PEDOMAN KEPALA LEMBAGA SANDI NEGARA

NOMOR 5 TAHUN 2016

TENTANG

KLASIFIKASI TINGKAT KERAHASIAAN INFORMASI

BAB I

PENDAHULUAN

A. UMUM

Sejalan dengan upaya mewujudkan tata pemerintahan yang baik, pemerintah menetapkan Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik yang mengatur seluruh Badan Publik untuk dapat memberikan pelayanan informasi yang terbuka, transparan dan bertanggungjawab kepada masyarakat. Dalam Pasal 2 Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, informasi milik Badan Publik dibagi menjadi dua jenis yaitu, Informasi Publik bersifat terbuka dan dapat diakses oleh setiap Pengguna Informasi Publik dan Informasi Publik yang Dikecualikan bersifat ketat dan terbatas. Informasi Publik yang dikecualikan bersifat rahasia sesuai dengan Undang-Undang, kepatutan, dan kepentingan umum didasarkan pada pengujian tentang konsekuensi yang timbul apabila suatu informasi diberikan kepada masyarakat serta setelah dipertimbangkan dengan seksama bahwa menutup Informasi Publik dapatmelindungi kepentingan yang lebih besar daripada membukanya atau sebaliknya. Merujuk definisi tersebut dan sebagai upaya pengamanan informasi maka setiap Badan Publik perlumenentukan klasifikasi tingkat kerahasiaan terhadap Informasi Publik yang Dikecualikan.

Sebagai acuan prosedur mengklasifikasikan tingkat kerahasiaan informasi publik yang dikecualikan maka disusunlah Pedoman Klasifikasi Tingkat Kerahasiaan Informasi guna membantu Unit Kerja atau Unit Sandi Instansi

Pemerintah dalam menjalankan pengamanan informasi publik yang dikecualikan dengan tepat dan obyektif.

B. MAKSUD DAN TUJUAN

1. Maksud

   Maksud ditetapkannya Pedoman Klasifikasi Tingkat Kerahasiaan Informasi adalah sebagai panduan dalam menentukan klasifikasi tingkat kerahasiaan informasi di Instansi Pemerintah dalam menyelenggarakan Persandian.

2. Tujuan

   Tujuan disusunnya Pedoman Klasifikasi Tingkat Kerahasiaan Informasi adalah untuk mewujudkan tahapan pengklasifikasian tingkat kerahasiaan informasi secara obyektif dan dapat dipertanggungjawabkan.

C. SASARAN

Sasaran Pedoman ini adalah terwujudnya klasifikasi tingkat kerahasiaan informasi untuk kepentingan keamanan nasional melalui tata cara klasifikasi tingkat kerahasiaan yang sesuai dengan kebutuhan, dan Pedoman ini ditujukan untuk Pemilik Informasi yang bertanggungjawab atas klasifikasi dan pengendalian informasi.

D. ASAS

1. Obyektif

   Klasifikasi tingkat kerahasiaan informasi harus dilakukan berdasarkan metode yang valid dan mengedepankan obyektivitas.

2. Terbatas

   Klasifikasi tingkat kerahasiaan informasi yang dikecualikan harus terbatas pada informasi tertentu untuk menghindari penafsiran yang subyektif dan kesewenangan.

E. RUANG LINGKUP

BAB I. PENDAHULUAN

BAB II. TINGKAT KERAHASIAAN INFORMASI

BAB III. TATA CARA KLASIFIKASI TINGKAT KERAHASIAAN INFORMASI

BAB IV. PENUTUP

F. PENGERTIAN

1. Informasi adalah keterangan, pernyataan, gagasan, dan tanda-tanda yang mengandung nilai, makna, dan pesan, baik data, fakta maupun penjelasannya yang dapat dilihat, didengar, dan dibaca yang disajikan dalam berbagai kemasan dan format sesuai dengan perkembangan teknologi informasi dan komunikasi secara elektronik ataupun nonelektronik.
2. Pengklasifikasian adalah proses penentuan dan penetapan tingkat kerahasiaan.
3. Tingkat kerahasiaan adalah tingkat rahasia informasi yang ditentukan dan ditetapkan berdasarkan pengujian tentang konsekuensi yang timbul apabila suatu informasi diberikan kepada publik.
4. Pemilik informasi adalah pegawai maupun pejabat Instansi Pemerintah yang karena fungsi dan jabatannya bertanggung jawab atas semua data dan Informasi Berklasifikasi yang dihasilkan serta dikelola dan/atau dikumpulkannya selama bekerja dan atas nama instansinya.

BAB II
TINGKAT KERAHASIAAN INFORMASI

Tingkat kerahasiaan informasi adalah tingkatan yang ditentukan dan ditetapkan terhadap informasi publik yang dikecualikan berdasarkan akibat yang dapat ditimbulkan bila informasi tersebut diketahui oleh pihak yang tidak berhak mengetahuinya.

