POLISI KAWALAN CAPAIAN LOGIKAL DAN KESELAMATAN KATA LALUAN

PEJABAT PENGARAH TANAH DAN GALIAN WILAYAH PERSEKUTUAN

1 JANUARI 2020

POLISI KAWALAN CAPAIAN LOGIKAL DAN KESELAMATAN KATA LALUAN

KANDUNGAN

Kandungan Dokumen

SEJARAH DOKUMEN

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

JADUAL PINDAAN POLISI KAWALAN CAPAIAN LOGIKAL DAN KESELAMATAN KATA LALUAN

Tarikh	Versi	Butiran Pindaan
17 November 2018	1.0	i. **Pengenalan:** muka surat 4, pindaan mengugurkan perkataan adalah perenggan dua: Kata laluan adalah merupakan kata kunci yang menjadi hak individu dan menjadi rahsia dari pengetahuan orang lain. Oleh itu pengguna adalah dinasihatkan menjaga kata laluan masing-masing dengan teliti agar tidak dicerobohi oleh pengguna lain. ii. **Perlindungan Kata Laluan:** muka surat 5, pindaaan perenggan: b) Kata laluan hendaklah dihafal dan jangan disalin atau dipapar di mana-mana media seperti buku catatan, peralatan mudah alih, *USB drive* dan sebagainya kerana dikhuatiri akan diketahui dan disalahgunakan oleh orang lain. Jika kata laluan perlu didokumenkan, pastikan ianya disampulkan dan dilakrikan(*seal*). Dokumen tersebut hendaklah diserahkan kepada CIO untuk disimpan di lokasi yang selamat. iii. **Perlindungan Kata Laluan:** muka surat 5, pindaaan perenggan: c) Gunakan kata laluan yang kukuh*(strong)* melalui kombinasi abjad, simbol dan nombor (*alphanumeric characters*) dan mempunyai sekurang-kurangnya dua belas (12) aksara sebagai contoh P@ssw0rd1234. Jangan menggunakan kata laluan yang mudah diteka seperti nama, nombor telefon, tarikh lahir, perkataan atau nombor-nombor umum. iv. **Perlindungan Kata Laluan:** muka surat 5, pindaaan perenggan: d) Pengguna tidak boleh menggunakan semula empat (4) kata laluan yang terdahulu dan digalakkan menukar kata laluan sekurang kurangnya:- i) Tiga (3) bulan sekali bagi pengguna aplikasi dan *login* komputer; atau ii) Satu (1) tahun sekali bagi sistem operasi atau pangkalan data (cth : Oracle, PHP, mySQL, MSSQL dll). v. **Perlindungan Kata Laluan:** muka surat 5, pindaaan perenggan: e) Kata laluan mesti ditukar dalam keadaan berikut: iii. Apabila ID dan kata laluan disyaki telah dicerobohi; atau vi. **Perlindungan Kata Laluan:** muka surat 5, pindaaan perenggan: h) Kata laluan tidak boleh mengguna abjad yang sama(*repeating characters*); vii. **Perlindungan Kata Laluan:** muka surat 5, pindaaan perenggan: k) Sekiranya kata laluan telah dicerobohi atau disyaki dicerobohi, pengguna hendaklah melaporkan kepada CERT

