POLISI KESELAMATAN RANGKAIAN

PEJABAT PENGARAH TANAH DAN GALIAN WILAYAH PERSEKUTUAN

1 JANUARI 2020

KANDUNGAN

Kandungan Dokumen

SEJARAH DOKUMEN

Tarikh Semakan Semula	Versi	Kelulusan	Tarikh Kuat Kuasa
-	1.0	Mesyuarat JPICT Bil 2/2014	1 Julai 2014
17 November 2018	2.0	Mesyuarat JPICT Bil 3/2019	

JADUAL PINDAAN POLISI KESELAMATAN RANGKAIAN

Tarikh	Versi	Butiran Pindaan
17 November 2018	1.0	i. **Capaian Logikal:** muka surat 5, pindaan ayat perenggan: iv. Maklumat capaian ke *server* peralatan rangkaian hendaklah direkodkan - pegawai, tarikh, masa dan aktiviti. Maklumat mestilah disimpan dan diarkibkan mengikut tempoh masa yang bersesuaian; ii. **Capaian Logikal:** muka surat 5, pindaan ayat perenggan: vi. Perubahan konfigurasi perisian mestilah direkodkan dan perlu mengisi borang permohonan dengan mendapatkan kebenaran daripada Pentadbir Rangkaian; iii. **Penyelenggaraan Peralatan:** muka surat 6, pindaan ayat perenggan: i. Memaklumkan pengguna sebelum melaksanakan penyelenggaraan; iv. **Rangkaian Setempat(*Local Area Network*):** muka surat 6, pindaan ayat perenggan: i. Penyambungan ke rangkaian PPTGWP hanya terhad kepada warga PPTG WP dan pembekal yang dibenarkan sahaja; v. **Integrasi Aplikasi Agensi Luar:** muka surat 7, pindaan ayat perenggan: ii. Pelaksanaan integrasi dengan agensi luar perlu mendapatkan kebenaran jabatan; vi. **PEMATUHAN POLISI:** muka surat 8, pindaan ayat perenggan petama: Polisi ini terguna pakai oleh keseluruhan penggunaan aset ICT di PPTGWP. Tiada pengecualian diberikan kepada sesiapapun. Kakitangan PPTGWP yang tetap, sementara, kontrak, agensi atau jabatan terlibat serta pembekal adalah terikat dengan dasar ini. Dasar ini turut terpakai kepada kakitangan yang bekerja secara jauh(*remote*). Polisi ini turut perlu dibaca bersama-sama dengan arahan/pekeliling dari semasa ke semasa;

1. PENGENALAN

1.1. Tujuan

Polisi ini bertujuan untuk menerangkan perlaksanaan keselamatan rangkaian PPTG WP yang merupakan infrastruktur rangkaian setempat (LAN) untuk penyambungan di antara workstation bagi tujuan komunikasi dan perkongsian maklumat/sumber.

1.2. Skop

i. Reka bentuk Keselamatan Rangkaian

Melibatkan reka bentuk keselamatan rangkaian yang mengambi kira perkara-perkara berikut:

a) Matlamat, objektif dan skop keselamatan (sama ada meliputi *end-to-end security, inter-network security* atau keselamatan pada tahap sistem dalaman sahaja);
b) Aset-aset yang perlu dilindungi termasuk jenis-jenis maklumat dan tahap keselamatan yang diperlukan; dan
c) Potensi ancaman dan serangan(*vulnerabilities*) serta mewujudkan sistem pencegahan, polisi dan prosedur untuk melindungi maklumat serta integriti rangkaian.

ii. Kawalan Keselamatan Rangkaian

Kawalan yang sewajarnya hendaklah diwujudkan untuk memastikan keselamatan data dalam rangkaian daripada ancaman dalaman dan luaran serta melindunginya daripada capaian tanpa kebenaran.