Kerahasiaan informasi diklasifikasikan dalam 3 tingkatan, yaitu:

1. Informasi Terbatas, merupakan informasi yang jika diakses oleh pihak yang tidak berkewenangan menimbulkan risiko rendah. Jika informasi tersebut diketahui oleh pihak yang tidak berhak dapat mengakibatkan kerusakan terhadap keamanan nasional.
2. Informasi Rahasia, merupakan informasi yang jika diakses oleh pihak yang tidak berkewenangan menimbulkan risiko sedang. Jika informasi tersebut diketahui oleh pihak yang tidak berhak dapat mengakibatkan kerusakan yang serius terhadap keamanan nasional.
3. Informasi Sangat Rahasia, merupakan informasi yang jika diakses oleh pihak yang tidak berkewenangan menimbulkan risiko tinggi. Jika informasi tersebut diketahui oleh pihak yang tidak berhak dapat mengakibatkan kerusakan yang sangat serius terhadap keamanan nasional.

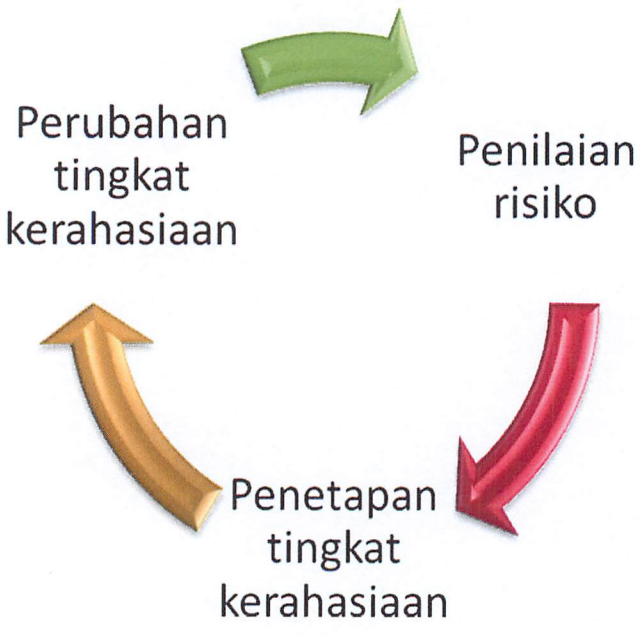
BAB III
TATA CARA KLASIFIKASI TINGKAT KERAHASIAAN

Klasifikasi tingkat kerahasiaan dilakukan terhadap informasi dalam rangka pengamanan informasi terhadap aset informasi yang dimiliki oleh organisasi karena dalam kenyataannya tidak semua informasi mempunyai nilai guna yang sama, atau memiliki risiko yang sama, mekanisme perlindungannyapun akan berbeda. Sehingga agar lebih efisien, informasi sebagai aset organisasi harus diberi klasifikasi tingkat kerahasiaan berdasarkan risiko, nilai guna data atau kriteria lain yang ditentukan dalam organisasi.

Tata cara klasifikasi tingkat kerahasiaan merupakan proses yang berkelanjutan, yang meliputi:

1. Penilaian risiko;
2. Penetapan tingkat kerahasiaan;
3. Perubahan tingkat kerahasiaan.

Proses klasifikasi tingkat kerahasiaan dapat dilihat melalui gambar berikut:



Gambar Tata Cara Klasifikasi Tingkat Kerahasiaan

A. PENILAIAN RISIKO

Penilaian risiko dilakukan oleh Unit Sandi Instansi Pemerintah dengan berkoordinasi kepada masing-masing Unit Kerja dengan cara menghitung risiko yang ditimbulkan jika suatu informasi diakses oleh pihak yang tidak berhak dengan membuat suatu matriks penilaian risiko. Informasi yang dinilai risikonya adalah informasi publik yang dikecualikan sebagaimana dimaksud dalam Undang-Undang Keterbukaan Informasi Publik, yaitu Informasi publik yang apabila dibuka dan diberikan dapat menyebabkan:

1. Terungkapnya rahasia pribadi;
2. Terungkapnya isi akta otentik yang bersifat pribadi dan kemauan terakhir ataupun wasiat seseorang;
3. Terganggunya ketahanan ekonomi nasional;
4. Terungkapnya kekayaan alam Indonesia;
5. Terganggunya kepentingan perlindungan hak atas kekayaan intelektual dan perlindungan dari persaingan tidak sehat;
6. Terungkapnya memorandum/surat-surat antar Badan Publik atau intra Badan Publik yang bersifat rahasia;
7. Terhambatnya proses pengadilan;
8. Terancamnya pertahanan dan keamanan negara;
9. Terganggunya hubungan luar negeri;
10. Terungkapnya informasi yang tidak boleh diungkapkan berdasarkan Undang-Undang.