		PPTGWP melalui emel ke certptgwp@ptgwp.gov.my dengan serta merta; dan viii. **Perlindungan Kata Laluan:** muka surat 5, pindaaan perenggan: l) Dilarang menyimpan katalaluan secara *autosaved mode*. ix. **Pengurusan ID dan Hak Capaian Logikal:** muka surat 5, pindaaan perenggan: b) Pentadbir Sistem akan mengemukakan dua (2) borang akuan penerimaan ID untuk disahkan. Satu (1) untuk simpanan pengguna dan satu salinan lagi untuk simpanan dan rujukan Bahagian Pengurusan Maklumat. Pengguna dikehendaki mematuhi arahan-arahan yang tercatat dalam borang akaun penerimaan ID tersebut. Bagi sistem dan aplikasi yang menggunakan notifikasi emel, penerimaan ID dan kata laluan akan dihantar melalui emel. x. **Pengurusan ID dan Hak Capaian Logikal:** muka surat 5, pindaaan perenggan: c) Pengguna mesti memaklumkan kepada Pentadbir Sistem dengan mengemukakan borang pengemaskinian atau pembatalan ID sekiranya mereka bertukar kerja atau berubah bidang tugas; xi. **Pengurusan ID dan Hak Capaian Logikal:** muka surat 5, pindaaan perenggan: f) Untuk sistem dan aplikasi, hak capaian untuk mengubah data dalam pangkalan data secara terus (*direct*) adalah tidak dibenarkan kecuali kemudahan tersebut tidak disediakan melalui sistem atau aplikasi terlibat; dan xii. **Pembatalan ID dan Hak Capaian:** muka surat 5, pindaaan perenggan: c) Pemilikan ID bukan hak mutlak seseorang kerana ianya tertakhluk kepada peraturan Jabatan dan boleh ditarik balik sekiranya penggunaannya melanggar peraturan; dan xiii. **Pembatalan ID dan Hak Capaian:** muka surat 5, pindaaan perenggan: d) Pentadbir sistem boleh membeku dan menamatkan akaun pengguna atas sebab-sebab berikut: i. ID bagi Kakitangan bertukar jabatan, berhenti atau bersara sepatutnya ditamatkan selepas empat belas (14) hari atau selepas menerima borang penamatan ID. ii. ID bagi Kakitangan diberhentikan atas sebab-sebab tatatertib atau melanggar dasar/polisi Jabatan ditamatkan serta merta; atau iii. ID bagi Kakitangan yang berada dalam siasatan pihak berkuasa harus dibekukan sementara sehingga kes selesai. xiv. **Jejak Audit(*Audit Trails*):** muka surat 5, pindaaan perenggan: b) Pentadbir Sistem hendaklah menyemak maklumat jejak audit secara berkala atau harian untuk memastikan kegunaan sistem adalah teratur dan tidak ada unsur-unsur mencurigakan.

		Sekiranya ada, Pentadbir Sistem hendaklah membuat siasatan segera dan melaporkannya kepada CERT PPTGWP. Di antara perkara yang perlu diperhatikan adalah; i. Kegagalan atau cubaan memasuki bahagian-bahagian sistem atau aplikasi yang di luar hak capaian pengguna berkenaan; ii. Penggunaan ID kritikal dimana tahap capaian dan kebolehannya tanpa had. (contoh : *super user*) ; iii. Corak penggunaan sistem yang luar biasa (contoh : luar dari waktu pejabat atau waktu kerja yang dibenarkan); iv. Perubahan kepada profil keselamatan (*security profile*); xv. **Jejak Audit(*Audit Trails*):** muka surat 5, pindaaan perenggan: Pentadbir Sistem hendaklah melindungi maklumat jejak audit daripada dihapus, diubahsuai, dipalsukan(*fabricate*) atau dibuat penyusunan semula dengan menggunakan *Machine Access Control* (MAC) atau tanda tangan digital(*digital signature*). xvi. **Jejak Audit(*Audit Trails*):** muka surat 5, pindaaan perenggan: Aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya. xvii. **Jejak Audit(*Audit Trails*):** muka surat 5, pindaaan perenggan: Merekodkan maklumat jejak audit sebanyak mungkin dan praktikal untuk digunakan bagi tujuan penyiasatan. Antaranya adalah : i. ID pengguna; ii. Fungsi, sumber dan maklumat yang digunakan atau diubah; iii. Tarikh dan masa(*time stamp*); iv. Alamat komputer (nama dan IP termasuk MAC IP) dan maklumat laluan rangkaian(*network path*); dan v. Transaksi atau program yang dilaksanakan.

