merubah file.

Idealnya Untuk para lead departemen mempunyai wewenang mendelete, memodifikasi file pekerjaan yang ada di directori kerja masing-masing departemen. Anggota dari tiap departemen hanya diperkenankan *read*, list folder dan diberikan izin merefisi perbaikan file kerjaannya. Departemen lain hanya bisa melihat file atau membaca file tetapi tidak diizinkan untuk memodifikasi.

3. **Observasi Jam Kerja**

Jam 09:00 - 18:00 WIB merupakan waktu jam kerja karyawan MSV Pictures yang berada di di gedung dua lantai dua STMIK AMIKOM Yogyakarta. Tetapi keadaan dilapangan, beberapa karyawan diruang tersebut lebih dari jam 18:00 WIB kadang sampai ditegur SATPAM. Entah sedang lembur, ber-internet, ataupun hanya sekedar bermain game. Belum ada pengaturan batasan mengakses server.

Keadaan seperti ini, diasumsikan memungkinkan adanya tindakan yang tidak diinginkan oleh pihak yang tidak bertanggung jawab. Seperti pencurian data, penggandaan data maupun pembocoran informasi data yang dimiliki oleh MSV Pictures kepada pihak luar akibat masih belum diterapkan kontrol waktu dalam mengakses server.

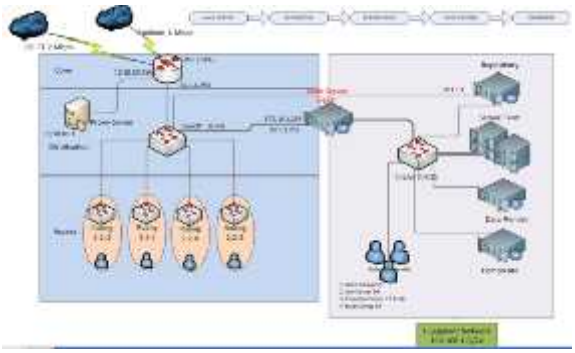
4. **Media Penyimpanan Portabel**

Port USB yang digunakan hanya tiga dari jumlah yang tersedia yaitu *input keyboard*, *mouse*, dan *digital drawing Wacom*. Perlu ada kebijakan *disable port* yang tidak digunakan, guna menghindari penggandaan data.

5. **Penggunaan CD/DVD**

Penggunaan CD/DVD ROM belum terkontrol oleh IT, kemungkinan besar *copy* data melalui CD/DVD dapat terjadi.

6. **Topologi Jaringan Internet dan Intranet**

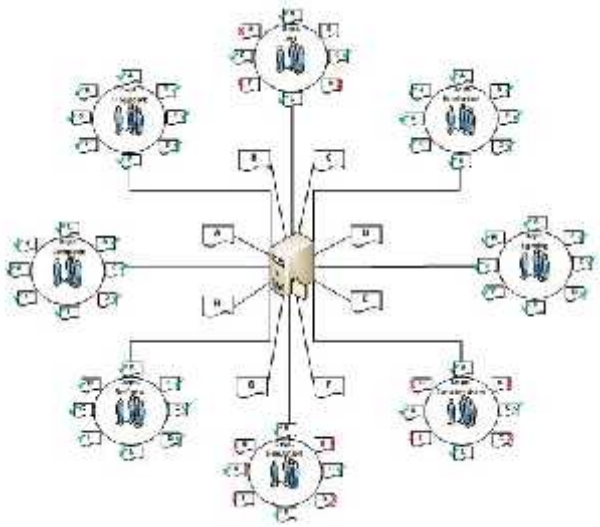


Gambar 1. *Topology Network*

Informasi yang dapat dari leader IT Support bahwa router mikrotik yang tersambung ke internet belum ada pemasangan security. Setelah dilakukan pemeriksaan ke router Mikrotik, keadaan akses mikrotik via FTP, SSH, TELNET keadaan *default*. Service yang tidak perlu semua masih aktif. Padahal yang dipakai hanya SSH. Setting masih default, artinya port SSH (22) dan semua IP boleh mengakses. Semua IP lokal maupun dari luar mempunyai peluang untuk masuk, karena belum ada pengaturan, seperti: hanya IP tertentu yang diizinkan mengakses router Mikrotik.