Pada tahapan penilaian risiko, analisis yang digunakan adalah analisis kualitatif dengan menggunakan ukuran tingkat risiko pada informasi yang dinilai untuk menggambarkan besarnya kemungkinan terjadinya ancaman (yaitu: rendah, sedang, dan tinggi) dan kemungkinan konsekuensi tersebut terjadi.

Penghitungan tingkat risiko dicocokkan dengan kemungkinan terjadinya ancaman dan tingkat kemudahan eksploitasi seperti dapat dilihat pada matriks yang ditunjukkan pada tabel berikut ini:

	KEMUNGKINAN ANCAMAN TERJADI (A)	RENDAH (R)			SEDANG (S)			TINGGI (T)		
	KEMUDAHAN EKSPLOITASI (E)	R	S	T	R	S	T	R	S	T
NILAI ASET (NA)	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Matriks Penilaian Risiko

Untuk setiap informasi, risiko dan ancaman yang relevan harus dipertimbangkan. Risiko dapat diidentifikasi dalam bidang-bidang berikut:

1. organisasi
2. proses dan prosedur
3. rutinitas manajemen
4. personel
5. lingkungan fisik
6. konfigurasi sistem informasi
7. perangkat keras, perangkat lunak atau peralatan komunikasi
8. ketergantungan pada pihak luar

Risiko dapat dikaitkan dengan sifat informasi yang dapat digunakan dengan cara atau untuk tujuan selain yang dimaksudkan ketika informasi dibuat. Kerentanan yang timbul dari sumber yang berbeda perlu dipertimbangkan.

Hal-hal yang menjadi pertimbangan dalam menentukan seberapa sering kemungkinan ancaman terjadi dan bagaimana mudahnya kerentanan dapat dieksploitasi adalah:

1. pengalaman dan statistik kemungkinan ancaman;
2. motivasi dan kemampuan, yang akan berubah dari waktu ke waktu, dan sumber daya yang tersedia untuk memungkinkan pihak yang tidak berhak, serta daya tarik dan kerentanan informasi untuk kemungkinan penyerangan;

3. faktor geografis, misalnya: kedekatan dengan bahan kimia atau tanaman minyak bumi, kemungkinan kondisi cuaca ekstrim, dan faktor-faktor yang dapat mempengaruhi kesalahan manusia dan kerusakan peralatan;
4. kerentanan, baik secara individual maupun agregasi;
5. kontrol yang ada dan seberapa efektif mereka mengurangi kerentanan.

Masukan untuk identifikasi ancaman dan perkiraan kemungkinan ancaman terjadi dapat diperoleh dari pemilik atau pengguna informasi, dari Unit Kerja yang bertanggungjawab dalam kepegawaian, rumah tangga atau umum dan ahli keamanan informasi, ahli keamanan fisik, Kementerian Hukum dan HAM, Kepolisian, serta organisasi lainnya termasuk badan hukum, BMKG, perusahaan asuransi, dan BNPB.

Pengalaman internal dari insiden dan penilaian ancaman sebelumnya harus dipertimbangkan dalam penilaian aset informasi. Jika menggunakan hasil penilaian ancaman sebelumnya, maka harus disadari bahwa ada perubahan terus-menerus dari ancaman yang relevan, terutama jika lingkungan pekerjaan atau sistem informasi berubah.

Skala nilai aset antara 1 –4. Penentuan skala nilai aset berdasarkan tingkat kepentingan aset tersebut yang ditentukan langsung oleh pemilik informasi, dengan rincian sebagai berikut:

1. 1 : penting untuk tingkat staf
2. 2 : penting untuk tingkat eselon III
3. 3 : penting untuk tingkat Unit Kerja
4. 4 : penting untuk tingkat Instansi Pemerintah

Informasi dinilai sebagai aset dengan memperkirakan nilainya sesuai skala di atas terhadap jenis risiko, yang misalnya dapat menyebabkan pengungkapan kerahasiaan, modifikasi, ketidaktersediaan informasi, dan perusakan serta habisnya biaya tertentu dikarenakan bocornya informasi.

Berikut disampaikan tabel yang merupakan contoh pengklasifikasian tingkat kerahasiaan berupa Data Materiil Sandi yang merupakan informasi publik yang dikecualikan karena merupakan informasi yang jika diketahui oleh pihak yang tidak berhak akan dapat menyebabkan terancamnya pertahanan dan keamanan negara.

NO	JENIS INFORMASI	ISI INFORMASI	KATEGORI	
			PUBLIK	DIKECUALIKAN
1	Data Materiil Sandi	Berisi data tentang peralatan sandi, kunci sistem sandi, alat kriptoanalisis, peralatan manajemen kunci, modul enkripsi, dan modul manajemen kunci		

Penilaian risiko dilakukan dengan memperkirakan kemungkinan terjadinya ancaman, kemudahan eksploitasi informasi, dan nilai aset yang diberikan berdasarkan masing-masing jenis risiko.