POLISI KAWALAN CAPAIAN LOGIKAL DAN KESELAMATAN KATA LALUAN

1. PENGENALAN

1.1. Tujuan

Kawalan capaian logikal bertujuan mengawal capaian ke atas maklumat, kemudahan- kemudahan proses maklumat, dan proses perkhidmatan berdasarkan keperluan perkhidmatan dan keperluan keselamatan. Peraturan kawalan capaian hendaklah mengambil kira penyebaran dan pengesahan maklumat.

Kata laluan merupakan kata kunci yang menjadi hak individu dan menjadi rahsia dari pengetahuan orang lain. Oleh itu pengguna dinasihatkan menjaga kata laluan masing-masing dengan teliti agar tidak dicerobohi oleh pengguna lain.

1.2. Skop

Untuk menguatkuasakan pengasingan tugas dan memastikan individu yang diberi tanggungjawab mempunyai akauntabiliti ke atas akses untuk melaksanakan fungsi tersebut. Ia perlu direkodkan dan dikemas kini.

2. PENYATAAN POLISI

2.1. Capaian kepada proses dan maklumat melalui aplikasi atau sistem dan kemudahan yang berkaitan hendaklah dikawal mengikut keperluan keselamatan, perundangan dan fungsi kerja pengguna bagi melindungi data dan perkhidmatan;

2.2. Pengguna yang diberi hak capaian hendaklah memastikan mereka menggunakan hak dan tanggungjawab yang dibenarkan sahaja; dan

2.3. Pengguna mesti melaporkan kepada Bahagian Pengurusan Maklumat apabila berlaku perubahan kepada fungsi kerja.

3. PENGURUSAN KAWALAN CAPAIAN

3.1. Pengguna sistem ICT boleh menjadi sebagai individu atau sekumpulan pengguna yang berkongsi kumpulan pengguna yang sama. Pengguna harus memikul tanggungjawab untuk menjaga keselamatan sistem ICT yang digunakan.

3.1.1. Kawalan Capaian Logikal Secara Umum

i. Semua sistem atau aplikasi perlu mempunyai garis panduan capaian logikal yang memaparkan keperluan atau kategori pengguna dan hak capaian yang berpatutan. Hak capaian pada umumnya diberikan atas dasar keperluan(*need to know and need to use basis*);

ii. Setiap pengguna, pentadbir dan penyelenggara aplikasi atau sistem akan diberi ID untuk memasuki aplikasi atau sistem serta hak capaiannya. Mereka yang diberi ID perlu memahami dan mematuhi syarat-syarat penggunaan sistem dan juga keistimewaan hak capaian masing-masing dan memastikan semua ID dilindungi dari disalah guna atau dicerobohi;

iii. ID umum sedia ada bagi aplikasi atau sistem seperti ID tetamu(*Guest*) atau ID tanpa identiti(*Anonymous*) perlu dipadamkan atau dikunci kegunaannya(*disable*) atau ditukar kata laluannya;
iv. Pentadbir Sistem mestilah memastikan ID pengguna tidak boleh dihapus atau digunakan semula(*recycle*);
v. Penggunaan ID milik orang lain adalah dilarang.

3.1.2. Perlindungan Kata Laluan

Bagi menjamin keselamatan kata laluan, pengguna perlulah mematuhi prosedur berikut;

