BUPATI BULELENG

PROVINSI BALI

PERATURAN BUPATI BULELENG

NOMOR 79 TAHUN 2017

TENTANG

STANDAR OPERASIONAL DAN PROSEDUR MANAJEMEN PENGAMANAN INFORMASI DIGITAL DI LINGKUNGAN PEMERINTAH KABUPATEN BULELENG

DENGAN RAHMAT TUHAN YANG MAHA ESA

BUPATI BULELENG,

Menimbang : a. bahwa dalam rangka meningkatkan layanan e-government di lingkungan Pemerintah Kabupaten Buleleng dalam bidang pengelolaan dan penyediaan informasi digital, maka perlu adanya standar operasional dan prosedur manajemen pengamanan informasi digital di lingkungan Pemerintah Kabupaten Buleleng;

b. bahwa berdasarkan pertimbangan sebagaimana dimaksud huruf a, perlu menetapkan Peraturan Bupati tentang standar operasional dan prosedur manajemen pengamanan informasi digital di lingkungan Pemerintah Kabupaten Buleleng;

Mengingat : 1. Undang-Undang Nomor 69 Tahun 1958 tentang Pembentukan Daerah-Daerah Tingkat II Dalam Wilayah Daerah-Daerah Tingkat I Bali, Nusa Tenggara Barat dan Nusa Teggara Timur (Lembaran Negara Republik Indonesia Tahun 1958 Nomor 122, Tambahan Lembaran Negara Republik Indonesia Nomor 1655);

2. Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 244, Tambahan Lembaran Negara Republik Indonesia Nomor 5587), sebagaimana telah diubah beberapa kali, terakhir dengan Undang-Undang Nomor 9 Tahun 2015 tentang Perubahan Kedua Atas Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2015 Nomor 58);

3. Peraturan Menteri Komunikasi dan Informatika Nomor 41 Tahun 2007 tentang Panduan Umum Tata Kelola Teknologi Informasi dan Komunikasi Nasional;

MEMUTUSKAN :

Menetapkan : PERATURAN BUPATI TENTANG STANDAR OPERASIONAL DAN PROSEDUR MANAJEMEN PENGAMANAN INFORMASI DIGITAL DI LINGKUNGAN PEMERINTAH KABUPATEN BULELENG.

BAB I

KETENTUAN UMUM

Pasal 1

Dalam Peraturan Bupati ini yang dimaksud dengan :

1. Daerah adalah Kabupaten Buleleng
2. Pemerintah Daerah adalah Pemerintah Kabupaten Buleleng.
3. Bupati adalah Bupati Buleleng.
4. Satuan Kerja Perangkat Daerah yang selanjutnya disingkat SKPD adalah perangkat daerah pada Pemerintah Daerah selaku pengguna/pengelola informasi digital.
5. Informasi digital yang selanjutnya disebut Informasi adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, electronic data interchange (EDI), surat elektronik (electronic mail), telegram, teleks, telecopy atau sejenisnya, huruf, tanda, angka, kode akses atau simbol yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.
6. Teknologi Informasi adalah suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisis, dan atau menyebarkan informasi.
7. Removable *media* adalah alat penyimpanan data komputer yang tidak terpasang secara permanen pada komputer sehingga mudah untuk dibawa dan dipindahkan dari satu komputer ke komputer lain.
8. *Firewall* adalah kombinasi perangkat keras dan perangkat lunak yang digunakan untuk membatasi akses menuju dan atau dari suatu jaringan komputer.
9. *Peak load testing* atau pengujian beban puncak adalah pengujian yang dilakukan terhadap sistem

informasi dengan melakukan simulasi permintaan akses oleh banyak pengguna untuk mengetahui apakah sistem informasi tersebut mampu melayani permintaan sesuai dengan yang diperkirakan.