Sebagai contoh berdasarkan risiko ancaman pada pertahanan dan keamanan negara jika data materiil sandi bocor kemungkinan terjadinya adalah tinggi karena data tersebut dapat dilihat oleh banyak personil Lembaga Sandi Negara dan dikirimkan melalui jaringan internet, lalu kemudahan eksploitasi ancaman tersebut juga tinggi karena data tersebut tersimpan pada komputer yang memiliki akses ke internet yang siapa saja dapat menyadapnya. Kemudian nilai aset yang diberikan terhadap data tersebut adalah 4 karena sangat pentingnya data tersebut. Maka berdasarkan matriks penilaian aset informasi hasil peringkat risikonya adalah 8.

	KEMUNGKINAN ANCAMAN TERJADI (A)	RENDAH (R)			SEDANG (S)			TINGGI (T)		
	KEMUDAHAN EKSPLOITASI (E)	R	S	T	R	S	T	R	S	T
NILAI ASET (NA)	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Berdasarkan penilaian risiko, selanjutnya dilakukan penetapan tingkat kerahasiaan. Dari daftar di atas dapat dilihat bahwa hasil peringkat risiko bernilai 8 (delapan).

B. PENETAPAN TINGKAT KERAHASIAAN

Penetapan Tingkat Kerahasiaan ditentukan berdasarkan penilaian risiko yang telah dilakukan. Selanjutnya diberikan pemeringkatan risiko, yang dipetakan dengan skala sebagai berikut:

1. Risiko rendah : nilainya 1 – 3, informasi pada tingkat ini diklasifikasikan ke dalam klasifikasi terbatas.
2. Risiko sedang : nilainya 4 – 6, informasi pada tingkat ini diklasifikasikan ke dalam klasifikasi rahasia.
3. Risiko tinggi : nilainya 7 – 8, informasi pada tingkat ini diklasifikasikan ke dalam klasifikasi sangat rahasia.

Berdasarkan pemeringkatan risiko, maka informasi data materiil sandi sebagaimana dijelaskan pada contoh penilaian risiko diatas, dapat diklasifikasikan ke dalam klasifikasi sangat rahasia, karena memiliki nilai risiko tinggi, yaitu 8 (delapan).

Penetapan tingkat kerahasiaan dilakukan oleh Kepala Instansi Pemerintah dan ditetapkan dalam bentuk surat penetapan klasifikasi.

Setiap klasifikasi tingkat kerahasiaan informasi memiliki jangka waktu pengecualian informasi sebagai berikut:

1. Sangat rahasia memiliki jangka waktu pengecualian 30 tahun;
2. Rahasia memiliki jangka waktu pengecualian 15 tahun;
3. Terbatas memiliki jangka waktu pengecualian 5 tahun.

C. PERUBAHAN KLASIFIKASI TINGKAT KERAHASIAAN

Perubahan klasifikasi tingkat kerahasiaan dilaksanakan melalui peninjauan secara berkala menurut klasifikasi berdasarkan isi dan jangka waktu pengecualian informasinya.

Peninjauan secara berkala sebagaimana dimaksud bertujuan untuk:

1. deklasifikasi informasi sebelum jangka waktu pengecualian berakhir;

2. deklasifikasi informasi sesuai dengan jangka waktu pengecualiannya; dan/atau
3. penundaan deklasifikasi informasi.

Peninjauan tersebut dilakukan oleh Pimpinan Unit Sandi dan ditetapkan oleh Kepala Instansi Pemerintah.

Pendeklasifikasian informasi sebelum jangka waktu pengecualiannya berakhir dapat dilakukan apabila isi informasi tersebut jika diketahui oleh publik sudah tidak memiliki akibat sebagaimana pada saat ditetapkan.Penundaan pendeklasifikasian informasi dapat dilakukan apabila isi informasi tersebut jika diketahui oleh publik masih memiliki akibat sebagaimana pada saat ditetapkan. Pimpinan Unit Sandi mengajukan permohonan penundaan pendeklasifikasian kepada Kepala Instansi Pemerintah.

BAB IV
PENUTUP

Pedoman klasifikasi tingkat kerahasiaan informasi ini diharapkan dapat bermanfaat dan dapat dijadikan acuan dalam proses klasifikasi tingkat kerahasiaan informasi Instansi Pemerintah sebagai salah satu upaya dalam pelayanan informasi yang terbuka, transparan dan bertanggungjawab kepada Publik dengan tetap mengedepankan aspek pengamanan informasi yang obyektif.

Ditetapkan di Jakarta
pada tanggal 8 Juni 2016
KEPALA LEMBAGA SANDI NEGARA

DJOKO SETIADI