



**PANDUAN TEKNIKAL KESELAMATAN SIBER
GERBANG PERKHIDMATAN DALAM TALIAN KERAJAAN
(MyGOVERNMENT)**

VERSI 1.0

KANDUNGAN

1.	Pengenalan	1
2.	Pematuhan kepada Standard dan Garis Panduan Keselamatan Siber	1
3.	Peranan Agensi.....	2
3.1	Pengesahan Pengguna	2
3.2	Pengurusan Akaun (<i>Credential</i>)	3
3.3	Perkhidmatan <i>Single Sign-On (SSO)</i>	3
3.4	Kebenaran (<i>Authorisation</i>).....	4
3.5	Indeks Umum	4
I.	Rujukan.....	5

GARIS PANDUAN KESELAMATAN SIBER GERBANG PERKHIDMATAN DALAM TALIAN KERAJAAN (PORTAL MYGOVERNMENT)

1. PENGENALAN

Portal MyGovernment merupakan gerbang tunggal perkhidmatan dalam talian kerajaan merentasi sektor perkhidmatan berkonsepkan *life-event* dan berpaksikan rakyat yang menawarkan perkhidmatan menerusi ruang siber.

Ruang siber ditakrifkan sebagai sistem-sistem teknologi maklumat dan komunikasi, maklumat yang disimpan dalam sistem-sistem tersebut, manusia yang berinteraksi dengan sistem-sistem ini secara fizikal atau maya serta persekitaran fizikal sistem-sistem tersebut disimpan.

Aspek keselamatan ruang siber merangkumi keselamatan maklumat di dalamnya perlu diteliti pada setiap peringkat / fasa iaitu Perolehan, Pembangunan, Pelaksanaan, Penyelenggaraan dan Pelupusan.

2. PEMATUHAN KEPADA STANDARD DAN GARIS PANDUAN KESELAMATAN SIBER

Agensi penyedia perkhidmatan dalam talian melalui portal MyGovernment **hendaklah** mematuhi standard dan garis panduan keselamatan maklumat dan ruang siber seperti berikut:

- i. Melaksanakan semua keperluan keselamatan berdasarkan Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA) bagi memastikan kawalan keselamatan yang sepadan dengan risiko ke atas aset-aset yang ditentukan;
- ii. Menyediakan Pelan Pengurusan Keselamatan Maklumat (*ISMP*) berdasarkan RAKKSSA bagi perkhidmatan dalam talian kerajaan yang ditawarkan;
- iii. Melaksanakan penilaian pematuhan, pemantauan dan penyelenggaraan ke atas *ISMP*, termasuk:

- a. Melaksanakan pematuhan Pengurusan Keselamatan Maklumat (*ISMS*) ke atas perkhidmatan dalam talian agensi;
 - b. Memastikan pembangunan, pengujian, pelaksanaan dan penyelenggaraan ke atas Pelan Pemulihan Bencana (*DRP*) perkhidmatan dalam talian agensi;
 - c. Memastikan perkhidmatan dalam talian agensi dicapai menggunakan saluran selamat sekurang-kurangnya protokol TLS versi 1.2 dengan *cipher suite* yang menggunakan *key length* sekurang-kurangnya 128 bit untuk *symmetric key* dan 2048 bit untuk *asymmetric key*;
 - d. Menyimpan log transaksi sekurang-kurangnya enam (6) bulan untuk tujuan semakan transaksi dengan mengambil kira sandaran (*back-up*) di luar premis; dan
 - e. Memastikan pemantauan ke atas trafik rangkaian bagi mengesan sebarang aktiviti yang mengganggu perkhidmatan dalam talian agensi.
- iv. Memastikan perkhidmatan dalam talian yang diberi adalah mematuhi semua arahan keselamatan maklumat yang sedang berkuat kuasa;
 - v. Memastikan perkongsian maklumat pengguna kepada agensi bukan kerajaan adalah mematuhi peraturan yang sedang berkuat kuasa; dan
 - vi. Memastikan *Personally Identifiable Information (PII)* yang di bawah kawalan perkhidmatan dalam talian kerajaan adalah mengambil kira kawalan-kawalan yang sepadan dengan risiko sebagaimana yang dinyatakan dalam RAKSSA.