10. *Stress testing* adalah pengujian yang dilakukan untuk mengetahui stabilitas sistem informasi jika menerima akses pengguna yang melebihi rata-rata.
11. *Memori volatile* adalah memori yang akan kehilangan data jika tidak ada arus listrik.
12. *Cookies* adalah informasi yang disimpan dalam komputer pengguna oleh web browser ketika mengakses suatu website yang dapat digunakan untuk mengenali kembali pengguna yang bersangkutan ketika melakukan akses berikutnya.
13. *Database* atau basis data adalah kumpulan dari berbagai jenis data yang disusun secara sistematis dan terstruktur berdasarkan metode tertentu sesuai kaidah teknologi informasi, dan merupakan dasar penyusunan informasi.
14. *File attachment* adalah file yang ikut disertakan dalam sebuah email sebagai lampiran.
15. *Social engineering* adalah teknik yang digunakan seseorang yang tidak berhak untuk memperoleh hak akses terhadap suatu sistem komputer dari orang yang berhak melalui telpon, email, tatap muka, dan sebagainya.
16. *File sharing* adalah tindakan yang dilakukan sehingga file yang terdapat dalam sebuah komputer dapat diakses dari komputer lain.
17. *System Administrator* adalah orang yang bertanggung jawab terhadap perencanaan, pengaturan dan pemeliharaan sistem komputer atau jaringan komputer sehigga dapat digunakan dengan baik oleh pengguna.
18. *Access Control* adalah suatu proses untuk mengatur / mengontrol siapa saja yang berhak mengakses

suatu resource-rosource tertentu yang terdapat di dalam sebuah sistem.

19. *Remote Management* adalah fitur yang memungkinkan seseorang untuk melakukan kendali dan penyesuaian pengaturan dari lokasi manapun.
20. *Remote Access* adalah kemampuan untuk mengakses komputer dari jarak jauh.
21. *Secure Socket Layers (SSL)* adalah teknologi keamanan internet yang memungkinkan untuk melakukan enkripsi terhadap data yang akan ditransmisikan.

BAB II
STANDAR OPERASIONAL DAN PROSEDUR

Pasal 2

Maksud dan tujuan diterbitkannya Standar Operasional dan Prosedur Manajemen Pengamanan Informasi Digital di Lingkungan Pemerintah Daerah adalah untuk dijadikan pedoman dan acuan oleh setiap SKPD di Pemerintah Daerah dalam menggunakan dan mengelola informasi digital untuk mendukung pelaksanaan *e-Government* yang efektif dan efisien dalam rangka meningkatkan pelayanan kepada masyarakat umum.

Pasal 3

Ruang lingkup Pedoman Standar Operasional dan Prosedur Manajemen Pengamanan Informasi Digital di Lingkungan Pemerintah Daerah adalah untuk :

1. penggunaan perangkat keras dan perangkat lunak;
2. pengaturan hak akses terhadap informasi;
3. pengelolaan sumber daya manusia;
4. pengelolaan informasi dan dokumen.

Pasal 4

(1) Manajemen pengaman informasi digital di lingkungan Pemerintah Daerah harus memperhatikan dan mempertimbangkan aspek-aspek berikut :

a. Asas Manfaat
Mampu dimanfaatkan seoptimal mungkin dan dapat menyajikan informasi yang bermanfaat dalam memperlancar pelaksanaan tugas.

b. Asas Keamanan dan Keandalan
Menjamin keamanan serta keadaan informasi yang diolah, disimpan dan disajikan.

c. Asas Efektif dan Efisien
Menunjang keberhasilan pelaksanaan tugas, baik tugas pokok maupun tugas penunjang secara efektif dan efisien.

d. Asas Keterpaduan
Merupakan satu kesatuan / keterpaduan dari berbagai kepentingan secara serasi dan proposional.

e. Asas Integrasi
Mampu memadukan / mempersatukan semua informasi strategis sebagai bahan pertimbangan dalam keputusan bagi pimpinan.

f. Asas Otorisasi
Mampu menjaga keabsahan hak milik atas penyajian informasi sesuai dengan kewenangan masing-masing.

(2) Penggunaan perangkat teknologi informasi yang portable (mudah dibawa) di lingkungan Pemerintah Daerah dibatasi dengan aturan-aturan untuk mencegah terjadinya kebocoran informasi sensitif milik Pemerintah Daerah.