2.2 Solusi

Administrator jaringan menerapkan sistem *avaibility* supaya menjamin bahwa data akan tersedia saat dibutuhkan. Seperti gambar dibawah ini:

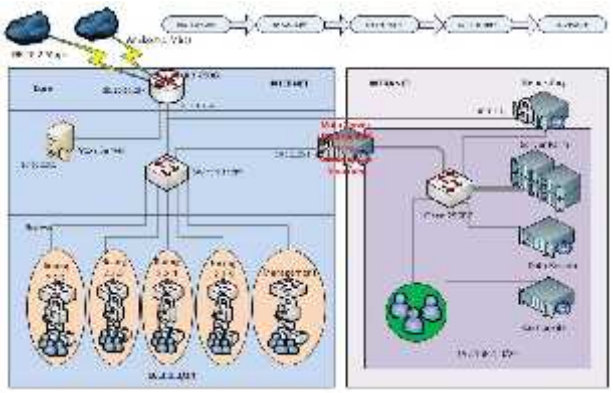


Gambar 2. *Solusi Privillage Management*

Memastikan user yang berhak atau user yang diotorisasi dapat menggunakan informasi dan perangkat terkait. Misal Dept. asset hanya boleh melihat data yang dimiliki Dept. *Concept Art*, sesama departemen *Concept Art*, hanya *Leader*-nya yang diizinkan men-*delete* data. dijamin kerahasiaannya dan integritas sebuah data.

Semua perangkat server dan komputer yang dipakai oleh karyawan, penggunaanya diotentikasi. *Domain Active Directory* berperan melakukan otentikasi dan menjaga *policy* yang telah diberikan setiap user dalam

menggunakan data, komputer, dan *device* yang telah di akomodir oleh domain.

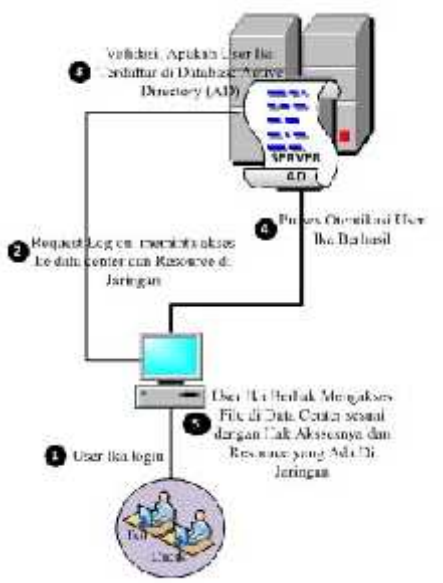


Gambar 3. *Solusi Otentikasi dan Central security policy*

2.2.1 Perancangan Sistem

Perancangan sistem yaitu berupa prosedur-prosedure control user maupun komputer terhadap resource yang ada di data center dan resource yang ada dijaringan. Agar *security policy* dapat berjalan dengan baik dan tidak terjadi hal-hal yang merugikan bagi PT. Mataran Surya Visi Pictures.

1. **Prosedur Implementasi *Active Directory***
    a. Pastikan preverred DNS server address menggunakan IP server *active directory*.
    b. Ubah komputer yang ingin bergabung ke *active directory* dari "WORKGROUP" ke "DOMAIN" (msv.com).
    c. Pastikan komputer direstart untuk kesempurnaan sebagai anggota *domain active directory*.
    d. Pastikan client yang telah tergabung dengan *Active Directory* "*User Control Account Setting* (UAC)" disetting "*Always notify*" yang direkomendasikan oleh windows
    e. User administrator lokal beserta passwordnya yang berhak memiliki hanya staf IT.
    f. Staf IT harus punya dokumentasi account administrator lokal dan account user active directory untuk mempermudah jikalau terjadi lupa terhadap account.
    g. Proses otentikasi User AD terhadap Resource di Jaringan



Gambar 4. *Proses otentikasi user AD*

Keterangan:
1. User Ika melakukan *login* di komputernya.
2. *Request Log On*, meminta akses ke Data Center dan resource yanf ada dijaringan.
3. Validasi, apakah user Ika ada di database sever Active Directory.
4. Jika ada maka proses login berhasil, jika tidak maka akan ditolak.
5. User ika berhak menggunakan resorce yang ada dijaringan dan file yang ada di data center berserta hak akses yang melekat di user Ika.

