KOMISI PEMILIHAN UMUM
REPUBLIK INDONESIA

Yth. 1. Para Deputi dan Inspektur Utama Setjen KPU RI;
2. Para Kepala Biro, Kepala Pusat, Inspektur Setjen KPU RI;
3. Ketua dan Anggota KPU Provinsi/KIP Aceh;
4. Sekretaris KPU Provinsi/KIP Aceh;
5. Ketua dan Anggota KPU/KIP Kabupaten/Kota;
6. Sekretaris KPU/KIP Kabupaten/Kota;

di -
Tempat

SURAT EDARAN
NOMOR: 3 TAHUN 2022
TENTANG
PENERAPAN KEBIJAKAN SISTEM MANAJEMEN KEAMANAN INFORMASI

A. Latar Belakang

Sertifikasi ISO 27001 – *Information Security Management System (ISMS)* atau yang di Indonesia biasa disebut sebagai SMKI (Sistem Manajemen Keamanan Informasi) adalah sebuah rencana manajemen yang menspesifikasikan kebutuhan-kebutuhan yang diperlukan untuk implementasi kontrol keamanan yang telah disesuaikan dengan kebutuhan organisasi. SMKI didesain untuk melindungi aset informasi dari seluruh gangguan keamanan.

Sistem manajemen keamanan informasi menjaga kerahasiaan, integritas dan ketersediaan informasi dengan penerapan suatu proses manajemen risiko dan memberikan keyakinan kepada pihak yang memerlukannya bahwa semua risiko ditangani dengan baik. Sistem manajemen keamanan informasi merupakan bagian dari dan terintegrasi dengan proses-proses organisasi dan keseluruhan struktur manajemen dan keamanan informasi dipertimbangkan dalam proses-proses disain, sistem informasi, dan pengendalian. Diharapkan bahwa implementasi sistem manajemen keamanan informasi akan disesuaikan sejalan dengan kebutuhan organisasi. Standar internasional ini dapat digunakan oleh pihak internal dan eksternal untuk menguji kemampuan organisasi dalam memenuhi persyaratan keamanan informasi yang ditetapkan oleh organisasi tersebut.

1. Kerahasiaan – memastikan bahwa informasi dapat diakses hanya untuk mereka yang memiliki otoritas untuk mempunyai akses.
2. Integritas – melindungi kelengkapan dan ketelitian informasi dan memproses metoda.

3. Ketersediaan – memastikan bahwa para pengguna yang memiliki otoritas mempunyai akses ke informasi dan berhubungan dengan aset ketika diperlukan.

B. Maksud dan Tujuan

1. Maksud dari kegiatan ini adalah agar masing-masing satuan kerja mampu menerapkan keamanan informasi dan kebersihan siber secara efektif , efisien, dan konsisten ;
2. Tujuan dari kegiatan ini adalah untuk memberikan kerangka kerja standar tentang bagaimana satuan kerja (satker) harus mengelola informasi dan datanya.

C. Ruang Lingkup

1. KPU Provinsi/KIP Aceh
2. KPU/KIP Kabupaten/Kota

D. Dasar

1. Undang-Undang Nomor 1 Tahun 2015 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 1 Tahun 2014 tentang Pemilihan Gubernur, Bupati dan Walikota Menjadi Undang-Undang (Lembaran Negara Republik Indonesia Tahun 2015 Nomor 23, Tambahan Lembaran Negara Republik Indonesia Nomor 5656) sebagaimana telah beberapa kali diubah terakhir dengan Undang-Undang Nomor 6 Tahun 2020 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 2 Tahun 2020 tentang Perubahan Ketiga atas Undang-Undang Nomor 1 Tahun 2015 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 1 Tahun 2014 tentang Pemilihan Gubernur, Bupati dan Walikota Menjadi Undang-Undang Menjadi UndangUndang (Lembaran Negara Republik Indonesia Tahun 2020 Nomor 193, Tambahan Lembaran Negara Republik Indonesia Nomor 6547);
2. Undang-undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251,Tambahan Lembaran Negara Republik Indonesia Nomor 5952);
3. Undang-Undang Nomor 7 Tahun 2017 tentang Pemilihan Umum (Lembaran Negara Republik Indonesia Tahun 2017 Nomor 182, Tambahan Lembaran Negara Republik Indonesia Nomor 6109);
4. Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185, Tambahan Lembaran Negara Republik Indonesia Nomor 6400);
5. Peraturan Pemerintah No 82 tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik ;
6. Peraturan Presiden nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik ;
7. SNI ISO/IEC 27001:2013 Sistem Manajemen Keamanan Informasi ;
8. ISO 31000:2018 Risk Management – Prinsip Prinsip Manajemen Risiko.