i. Rahsiakan kata laluan.
ii. Kata laluan hendaklah dihafal dan jangan disalin atau dipapar di mana-mana media seperti buku catatan, peralatan mudah alih, *USB drive* dan sebagainya kerana dikhuatiri akan diketahui dan disalahgunakan oleh orang lain. Jika kata laluan perlu didokumenkan, pastikan ianya disampulkan dan dilakrikan(*seal*). Dokumen tersebut hendaklah diserahkan kepada CIO untuk disimpan di lokasi yang selamat.
iii. Gunakan kata laluan yang kukuh*(strong)* melalui kombinasi abjad, simbol dan nombor(*alphanumeric characters*) dan mempunyai sekurang-kurangnya dua belas (12) aksara sebagai contoh P@ssw0rd1234. Jangan menggunakan kata laluan yang mudah diteka seperti nama, nombor telefon, tarikh lahir, perkataan atau nombor-nombor umum.
iv. Pengguna tidak boleh menggunakan semula empat (4) kata laluan yang terdahulu dan digalakkan menukar kata laluan sekurang kurangnya:-
    a) Tiga (3) bulan sekali bagi pengguna aplikasi dan *login* komputer; atau
    b) Satu (1) tahun sekali bagi sistem operasi atau pangkalan data (cth : Oracle, PHP, mySQL, MSSQL dll).
v. Kata laluan mesti ditukar dalam keadaan berikut:
    a) Semasa memasuki sistem untuk kali pertama(*first login*) atau selepas kata laluan di set semula;
    b) Kata laluan asal(*default)* yang diberikan bersama aplikasi atau sistem yang dibekalkan oleh Pentadbir Sistem;
    c) Apabila ID dan kata laluan disyaki telah dicerobohi; atau
    d) Apabila berlaku pertukaran tugas.
vi. Kata laluan tidak boleh sama dengan ID pengguna;
vii. Tentukan had masa pengesahan selama 2 minit (mengikut kesesuaian sistem). Jika tidak sesi akan ditamatkan.
viii. Kata laluan tidak boleh mengguna abjad yang sama(*repeating characters*);
ix. Dilarang memaparkan kata laluan pada medan kemasukkan kata laluan sistem atau aplikasi(*non-display mode*).
x. Melaksanakan penyulitan(*encryption*) kata laluan ketika proses penghantaran.
xi. Sekiranya kata laluan telah dicerobohi atau disyaki dicerobohi, pengguna hendaklah melaporkan kepada CERT PPTGWP melalui emel ke certptgwp@ptgwp.gov.my dengan serta merta; dan
xii. Dilarang menyimpan katalaluan secara *autosaved* mode.

3.1.3. Pengurusan ID dan Hak Capaian Logikal

i. ID dan capaian logikal hanya boleh diberi selepas borang permohonan diisi dengan lengkap oleh pengguna, disokong atau disahkan oleh Ketua Bahagian/Unit dan diluluskan oleh Ketua Bahagian Pengurusan Maklumat/Ketua Jabatan;

ii. Pentadbir Sistem akan mengemukakan dua (2) borang akuan penerimaan ID untuk disahkan. Satu (1) untuk simpanan pengguna dan satu salinan lagi untuk simpanan dan rujukan Bahagian Pengurusan Maklumat. Pengguna dikehendaki mematuhi arahan-arahan yang tercatat dalam borang akaun penerimaan ID tersebut. Bagi sistem dan aplikasi yang menggunakan notifikasi emel, penerimaan ID dan kata laluan akan dihantar melalui emel.

iii. Pengguna mesti memaklumkan kepada Pentadbir Sistem dengan mengemukakan borang pengemaskinian atau pembatalan ID sekiranya mereka bertukar kerja atau berubah bidang tugas;

iv. Pentadbir Sistem perlu menyediakan senarai terkini pengguna aplikasi atau sistem sekurang-kurangnya setahun sekali;

v. Pentadbir Sistem perlu menyemak dan menyelaras senarai terkini pengguna dan membandingkannya dengan borang permohonan dan pelupusan ID sekurang-kurangnya setahun sekali.

vi. Untuk sistem dan aplikasi, hak capaian untuk mengubah data dalam pangkalan data secara terus(*direct*) adalah tidak dibenarkan kecuali kemudahan tersebut tidak disediakan melalui sistem atau aplikasi terlibat; dan

vii. Menghadkan dan mengawal penggunaan program utiliti yang berkemampuan mengatasi sebarang kawalan sistem dan aplikasi. Penggunaan program utiliti perlulah mendapat kebenaran Ketua Bahagian Pengurusan Maklumat/Ketua Jabatan.