Proses tersebut juga berlaku untuk semua user yang ada seperti Didik, Ika dan yang lain.

2. **Perancangan Keamanan Informasi Berdasarkan CIA**

Komponen-komponen *Informasion Security*

a. Confidentiality
    1. Folder kerja Manager, aset proyek film animasi bersifat privasi, dipastikan kerahasiann data. Yaitu dengan menerapkan share dan security permission dan owner file.
    2. Semua account bersifat rahasia, tidak diperbolehkan memberitahu atau memberikan account kepada user yang tidak mempunyai otoritas.
    3. Dipberlakukan penggantian password berkala dengan menerapkan batas waktu password.

b. Integrity
    1. Data final, hasil pekerjaan tiap departemen hanya lead departemen yang diperbolehkan memodify, memindahkan ataupun mendelete. Penerapannya dapat dilakukan di share permission dan security permission.

2. IP address tiap komputer tidak boleh dirubah, hal ini untuk menghindari konflik ip addres, dan tidak konsistennya manajemen banwidth di router.
3. Tidak ada perubahan aplikasi baik penambahan maupun pengurangan. Hal tersebut harus terkontrol oleh IT support.

c. Avaibility

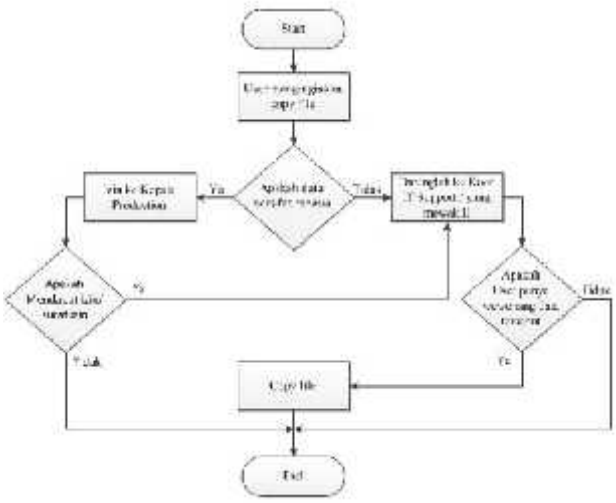
1. Data tersedia hanya untuk member atau group dan diberikan otoritas.
2. Hak akses dan security permission tetap sasaran pada user yang diberi otoritas.
3. Mengakses server ataupun meremote resource yang ada dijaringan seperti router, remote komputer, dipastikan orang-orang tertentu dengan menerapkan avaibility IP atau user account yang diperbolehkan akses.

3. **Perancangan jaringan**

1. Router yang menghubungkan jaringan LAN dan Internet harus menerapkan *firewall*.
2. Menutup *port* maupun *service* yang tidak perlu dan hanya IP tertentu yang dapat mengakses router mikrotik.
3. *Security management*, digunakan untuk mengawasi dan mengontrol jaringan