2. KESELAMATAN PERALATAN RANGKAIAN

2.1. Keselamatan Fizikal

i. Peralatan rangkaian ditempatkan di tempat yang bebas daripada risiko di luar jangkaan seperti banjir, gegaran, kekotoran dan sebagainya;
ii. Suhu hendaklah terkawal dalam had suhu operasi peralatan rangkaian berkenaan;
iii. Memasang Uninterruptible Power Supply (UPS) dengan minimum 15 minit masa beroperasi tunggu sedia jika terputus bekalan elektrik;
iv. Bekalan Kuasa UPS hendaklah disambungkan kepada punca bekalan kuasa Generator Set(*Genset*) bangunan sekiranya ada. Perkara ini akan mengurangkan risiko peralatan rangkaian rosak apabila tempoh bekalan kuasa terputus melebihi 15 minit atau pada luar waktu bekerja; dan
v. Semua peralatan sokongan bekalan kuasa hendaklah disemak dan diuji secara berkala.

2.2. Capaian Fizikal

i. Capaian Pengkabelan Rangkaian

Langkah-langkah yang perlu diambil untuk melindungi kabel rangkaian daripada di capai oleh orang yang tidak berkenaan :

a) Melindungi pengkabelan di dalam kawasan awam dengan cara memasang pembuluh(*conduit*) atau lain-lain mekanisma perlindungan;
b) Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat; dan

c) Pusat pendawaian terletak dalam ruang atau bilik yang berkunci dan hanya boleh dicapai oleh kakitangan yang dibenarkan sahaja.

ii. Capaian Peralatan Rangkaian

a) Peralatan hendaklah ditempatkan di tempat yang selamat dan terkawal;
b) Peralatan rangkaian terletak dalam ruang atau bilik yang berkunci dan hanya boleh dicapai oleh kakitangan yang dibenarkan sahaja; dan
c) Peralatan perlu dilabelkan dengan jelas.

2.3. Capaian Logikal

i. ID dan kata laluan diperlukan untuk mencapai perisian rangkaian. Capaian hanya boleh dibuat oleh kakitangan yang dibenarkan sahaja;
ii. ID capaian kakitangan ke atas perisian rangkaian hendaklah diklasifikasikan mengikut peranan;
iii. Komposisi kata laluan mestilah konsisten dengan garis panduan yang telah ditetapkan;
iv. Maklumat capaian ke server peralatan rangkaian hendaklah direkodkan - pegawai, tarikh, masa dan aktiviti. Maklumat mestilah disimpan dan diarkibkan mengikut tempoh masa yang bersesuaian;
v. Rangkaian hanya menerima trafik daripada alamat IP dalaman yang berdaftar sahaja;
vi. Perubahan konfigurasi perisian mestilah direkodkan dan perlu mengisi borang permohonan dengan mendapatkan kebenaran daripada Pentadbir Rangkaian;
vii. Perubahan konfigurasi hendaklah dikendalikan secara berpusat; dan
viii. Seorang pentadbir sistem rangkaian hendaklah dilantik untuk mengawasi semua capaian dan konfigurasi rangkaian dari semasa ke semasa.

2.4. Penggunaan Peralatan Tanpa Kebenaran.

Penggunaan peralatan rangkaian tanpa kebenaran boleh dikawal dengan :-

i. Mengadakan kawalan capaian logikal seperti yang disebutkan di para 2.2;
ii. Menempatkan peralatan di tempat yang selamat;
iii. Bilik pendawaian atau *wiring closet* hanya boleh dicapai oleh kakitangan yang dibenarkan sahaja; dan
iv. Menyelenggara inventori peralatan dan membuat semakan secara berkala.

2.5. Konfigurasi Peralatan

Peralatan di konfigurasi dengan betul dengan mengambil langkah-langkah berikut:-

i. Mengaktifkan perkhidmatan yang diperlukan sahaja;
ii. Capaian untuk konfigurasi dihadkan melalui nod atau alamat IP yang dibenarkan sahaja;
iii. Menggunakan kata laluan yang selamat; dan
iv. Dilaksanakan oleh kakitangan yang terlatih dan dibenarkan sahaja.