3. PERANAN AGENSI

Agensi perlu melaksanakan proses mengesahkan identiti / pendaftaran pengguna, pengurusan akuan (*credential*) serta menguruskan kebenaran (*authorisation*).

3.1 Pengesahan Pengguna

Agensi hendaklah mengesahkan identiti / pendaftaran pengguna melalui kaedah berikut:

- i. Pengesahan identiti hendaklah dilakukan mengikut amalan baik berdasarkan standard ISO/IEC 29115 *Entity Authentication Assurance Framework*;
- ii. Tahap Jaminan/*Level of Assurance* (LoA) yang diperlukan untuk perkhidmatan di Portal MyGovernment adalah sekurang-kurangnya LoA 3; dan
- iii. Unit Pemodenan Tadbiran Dan Perancangan Pengurusan Malaysia (MAMPU) hendaklah melaksanakan penilaian pematuhan tahap jaminan ke atas agensi.

3.2 Pengurusan Akuan (*Credential*)

Agensi hendaklah memenuhi perkara-perkara berikut dalam pengurusan akuan (*credential*):

- i. Agensi yang menguruskan akuan ialah agensi yang sama atau berbeza daripada agensi yang mendaftarkan pengguna;
- ii. Memberikan akuan tunggal yang diperoleh daripada *Credential Management System* kepada pengguna selepas pengesahan identiti; dan
- iii. Memastikan akuan tunggal yang diberikan kepada pengguna hanya dibekalkan oleh *Credential Management System* yang disahkan oleh Kerajaan berdasarkan standard dan garis panduan.
- iv. Memastikan mematuhi standard yang ditetapkan iaitu;
 - a. Bagi pengesahan identiti LoA 3, *credential* boleh dalam bentuk faktor tunggal (*single factor*); dan
 - b. Bagi pengesahan identiti LoA 4, *credential* hendaklah dalam bentuk dwifaktor (*two factor*).

3.3 Perkhidmatan *Single Sign-On* (SSO)

Agensi perlu memenuhi perkara-perkara berikut dalam perkhidmatan SSO seperti berikut:

- i. Akaun tunggal hanya boleh digunakan oleh pengguna berdaftar sahaja untuk tujuan capaian perkhidmatan dalam talian kerajaan; dan
- ii. Semua perkhidmatan dalam talian kerajaan pelbagai sektor perkhidmatan hendaklah dicapai menggunakan akaun tunggal melalui satu log masuk sahaja.
- iii. Memastikan mematuhi standard yang ditetapkan iaitu;
 - a. Perkhidmatan dalam talian agensi hendaklah mempunyai mekanisme untuk mengendalikan pengesahan identiti melalui standard SAML versi 2.0 bagi tujuan menyediakan perkhidmatan SSO kepada pengguna dengan menggunakan akaun tunggal.

3.4 Kebenaran (*Authorisation*)

Kebenaran bagi capaian perkhidmatan dalam talian agensi ditentukan oleh agensi penyedia perkhidmatan. Kebenaran hendaklah berdasarkan capaian minimum (*least privileged access*) seperti yang dinyatakan dalam RAKKSSA. Agensi perlu memaparkan pernyataan 'Anda tidak mempunyai akses ke sistem ini' bagi capaian ke sistem yang tidak dibenarkan.

3.5 Indeks Umum

Perkhidmatan dalam talian agensi hendaklah menggunakan indeks umum untuk kebenaran capaian. Indeks umum ialah nombor kad pengenalan bagi warganegara Malaysia dan nombor passport didahului dengan kod negara mengikut standard ISO 3166-1 bagi bukan warganegara.

I. RUJUKAN

Pembangunan panduan teknikal ini merujuk kepada standard seperti yang berikut:

- [1] Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA) Versi April 2016
- [2] ISO/IEC 29115:2013 *Entity Authentication Assurance Framework*
- [3] *Transport Layer Security (TLS) Protocol* Versi 1.2
- [4] *Security Assertion Markup Language (SAML) Versi 2.0*
- [5] ISO 3166-1 *Alpha 2 Country Code*
- [6] Arahan Keselamatan (Semakan dan Pindaan 2017)