PENGURUSAN REKOD RAHSIA RASMI DALAM PERSEKITARAN ICT

OLEH:

BAHAGIAN KESELAMATAN PERLINDUNGAN ICT DAN RAHSIA RASMI
PEJABAT KETUA PEGAWAI KESELAMATAN KERAJAAN (CGSO)

AGENDA

1. PENGENALAN
2. KEPERLUAN KESELAMATAN PERLINDUNGAN MAKLUMAT
3. PENGURUSAN MAKLUMAT RAHSIA RASMI DALAM PERSEKITARAN ICT
4. RUMUSAN

PENGENALAN

TUJUAN

Memberi panduan dan penjelasan kepada agensi mengenai Pengurusan Rekod Rahsia Rasmi Dalam Persekitaran ICT selaras dengan peruntukan Arahan Keselamatan (Semakan dan Pindaan 2017).

OBJEKTIF

Melindungi maklumat dan sistem maklumat daripada capaian, penggunaan dan pengubahsuaian dengan cara yang tidak dibenarkan.

KEPERLUAN PERLINDUNGAN KESELAMATAN MAKLUMAT

KERAHSIAAN

Maklumat tidak didedahkan sewenangnya atau dibiarkan diakses tanpa kebenaran

Authentication
Encryption

INTEGRITI

Maklumat Sentiasa lengkap, tepat, dan kemaskini. Hanya boleh diubah dengan cara yang dibenarkan sahaja

Hashing/Encryption
Auditing

KETERSEDIAAN

Memastikan maklumat sentiasa boleh diakses pada bila-bila masa oleh pengguna yang dibenarkan sahaja

Backup
Redundant system/cluster

TIDAK BOLEH DISANGKAL

Jaminan bahawa seseorang tidak menafikan kesahihan sesuatu maklumat

Digital Signature

PENGURUSAN MAKLUMAT RAHSIA RASMI DALAM PERSEKITARAN ICT

PERLAKSANAAN PENGURUSAN REKOD ELEKTRONIK BAGI AGENSI KERAJAAN

- Kaedah pelaksanaan pembangunan sistem:
  - Dibangunkan secara dalaman; dan
  - Dibangunkan dengan pihak pembekal luar.

- Pengurusan Rekod Elektronik adalah tertakluk kepada Bab 5 (Keselamatan Rahsia Rasmi Dalam Persekitaran Teknologi Maklumat Dan Komunikasi (ICT)) & para 60, Arahan Keselamatan (Semakan dan Pindaan 2017) dan Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA) serta Dasar Keselamatan ICT (DKICT) Agensi.

PENGURUSAN MAKLUMAT RAHSIA RASMI DALAM PERSEKITARAN ICT

PRA SYARAT PEMBANGUNAN SISTEM

1. Menentukan Klasifikasi Data
2. Penilaian Risiko
3. Infrastruktur Sistem *(on-premis/outside provider)*
4. Keperluan Ciri-ciri Kawalan Keselamatan Sistem
5. Kawalan Keselamatan Personel
6. Rujukan awal cadangan pembangunan sistem pada Pejabat CGSO

PENGURUSAN MAKLUMAT RAHSIA RASMI DALAM PERSEKITARAN ICT

1. Proses Pengelasan Rahsia Rasmi
   - Pelantikan Pegawai Pengelas di bawah Seksyen 2B, Akta Rahsia Rasmi
   - Dilaksanakan secara konvensional terlebih dahulu (di luar sistem)
   - Buku Daftar Suratan Rahsia Rasmi (AM 492, AM 492 A)

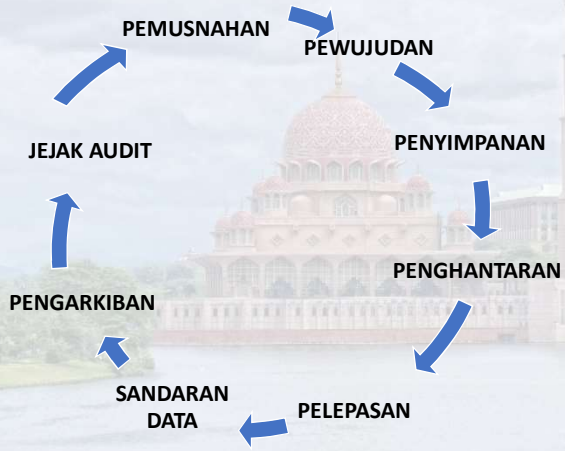
2. Proses Pengelasan Semula Rahsia Rasmi
   - Pegawai Pengelasan Semula di bawah Seksyen 2C, ARR
   - Dilaksanakan secara konvensional terlebih dahulu (di luar sistem)
   - Buku Daftar Suratan Rahsia Rasmi (AM 492, AM 492 B)