4. ***Policy User* Terhadap Data**

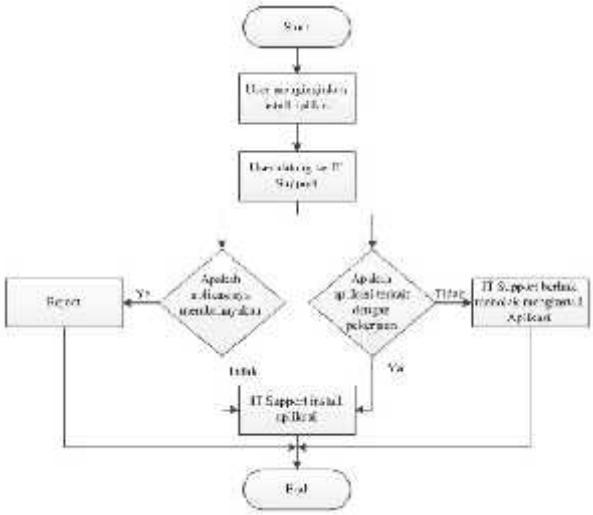
1. Data yang tersimpan di server, pendistribusiannya tepat sasaran kepada user yang berhak atau yang diberi otoritas.
2. Dilarang memindahkan, men-transfer, mem-foto copy, atau menyalin data yang ada di dalam *server data center* untuk kepentingan yang tidak berhubungan dengan pekerjaan.
3. Dilarang membocorkan dalam bentuk apapun data yang dimiliki MSV Pictures.
4. Transfer data dari dan ke dalam perangkat dan fasilitas pengolahan data dan informasi perusahaan dengan menggunakan removable media hanya boleh dilakukan oleh IT support.
5. Kerahasiaan data harus dijaga oleh setiap karyawan yang diberikan akses, dilarang meletakkan *username* dan *password* aplikasi yang penting secara sembarangan (misalnya catatan ditempel pada monitor).



Gambar 5. *Prosedure copy file*

5. **Prosedure Install Aplikasi**

1. IT support menginventarisir kebutuhan software yang digunakan disetiap departemen untuk keperluan kerja saja.
2. User tidak berhak menginstall aplikasi apapun dikomputer sendiri maupun dikomputer rekan kerja
3. User yang menginginkan tambahan aplikasi harap datang ke IT support.
4. IT Support berhak menolak menginstallkan aplikasi jikalau aplikasi tersebut tidak berhubungan dengan kerja atau karena membahayakan bagikomputer sendiri maupun komputer yang ada di jaringan.

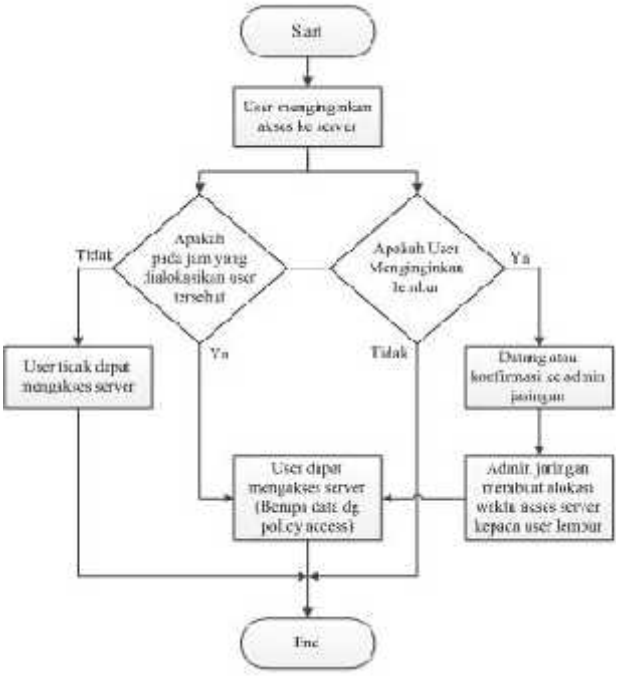


Gambar 6. *Prosedur install aplikasi*

6. ***Connection Policy***

1. Setiap user dapat mengakses internet dan memiliki batasan bandwidth untuk akses internet pada jam kerja (09.00-17.00 wib)
2. Semua user dilarang mengakases website porno atau website underground.

3. User men-download file, bandwidth dibatasi, bila ingin mendownload file dengan ukuran besar datanglah ke Admin jaringan.
4. Server datacenter dan server repository hanya dapat diakses pada jam kerja yaitu dari jam 09.00 sampai dengan 18.00.
5. Bila user kerja lembur dan ingin terkoneksi dengan data center user harap lapor atau konfirmasi kepada admin jaringan atau IT support, agar akses ke server dibukakan oleh admin.