2.6. Penyelenggaraan Peralatan

i. Memaklumkan pengguna sebelum melaksanakan penyelenggaraan; mengikut jadual yang ditetapkan atau mengikut keperluan.
ii. Peralatan hendaklah diselenggarakan secara berkala;
iii. Mempunyai rekod penyelenggaraan; dan

iv. Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan.

3. KEBOLEHCAPAIAN PENGGUNA(*USER ACCESSIBILITY*)

3.1. Rangkaian Setempat(*Local Area Network*)

i. Penyambungan ke rangkaian PPTGWP hanya terhad kepada warga PPTG WP dan pembekal yang dibenarkan sahaja;
ii. Hanya komputer kepunyaan PPTGWP yang dibenarkan untuk disambungkan ke rangkaian;
iii. Pengguna luar perlu mendapatkan kebenaran daripada Bahagian Pengurusan Maklumat sebelum membuat capaian ke rangkaian PPTGWP;
iv. Setiap perkakasan atau peranti luar yang ingin berhubung ke dalam rangkaian PPTGWP perlu mematuhi perkara-perkara berikut:-
    a) Mempunyai antivirus yang *updated* dan terkini
    b) Memastikan peralatan telah dilengkapi dengan *patches* sistem operasi yang terkini
v. Perisian pengintip(*sniffer*) atau penganalisis rangkaian(*network analyser*) tidak di benar digunakan pada semua komputer;
vi. Memasang perisian Instrution *Preventive System* (IPS) bagi mengesan sebarang cubaan menceroboh atau aktiviti-aktiviti klain yang boleh mengancam sistem dan maklumat PPTGWP;
vii. Memasang *Web Content Filtering* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang; dan
viii. Penggunaan teknologi *Packet Shaper* untuk mengawal aktiviti (*video conferencing, video streaming, chat, downloading*) untuk menguruskan penggunaan jalur lebar*(bandwidth)* yang maksimum dan lebih berkesan.

4. SAMBUNGAN DENGAN LAIN-LAIN RANGKAIAN

4.1. Capaian Yang Tidak Digalakkan

i. Capaian secara *remote* perlu mendapat kebenaran dari Pentadbir Rangkaian PPTGWP.

4.2. '*Firewall*'

i. Semua aliran trafik (multimedia dan data) dari dalam ke luar PPTG WP dan sebaliknya mestilah melalui *firewall;*
ii. Hanya trafik yang disahkan sahaja dibenarkan untuk melepasinya berasaskan kepada Dasar Keselamatan ICT PPTG WP;
iii. Reka bentuk *firewall* hendaklah mengambil kira perkara-perkara berikut:
    a) Keperluan audit dan arkib;
    b) Kebolehsediaan;
    c) Kerahsiaan; dan
    d) Melindungi maklumat PPTGWP.

4.3. Integrasi Aplikasi Agensi Luar

i. Semua integrasi aplikasi PPTGWP hendaklah menggunakan perkhidmatan *web service* dan kaedah SFTP; dan

ii. Pelaksanaan integrasi dengan agensi luar perlu mendapatkan kebenaran jabatan.

5. PEMATUHAN POLISI

Polisi ini terguna pakai oleh keseluruhan penggunaan aset ICT di PPTGWP. Tiada pengecualian diberikan kepada sesiapapun. Kakitangan PPTGWP yang tetap, sementara, kontrak, agensi atau jabatan terlibat serta pembekal adalah terikat dengan dasar ini. Dasar ini turut terpakai kepada kakitangan yang bekerja secara jauh(*remote*). Polisi ini turut perlu dibaca bersama-sama dengan arahan/pekeliling dari semasa ke semasa. Dalam keadaan-keadaan tertentu yang seperti dihuraikan pada mana-mana pernyataan dasar, pihak ketiga perlu menghormati segala penyataan yang terdapat di dalam dasar sedia ada.