CONTOH JENIS-JENIS REKOD DI DALAM Digital Document Management System (DDMS)

BIL	JENIS REKOD		
1	Agenda mesyuarat	18	Minit ceraian
2	Akta/ Ordinan	19	Minit Mesyuarat
3	Carta	20	Nota Mesyuarat/ Perbincangan
4	Dokumen Tender/ Sebutharga	21	Pekeliling
5	Emel	22	Perjanjian/ Memorandum
6	Emel muatnaik (tidak berkaitan)	23	Piawaian/ Standard
7	Fail	24	Poster
8	Faks	25	Prosiding
9	Foto	26	Siaran Akhbar
10	Garis Panduan/ Panduan	27	Sijil
11	Kertas Kerja/ Kertas Konsep	28	Slaid Pembentangan
12	Kertas Pertimbangan	29	Surat Menyurat
13	Laporan	30	Teks Ucapan
14	Lukisan Teknikal	31	Terbitan
15	Maklumbalas Mesyuarat	32	Borang
16	Memo	33	Jadual
17	Minit bebas		

PENGURUSAN MAKLUMAT DALAM PERSEKITARAN ICT

PROSES KITARAN HAYAT MAKLUMAT RAHSIA RASMI DALAM ELEKTRONIK



Information security must protect information throughout the **life span of information**, from the initial of creation of the information on through to the final disposal of information.

PENGURUSAN MAKLUMAT RAHSIA RASMI DALAM PERSEKITARAN ICT

PENGENDALIAN MAKLUMAT SEMASA PROSES PEWUJUDAN REKOD RAHSIA RASMI ELEKTRONIK

Rekod fizikal perlu mengambil kira beberapa perkara seperti berikut:

- Penawanan rekod melalui mesin pengimbas khusus yang berdaftar.
- Penentuan peranan pengguna selaras dengan kehendak Arahan Keselamatan (Semakan dan Pindaan 2017)

1. Admin Agensi	4. Pendaftar Kecil Rahsia
2. Pengurus Rekod	*5. Information Worker (IW)*
3. Pendaftar Rahsia	6. Pengguna Biasa

- Penetapan *Security Clearance* bagi kawalan dan kebenaran akses.
  - ➢ Menjalani tapisan keselamatan.

PENGURUSAN MAKLUMAT RAHSIA RASMI DALAM PERSEKITARAN ICT

KAWALAN CAPAIAN REKOD RAHSIA RASMI ELEKTRONIK

- Capaian kepada rekod rahsia rasmi dalam elektronik hendaklah dikawal setiap masa.
- Pengguna yang telah dikenalpasti berdasarkan peranan di agensi.
- Pengasingan capaian bagi rekod rasmi dan rekod rahsia rasmi.
- Kawalan capaian rahsia rasmi melalui *multifactor authentication (MFA).*
- Capaian hanya kepada rekod rahsia rasmi kepada yang dibenarkan sahaja.
- Capaian ke sistem melalui protokol *https*.
- Penentuan klasifikasi maklumat hendaklah dirujuk ke Pejabat CGSO. Rekod elektronik yang dipaparkan samada secara preview ataupun yang dimuat turun ke dalam komputer hendaklah dilindungi:
- Penggunaan *watermark* bagi mengelakkan kebocoran maklumat rahsia rasmi;
- Rekod elektronik yang dimuat turun berada dalam bentuk enkrip;

PENGURUSAN MAKLUMAT RAHSIA RASMI DALAM PERSEKITARAN ICT

KAWALAN PENYIMPANAN REKOD RAHSIA RASMI ELEKTRONIK

- Maklumat rahsia rasmi yang disimpan hendaklah **dienkrip**.
- Sistem mestilah berupaya **menjana *hash value*** bagi setiap rekod yang telah diimbas dan disimpan bagi tujuan validasi terhadap intergriti rekod.
- Penyimpanan rahsia rasmi hendaklah dilindungi secara **fizikal & logikal** mengikut perkembangan teknologi dan arahan-arahan Kerajaan dari semasa ke semasa.
  - Kawalan secara fizikal - pengasingan server/rak server
    - pemantauan cctv/kad akses elektronik
  - Kawalan secara logikal - Segmentasi Rangkaian
    - reka bentuk server 3 tier (web/aplikasi/pangkalan data)

PENGURUSAN MAKLUMAT RAHSIA RASMI DALAM PERSEKITARAN ICT

KAWALAN PENYIMPANAN REKOD RAHSIA RASMI ELEKTRONIK

- Penyimpanan maklumat Rahsia Rasmi dalam pengkomputeran awan *(cloud computing)* tertakluk kepada Arahan Keselamatan (Semakan dan Pindaan 2017):
  - ✓ hanya yang dibangunkan dan dibenarkan oleh Kerajaan; dan
  - ✓ Tertakluk kepada arahan yang dikeluarkan oleh Kerajaan dari semasa ke semasa.
- Penggunaan *cloud computing* yang disediakan oleh perkhidmatan luar adalah tidak dibenarkan bagi maklumat rahsia rasmi.