(3) Akses terhadap informasi milik Pemerintah Daerah diatur dengan *access control* untuk mencegah terjadinya akses ilegal dan penyalahgunaan informasi yang merugikan kepentingan pemerintah dan masyarakat.

(4) Perlindungan terhadap aset informasi milik Pemerintah Daerah dilakukan dengan memperhatikan asas :

a. *confidentiality* (kerahasiaan) yang menjamin bahwa informasi hanya dapat diakses oleh yang berwenang;

b. *integrity* (*integritas*) yang menjamin bahwa *informasi* hanya dapat *diubah* oleh yang berwenang;

c. *availability* (ketersediaan) yang menjamin bahwa informasi dapat selalu tersedia *untuk* diakses oleh yang berwenang.

(5) Pemerintah Daerah menugaskan dan memberikan pelatihan kepada beberapa karyawannya agar memiliki kualifikasi cukup untuk mengelola perangkat teknologi informasi dan komunikasi baik perangkat keras maupun perangkat lunak.

(6) Semua karyawan Pemerintah Daerah memiliki tanggung jawab untuk ikut serta melindungi dan memelihara keamanan informasi milik Pemerintah Daerah.

(7) Karyawan Pemerintah Daerah yang diberi tugas dan tanggung jawab untuk mengelola informasi milik Pemerintah Daerah wajib melakukan *backup* secara berkala untuk menjaga keberlangsungan operasional perangkat teknologi informasi dan komunikasi jika terjadi kerusakan maupun bencana.

(8) Setiap perangkat teknologi informasi dan komunikasi milik Pemerintah Daerah memiliki dokumentasi serta petunjuk operasional yang memadai.

Pasal 5

(1) Hanya karyawan Pemerintah Daerah yang boleh menggunakan *removable* media untuk melakukan transfer data dari dan ke dalam perangkat teknologi informasi Pemerintah Daerah.

(2) Pekerjaan perbaikan dan pemeliharaan perangkat keras yang tidak dilakukan sendiri oleh Pemerintah Daerah hanya boleh diserahkan kepada pihak ketiga (rekanan) yang sudah ditunjuk secara resmi oleh Pemerintah Daerah.

(3) Penggunaan komputer portable (laptop) sebagai komputer kerja oleh karyawan Pemerintah Daerah harus atas sepengetahuan pejabat yang berwenang.

(4) Karyawan Pemerintah Daerah yang menggunakan komputer portable (laptop) sebagai komputer kerja bertangungjawab atas kerahasiaan informasi milik Pemerintah Daerah yang terdapat dalam perangkat tersebut.

(5) Pemindahan perangkat keras milik Pemerintah Daerah ke lokasi di luar lingkungan Pemerintah Daerah harus mendapat ijin dan atau pengawasan dari pejabat yang berwenang atau karyawan Pemerintah Daerah yang diberi wewenang.

(6) Removable media yang berisi informasi penting dan rahasia harus disimpan dalam tempat penyimpanan yang aman dan terkunci serta tahan api.

(7) Semua perangkat penyimpanan data digital milik Pemerintah Daerah hanya boleh dimusnahkan atas ijin dari pejabat yang berwenang.

(8) Karyawan Pemerintah Daerah yang bekerja dengan komputer harus memastikan bahwa layar komputer kerja dalam keadaan kosong dan terkunci ketika ditinggalkan.

Pasal 6

(1) Semua sistem informasi milik Pemerintah Daerah harus memiliki fitur access control yang mampu melakukan pembatasan akses informasi oleh pengguna yang mana pengelompokan pengguna ditentukan oleh kebijakan Pemerintah Daerah.

(2) Semua sistem informasi milik Pemerintah Daerah harus dilengkapi dengan fitur yang mengharuskan user untuk menggunakan password yang panjangnya minimal 8 (delapan) karakter.

(3) Akses terhadap sistem informasi dan dokumen milik Pemerintah Daerah hanya boleh dilakukan oleh pengguna yang diberi wewenang.