Gambar 7. *Prosedure akses server terhadap alokasi waktu*

7. **Prosedur komputer client & Penggunaanya**

1. Port USB yang tidak terpakai harus di-*disable*. Perangkat yang telah terpasang di lem tembak, agar user tidak memanfaatkan untuk kepentingan *copy* file.
2. User tidak punya otoritas mengganti IP address. Hak penuh dimiliki oleh administrator jaringan MSV Pictures.
3. User tidak diperkenankan menyimpan data pekerjaanya di drive C:\
4. *Trouble* hardware maupun software segera lapor ke IT support dapat melalui *chatting* lokal maupun datang langsung ke ruang IT support.
5. Komputer jika ditinggal pergi harus dilakukan log out

8. **Keamanan dan kerahasiaan *username* dan *password***

1. Seluruh karyawan harus menjaga kerahasiaan username dan password miliknya atau milik orang lain yang dipercayakan kepadanya.
2. *Username* dan *password* masing-masing karyawan tidak diperkenankan diberitahukan kepada siapapun yang tidak berkepentingan, kecuali mendapat ijin dari atasan.
3. *Password* harus diganti secara berkala oleh user.

9. **Kebijakan Management Backup Data**

Kebijakan ini mengatur hal-hal yang harus dilakukan dalam melakukan backup data bagi karyawan MSV Pictures yang berkepentingan dan dijalankan secara terjadwal atau sesuai kebutuhan. Diantara kebijakan tersebut adalah:

1. Proses backup hanya dilakukan oleh leader IT support.
2. Proses Restore hanya boleh dilakukan apabila terjadi masalah pada data asli atau keadaan sedang dibutuhkan.
3. Memastikan proses backup atau restore telah berjalan baik dan berhasil.
4. Seluruh backup harus disimpan di tempat yang aman.

2.2.2 Implementasi

Penerapan *Domain Controler Active Directory* di sistem jaringan dapat berjalan dengan baik, melakukan otentikasi dan menjaga policy, akses control kepada user dalam menggunakan data dan komputer yang dipakai.

Uji Security dan Authorization Folder and File

Share dan *security permission* data perlu dilakukan, guna menetapkan siapa yang berhak dan tidak berhak terhadap data. Dan seberapa berhak user menggunakan data pada ruang lingkup kerjanya.Artinya hal tersebut menerapkan bagian dari elemen kemanan informasi yaitu *Convidentiality*, *Integrity* dan *Availability*.

Tabel 1. *Hasil yang diharapkan*

No	Nama Pengujian	Tujuan	Skenario	Hasil Yang Diharapkan	Kepada
1	Menguji [illegible]	Pendistribusian data [illegible]	Menetapkan *Share Permission* dan *Security permission*	Dapat Paste, Save dan Dapat Delete Pekerjaan di Folder Kerja"	User Departemen
2	Menguji [illegible]	Pendistribusian data [illegible]	Menetapkan *Share Permission* dan *Security permission*	Dapat Paste, Save, Edit Pekerjaanya tetapi tidak diizinkan delete Pekerjaan di Folder Kerja	Member Departemen
3	Menguji [illegible]	Pendistribusian data [illegible]	Menetapkan *Share Permission* dan *Security permission*	[illegible]	User Unauthorized Atau Others Departemen
4	Menguji [illegible]	Pendistribusian data [illegible]	Menetapkan *Share Permission* dan *Security permission*	Datang Menyalin Mendelete, Drag Folder [illegible]	User Unauthorized Atau Others Departemen
5	Menguji [illegible]	Pendistribusian data [illegible]	Menetapkan *Share Permission* dan *Security permission*	Ditemkan Melihat Isi Folder Tetapi Un authorized [illegible]	User Unauthorized Atau Others Departemen
6	Menguji [illegible]	Pendistribusian data [illegible]	Menetapkan *Share Permission* dan *Security permission*	Departemen [illegible] mengakses data, Un authorized Datang Mem[illegible]	Departemen [illegible] dan Departemen Lainnya