PENGURUSAN MAKLUMAT RAHSIA RASMI DALAM PERSEKITARAN ICT

PENGENDALIAN SEMASA PROSES PENGHANTARAN REKOD RAHSIA RASMI ELEKTRONIK

- Memastikan maklumat rahsia rasmi yang dihantar melalui medium komunikasi elektronik sentiasa dienkrip;
- Penghantaran maklumat rahsia rasmi melalui e-mel rasmi:
  - ➢ Perlu mematuhi Arahan Keselamatan (Semakan dan Pindaan 2017) para 134;
  - ➢ Sistem emel perlu mempunyai kemudahan enkripsi untuk penghantaran emel rahsia rasmi yang selamat;
  - ➢ Penggunaan katalaluan (sekurang-kurangnya) bagi maklumat SULIT dan TERHAD.

PENGURUSAN MAKLUMAT RAHSIA RASMI DALAM PERSEKITARAN ICT

PELEPASAN REKOD RAHSIA RASMI ELEKTRONIK

- Prinsip-prinsip keselamatan:
  - ➢ Prinsip Perlu Mengetahui;
  - ➢ Prinsip Perlu Menyimpan; dan
  - ➢ Prinsip Lihat dan Kembalikan.
- Had kawalan akses kepada yang dibenarkan sahaja.

PENGURUSAN MAKLUMAT RAHSIA RASMI DALAM PERSEKITARAN ICT

KEPERLUAN PROSES SANDARAN DATA BAGI REKOD RAHSIA RASMI ELEKTRONIK

- Keperluan sandaran data *(backup data)* ke atas maklumat rahsia rasmi :
  - ➢ Memastikan kesinambungan perkhidmatan sekiranya berlaku gangguan terhadap sistem
  - ➢ Dilaksanakan secara berkala berdasarkan peraturan semasa yang berkuat kuasa untuk memastikan bahawa sistem boleh dipulihkan
  - ➢ Disimpan dalam persekitaran yang selamat dan lokasi yang berasingan
  - ➢ Bekas media sandaran, lokasi dan infrastruktur yang menempatkan bekas media sandaran hendaklah disahkan oleh CGSO dan sebarang perubahan hendaklah mendapat pengesahan semula daripada CGSO.

PENGURUSAN MAKLUMAT RAHSIA RASMI DALAM PERSEKITARAN ICT

KEPERLUAN PENGARKIBAN DAN JEJAK AUDIT BAGI REKOD RAHSIA RASMI ELEKTRONIK

- Proses pengelasan semula perlu dilaksanakan terlebih dahulu bagi mana-mana rekod yang hendak diarkibkan.
- Sistem yang mengendalikan maklumat rahsia rasmi hendaklah mempunyai mekanisma jejak audit bagi mengesan sebarang perubahan yang berlaku kepada maklumat disimpan.
- Jejak audit merangkumi akses pengguna, pewujudan data serta perubahan yang dilakukan bagi memastikan transaksi yang berlaku di dalam sistem direkodkan.
- Keperluan jejak audit juga penting bagi tujuan pengauditan untuk menyemak sekiranya berlaku perlanggaran polisi terhadap data yang disimpan.

PENGURUSAN MAKLUMAT RAHSIA RASMI DALAM PERSEKITARAN ICT

PELUPUSAN/PEMUSNAHAN BAGI REKOD RAHSIA RASMI ELEKTRONIK

- Sebarang pemusnahan/pelupusan maklumat rahsia rasmi perlu mendapat kebenaran Ketua Jabatan;
- Merangkumi pelupusan data dan media storan elektronik;
- Pelupusan secara logikal dan fizikal;
- Prosedur pelupusan sepertimana dalam Garis Panduan Sanitasi Media Sektor Awam;
- Pengelasan semula maklumat rahsia rasmi sebelum tindakan pelupusan diambil;

RUMUSAN

Semua jabatan yang menguruskan rahsia rasmi dalam persekitaran ICT hendaklah mematuhi tatacara pengurusan rahsia rasmi dan tertakluk kepada arahan-arahan yang dikeluarkan oleh Kerajaan dari semasa ke semasa.

Rujukan kepada Pejabat CGSO jika jabatan dan agensi mempunyai cadangan untuk membangunkan sistem yang mengandungi maklumat rahsia rasmi.

SESI SOAL JAWAB