(4) Semua karyawan Pemerintah Daerah yang memiliki akses terhadap sistem informasi milik Pemerintah Daerah wajib menjaga kerahasiaan akun dan password yang dipercayakan kepadanya.

(5) Semua karyawan Pemerintah Daerah yang memiliki akses terhadap sistem informasi milik Pemerintah Daerah wajib melakukan perubahan password secara berkala.

(6) Instalasi dan modifikasi perangkat lunak yang terdapat pada komputer milik Pemerintah Daerah hanya boleh dilakukan oleh petugas yang berwenang atau oleh pihak lain atas seijin Pemerintah Daerah dan pengaturannya merujuk kepada SOP pengelolaan perangkat lunak dan pengembangan aplikasi sistem informasi dan komunikasi SKPD.

(7) Akses fisik terhadap komputer milik Pemerintah Daerah hanya boleh dilakukan oleh karyawan Pemerintah Daerah.

(8) Akses terhadap sistem informasi Pemerintah Daerah harus dicatat dalam file log dan dimonitor untuk mendeteksi terjadinya penyalahgunaan sistem informasi serta untuk evaluasi terhadap kebijakan pengelompokan access control.

(9) Karyawan Pemerintah Daerah yang ketugasannya sudah tidak lagi menggunakan suatu sistem informasi harus segera dihapus akunnya dari sistem informasi tersebut.

(10) Akses internet dari dalam jaringan komputer Pemerintah Daerah diatur dengan perangkat yang dapat melakukan filterisasi terhadap informasi yang dilarang oleh Pemerintah Daerah.

(11) Akses internet dari dan ke jaringan komputer Pemerintah Daerah dibatasi dengan firewall yang pengaturannya merujuk kepada SOP pengembangan dan pemeliharaan infrastruktur jaringan Pemerintah Daerah.

(12) Remote access kedalam jaringan komputer Pemerintah Daerah hanya boleh dilakukan oleh karyawan Pemerintah Daerah yang diberi wewenang dan atas sepengetahuan pejabat yang berwenang.

(13) Remote management terhadap perangkat jaringan dan server oleh system administrator tidak boleh dilakukan dari sembarang komputer, kecuali dengan ijin dan sepengetahuan pejabat yang berwenang.

(14) Komputer milik Pemerintah Daerah yang fungsi utamanya adalah untuk mengakses sistem

informasi yang berhubungan dengan pelayanan masyarakat tidak diperbolehkan untuk mengakses dan mengambil file dari internet.

Pasal 7

(1) Pemerintah Daerah menugaskan berapa karyawannya sebagai system administrator yang bertanggungjawab untuk memelihara perangkat keras dan perangkat lunak teknologi informasi dan komunikasi.

(2) Komputer milik Pemerintah Daerah yang fungsi utamanya adalah untuk mengakses sistem informasi yang berhubungan dengan pelayanan masyarakat harus dilengkapi dengan antivirus diupdate/diperbaharui secara berkala.

(3) Pendistribusian informasi milik Pemerintah Daerah dalam bentuk file harus atas sepengetahuan pejabat yang berwenang.

(4) Pendistribusian informasi yang bersifat rahasia harus dilindungi dengan enkripsi dan digital signature.

(5) File yang berasal dari email attachment tidak boleh dibuka sebelum discan dengan antivirus.

(6) Karyawan Pemerintah Daerah yang memiliki akun email di server email Pemerintah Daerah wajib menjaga agar akunnya tidak mengalami overquota.

(7) Karyawan Pemerintah Daerah yang menerima email dari pihak ketiga dan dicurigai sebagai email sampah tidak diperkenankan untuk membuka email tersebut.

(8) Pemerintah Daerah menugaskan beberapa karyawannya untuk bertanggungjawab dan melakukan pemeliharaan terhadap informasi yang ditampilkan dalam situs resmi Pemerintah Daerah.

(9) File yang tidak dikenal asal-usulnya tidak boleh dibuka dengan komputer milik Pemerintah Daerah.

(10) Pemerintah Daerah menugaskan beberapa karyawannya untuk bertanggungjawab dan melakukan pemeliharaan terhadap database milik Pemerintah Daerah.