Tabel 2. *Penetapan Security permission secara teknis*

Folder	Akses Permission	Kepada
Drive D:\	Full Control	Administrator (MSV Administrator)
Data Asset2	Read/Write	Domain Users (MSV Domain users) atau Seluruh Departemen MSV
CGI	Read/Write	Administrator & Domain User (MSV Domain users) atau seluruh Organisasi MSV
Asset	Read+Write	Administrator & Domain User (MSV Domain users) atau seluruh Organisasi MSV
Character	R+W+X+C	Lead Character ([illegible]@msv.com)
	R+W+X	Member Character
[illegible]	R+W+X+C	Lead Character ([illegible]@msv.com)
	R+W+X	Member Character
[illegible]	R+W+X+C	Lead Character ([illegible]@msv.com)
	R+W+X	Member Character
[illegible]	R+W+X+C	Lead Character ([illegible]@msv.com)
	R+W+X	Member Character
Creatures Animals	R+W+X+C	Lead Character ([illegible]@msv.com)
	R+W+X	Member Character

Tabel 3. *Hasil Setelah Implementasi Sistem*

No	Entitas Obyek Observasi	Kondisi	
		Terpenuhi	Tidak Terpenuhi
1	Tingkatan privilege user	X	
2	Kontrol mode administrator	X	
3	Otentikasi user logon ketika mengakses server Data Center	X	
4	Kendali menginstall aplikasi	X	
5	Kontrol interface dan IP address network	X	
6	Otentikasi user logon ketika mengakses komputer user	X	
7	Otoritas hak akses terhadap file share/direktori di Data Center	X	
8	Manajemen Service server (FTP, SSH, TELNET, WWW) dan Manajemen IP [illegible]	X	
9	Sistem backup data	X	
10	Manajemen [illegible]	X	
11	Pengendalian penggunaan [illegible]	X	
12	Batasan waktu mengakses data di server Data Center	X	

3. Kesimpulan

Administrator jaringan dalam mengelola obyek-obyek yang ada dapat dimanajemen secara terpusat dengan cara menjadikan komputer workgroup menjadi satu domain. dengan satu domain dengan server *Domain Controller Active*

Group policy Active Directory Domain Services dapat dimanfaatkan untuk mengoptimalkan *security policy* terhadap hak akses data berdasarkan departemen masing-masing

Saran untuk sistem *Domain Controller Active Directory* akan lebih baik jika dilakukan penambahan server backup atau replikasi main server active directory, untuk menjaga kestabilan proses otentikasi user dan ketersediaan database server *Active Directory*. Dan perlu didukung adanya SOP kerja karyawan.

Daftar Pustaka

[1] R. von Solms, “Information security management: why standards are important,” *Inf. Manag. Comput. Secur.*, vol. 7, no. 1, pp. 50–58, Mar. 1999.

[2] B. McQuaide, “Identity and Access Management,” *Inf. Syst. Control J.*, vol. 4, pp. 35–38, 2003.

[3] W. Zeng, S. E. Parkin, and A. van Moorsel, “Digital Rights Management,” Technical Report: CS-TR-1223, School of Computing Science, Newcastle University, 2010.

[4] D. A. Akopyan and A. D. Yelyakov, “Cybercrimes in the information structure of society: a survey,” *Sci. Tech. Inf. Process.*, vol. 36, no. 6, pp. 338–350, 2009.

[5] F. Farahmand, “Developing a Risk Management System for Information Systems Security Incidents,” Georgia Institute of Technology, 2004.

Biodata Penulis

Ahmad Sa’di, memperoleh gelar Sarjana Komputer (S.Kom), Jurusan Teknik Informatika STMIK AMIKOM Yogyakarta, lulus tahun 2013.
Saat ini menjadi Staf di PT. MSV Pictures Yogyakarta sebagai Administrator Jaringan Komputer.

Melwin Syafrizal, memperoleh gelar Sarjana Komputer (S.Kom), Jurusan Teknik Informatika STMIK AMIKOM Yogyakarta, lulus tahun 2004. Memperoleh gelar Master of Engineering (M.Eng.) Program Pasca Sarjana Magister Teknik Informatika Universitas Gajah Mada Yogyakarta, lulus tahun 2009.
Saat ini menjadi Dosen di STMIK AMIKOM Yogyakarta.