3.1.4. Pembatalan ID dan Hak Capaian

i. Hak capaian pengguna yang tidak diperlukan lagi hendaklah dibatalkan;

ii. Penggantungan ID perlu dikuatkuasakan secara automatik apabila berlaku tiga kali kesalahan kata laluan berturut-turut. Pengguna perlu membuat permohonan pengaktifan semula ID tersebut.

iii. Pemilikan ID bukan hak mutlak seseorang kerana ianya tertakhluk kepada peraturan Jabatan dan boleh ditarik balik sekiranya penggunaannya melanggar peraturan; dan

iv. Pentadbir sistem boleh membeku dan menamatkan akaun pengguna atas sebab-sebab berikut:

a) ID bagi Kakitangan bertukar jabatan, berhenti atau bersara sepatutnya ditamatkan selepas empat belas (14) hari atau selepas menerima borang penamatan ID.

b) ID bagi Kakitangan diberhentikan atas sebab-sebab tatatertib atau melanggar dasar/polisi Jabatan ditamatkan serta merta; atau

c) ID bagi Kakitangan yang berada dalam siasatan pihak berkuasa harus dibekukan sementara sehingga kes selesai.

3.1.5. Jejak Audit(*Audit Trails*)

Jejak audit merupakan rekod aktiviti-aktiviti yang berlaku dalam sistem secara kronologi untuk sesuatu peristiwa dan ianya penting bagi mewujudkan akauntabiliti sistem. Maklumat jejak audit penting dalam sesuatu penyiasatan apabila berlaku sesuatu masalah.

i. Setiap aktiviti capaian sistem maklumat dan aplikasi oleh pengguna hendakah direkodkan dengan mengaktifkan log aktiviti dan sistem(*event log and system log*);

ii. Pentadbir Sistem hendaklah menyemak maklumat jejak audit secara berkala atau harian untuk memastikan kegunaan sistem adalah teratur dan tidak ada unsur-unsur mencurigakan. Sekiranya ada, Pentadbir Sistem hendaklah membuat siasatan segera dan melaporkannya kepada CERT PPTGWP. Di antara perkara yang perlu diperhatikan adalah;
   a) Kegagalan atau cubaan memasuki bahagian-bahagian sistem atau aplikasi yang di luar hak capaian pengguna berkenaan;
   b) Penggunaan ID kritikal dimana tahap capaian dan kebolehannya tanpa had. (contoh : *super user*) ;
   c) Corak penggunaan sistem yang luar biasa (contoh : luar dari waktu pejabat atau waktu kerja yang dibenarkan);
   d) Perubahan kepada profil keselamatan(*security profile*);

iii. Fail jejak audit bagi sistem atau aplikasi perkhidmatan teras yang berprofil tinggi hendaklah disimpan selama mungkin. Sekiranya *housekeeping* perlu dilaksanakan salinan pendua perlu dibuat.

iv. Pentadbir Sistem hendaklah melindungi maklumat jejak audit daripada dihapus, diubahsuai, dipalsukan(*fabricate*) atau dibuat penyusunan semula dengan menggunakan *Machine Access Control* (MAC) atau tanda tangan digital(*digital signature*).

v. Aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya.

vi. Pelarasan waktu dan masa berkaitan dengan sistem pemprosesan maklumat dalam PPTGWP atau domain keselamatan perlu diselaraskan dengan sumber waktu yang dipersetujui.

vii. Merekodkan maklumat jejak audit sebanyak mungkin dan praktikal untuk digunakan bagi tujuan penyiasatan. Antaranya adalah :
   a) ID pengguna;
   b) Fungsi, sumber dan maklumat yang digunakan atau diubah;
   c) Tarikh dan masa*(time stamp);*
   d) Alamat komputer (nama dan IP termasuk MAC IP) dan maklumat laluan rangkaian(*network path*); dan
   e) Pengguna sistem ICT boleh menjadi sebagai individu atau sekumpulan pengguna yang berkongsi kumpulan pengguna yang sama. Pengguna harus memikul tanggungjawab untuk menjaga keselamatan sistem ICT yang digunakan.