(11) Modifikasi terhadap database yang tidak melalui aplikasi sistem informasi harus atas sepengetahuan pejabat yang berwenang.

(12) Removable media di lingkungan Pemerintah Daerah hanya boleh digunakan oleh karyawan yang diberi ijin dan atas sepengetahuan pejabat yang berwenang.

(13) Informasi yang disimpan dalam sistem informasi milik Pemerintah Daerah memiliki retensi yang sesuai dengan pedoman kearsipan pada Pemerintah Daerah.

(14) Pembuatan database baru harus melalui pengecekan untuk memastikan bahwa dapat bekerja dengan baik sebelum digunakan untuk menyimpan data yang sesungguhnya dan digunakan dalam operasional.

(15) File harus disimpan dengan nama yang mencerminkan isi file.

(16) Klasifikasi kerahasiaan dan kepemilikan dokumen harus dicantumkan dalam header atau footer dokumen tersebut.

(17) Recycle bin dan file temporer dalam komputer milik Pemerintah Daerah harus dihapus setidaknya 1 (satu) minggu sekali.

(18) Karyawan Pemerintah Daerah yang bekerja menggunakan komputer PC dan laptop harus melakukan back up secara berkala terhadap file kerjanya.

(19) System administrator yang bertanggungjawab terhadap database harus melakukan backup secara berkala dalam removable media dan storage server.

(20) System administrator yang bertanggungjawab terhadap database harus melakukan pengujian terhadap backup database dan memastikan bahwa backup tersebut tidak cacat.

(21) Karyawan Pemerintah Daerah yang sehari-harinya bekerja dengan file harus melakukan backup terhadap file kerjanya secara berkala dalam removable media.

(22) Backup dalam removable media harus dienkripsi dan disimpan di tempat yang aman dan terpercaya di luar gedung milik Pemerintah Daerah seperti misalnya safe deposit box di bank.

(23) Semua informasi digital yang dialihmediakan kedalam bentuk cetakan (hardcopy) untuk diberikan kepada pihak ketiga harus atas sepengetahuan pejabat yang berwenang.

(24) File yang berisi informasi rahasia harus dilindungi dengan password dan disimpan dalam format yang tidak dapat diubah tanpa kewenangan yang cukup.

(25) Tanggungjawab pengelolaan data dan informasi yang dikategorikan sensitif oleh Pemerintah Daerah harus ditangani oleh 2 (dua) orang karyawan dan perubahan yang dilakukan oleh salah satunya harus diketahui oleh yang lain.

Pasal 8

(1) Pembuatan sistem informasi yang tidak dilakukan secara swadaya oleh Pemerintah Daerah hanya boleh diserahkan kepada pihak ketiga (rekanan) yang sudah ditunjuk secara resmi oleh Pemerintah Daerah atau Pemerintah Pusat.

(2) Kode sumber yang terdapat pada semua sistem informasi yang dibuat untuk Pemerintah Daerah tidak boleh diberikan kepada pihak lain.

(3) Sistem Informasi yang dibuat untuk Pemerintah Daerah harus mengalami pengujian dan dinyatakan lulus oleh pejabat yang berwenang sebelum digunakan dalam operasional sehari-hari di lingkungan Pemerintah Daerah.

(4) Pengujian terhadap sistem informasi baru yang menggunakan data riil milik Pemerintah Daerah harus dilakukan dengan pengawasan oleh karyawan Pemerintah Daerah yang ditunjuk oleh pejabat yang berwenang.

(5) Pengujian terhadap sistem informasi untuk Pemerintah Daerah meliputi peak *loading* dan *stress testing*.

(6) Sebelum suatu sistem informasi Pemerintah Daerah digunakan, akun dan *password* yang dipakai untuk pengujian harus dihapus.

(7) Sebelum digunakan sepenuhnya, sistem informasi yang mengalami peremajaan maupun sistem informasi baru yang tujuannya untuk menggantikan sistem informasi yang sudah ada, harus digunakan secara paralel dengan sistem informasi yang sudah ada hingga dinyatakan sempurna oleh pejabat yang berwenang.

(8) Sistem Informasi yang dibuat untuk Pemerintah Daerah harus dirancang agar tidak menampilkan

pesan kesalahan yang dapat memperlihatkan desain dan konfigurasi sistem informasi tersebut.

(9) Sistem informasi yang menangani data dan informasi yang dikategorikan sensitif dan rahasia oleh Pemerintah Daerah harus mampu melakukan enkripsi jika data dan informasi tersebut mengalami kondisi-kondisi sebagai berikut :

a. tersimpan dalam file atau database;

b. tersimpan dalam registry sistem operasi;

c. tersimpan dalam memori volatile;

d. terkirim ke komputer lain;

e. tersimpan sebagai cookies.

(10) Sistem informasi yang mengalami peremajaan maupun sistem informasi baru harus memiliki dokumentasi penggunaan dan pemeliharaan teknis.

(11) Sistem informasi yang dibuat dalam bentuk website dan terhubung dengan internet harus mendukung standar *http protocol* yang sudah dilengkapi teknologi *Secure Socket Layers (SSL)* atau *https*.

Pasal 9

(1) System administrator secara berkala mendapatkan pelatihan untuk meningkatkan pengetahuan dan kemampuan sesuai dengan bidang yang ditanganinya.

(2) Pelatihan harus diberikan kepada karyawan Pemerintah Daerah yang akan menggunakan dan melakukan pemeliharaan teknis terhadap sistem informasi yang baru.

(3) Karyawan Pemerintah Daerah yang sehari-harinya bekerja dengan perangkat teknologi informasi secara berkala mendapatkan pelatihan mengenai pemahaman terhadap keamanan informasi yang meliputi antara lain :

a. pemahaman agar mampu mengamankan laptop dan informasi yang terdapat di dalamnya;

b. pemahaman agar tidak meggunakan password yang berkaitan dengan data pribadi;

c. pemahaman agar tidak menyimpan password di sembarang tempat;

d. pengetahuan tentang informasi yang dianggap sensitif dan harus dijaga kerahasiaannya;

e. pengetahuan tentang bahaya yang dapat ditimbulkan oleh file attachment dalam email yang dikirimkan oleh pihak yang tidak dikenal;

f. pemahaman agar mampu mengindari ancaman keamanan dari social engineering;

g. pengetahuan tentang bahaya yang dapat ditimbulkan oleh instalasi perangkat lunak yang tidak dikenal pada komputer kerja;

h. pengetahuan tentang bahaya yang dapat ditimbulkan dengan mengaktifkan file sharing pada komputer kerja tanpa seijin system administrator.

(4) Karyawan Pemerintah Daerah yang sehari-harinya bekerja dengan perangkat teknologi informasi milik Pemerintah Daerah tidak diperbolehkan melakukan perubahan terhadap konfigurasi perangkat lunak baik sistem operasi maupun program aplikasi yang terdapat pada komputer kerjanya.

(5) Tindakan yang harus dilakukan oleh karyawan Pemerintah Daerah dalam menangani dan merespon insiden yang mengancam keamanan informasi antara lain :

a. mengisolir komputer yang dicurigai mengalami masalah dengan memutus kabel jaringan dan tidak melakukan copy data dari atau ke komputer tersebut melalui media apa pun.

b. segera melaporkannya pada system administrator.

BAB III

KETENTUAN PENUTUTUP

Pasal 10

Peraturan Bupati ini mulai berlaku pada tanggal diundangkan.

Agar setiap orang mengetahuinya, memerintahkan pengundangan Peraturan Bupati ini dengan penempatannya dalam Berita Daerah Kabupaten Buleleng.

Ditetapkan di Singaraja
pada tanggal 22 Nopember 2017

BUPATI BULELENG,

PUTU AGUS SURADNYANA

Diundangkan di Singaraja
pada tanggal 22 Nopember 2017
SEKTRETARIS DAERAH KABUPATEN BULELENG,

DEWA KETUT PUSPAKA

BERITA DAERAH KABUPATEN BULELENG TAHUN 2017 NOMOR 79