E. Isi Edaran

Dalam rangka penerapan kebijakan Sistem Manajemen Keamanan Informasi *(SMKI)* berdasarkan standar ISO/IEC 27001 : 2013, bersama ini kami meminta kepada seluruh KPU Provinsi/ KIP Aceh dan KPU/ KIP Kabupaten/Kota, untuk melakukan hal – hal sebagai berikut :

1. Personil di lingkungan KPU Provinsi/ KIP Aceh dan KPU/ KIP Kabupaten/Kota yang menggunakan aset informasi milik satuan kerja (satker) harus bertanggung jawab terhadap penggunaan aset informasi yang sesuai dengan prinsip keamanan informasi, yaitu :
   a. Menggunakan aset informasi dengan benar untuk menghindari risiko kehilangan atau kerusakan;
   b. Menjaga kerahasiaan aset informasi dan informasi yang tersimpan;
   c. Melindungi aset informasi terhadap akses yang tidak sah atau tidak memiliki otoritas; dan
   d. Tidak menggunakan aset informasi untuk kepentingan yang bertentangan dengan etika, peraturan, dan hukum yang berlaku serta merugikan satuan kerja (satker) di masing-masing daerah.
2. Semua aset informasi harus dilakukan identifikasi dan inventarisasi;
3. Semua aset informasi harus ditetapkan penanggungjawabnya;
4. Semua aset informasi hanya boleh digunakan untuk kepentingan satuan kerja (satker);
5. Informasi pada satuan kerja (satker) harus diklasifikasikan sesuai dengan persyaratan hukum, nilai, kritikalitas, dan kerentanan terhadap pengungkapan atau pemodifikasian yang tidak sah. Klasifikasi informasi terbagi menjadi 3 kelas, yaitu : Rahasia, Terbatas dan Publik.
6. Media yang dapat dipindahkan *(removable media)* seperti CD, *Portable Harddisk*, *Flash Disk*, dan *Tape Backup*, yang menyimpan informasi rahasia harus disimpan di lokasi yang aman, yaitu di lokasi yang telah ditentukan;
7. *Flash Disk* tidak boleh digunakan untuk menyimpan informasi rahasia secara permanen. Jika *flash disk* digunakan untuk pertukaran informasi rahasia, maka informasi rahasia tersebut harus segera dihapus setelah pertukaran dilakukan;
8. Jika aset informasi akan dipindahtangankan keluar dari lingkungan satuan kerja (satker), maka informasi yang disimpan harus diformat atau dihapus dengan metode yang aman;
9. Media yang dapat dipindahkan *(removable media)* yang telah dan atau tidak dapat dibaca oleh sistem komputer atau mengalami kerusakan harus dihancurkan secara fisik;
10. KPU Provinsi/ KIP Aceh dan KPU/ KIP Kabupaten/Kota wajib mengganti kata sandi *(password)* email secara berkala minimal **1 kali setiap 3 bulan**;
11. Seluruh *Administrator CPanel* Website dan *Administrator* pengelola website KPU Provinsi/ KIP Aceh dan KPU/ KIP Kabupaten/Kota wajib mengganti kata sandi *(password)* secara berkala minimal **1 kali setiap bulan**.
12. Pembuatan kata sandi *(password)* harus terdiri dari :

a. Kombinasi antara huruf kapital, huruf kecil, dan karakter khusus;
b. Sulit ditebak, tetapi mudah diingat oleh pengguna;
c. Bukan merupakan kata atau akronim dari nama sendiri atau kerabat, tanggal lahir, alamat rumah, dan sebagainya;
d. Tidak sama dengan nama akun pengguna, baik sebagian atau seluruhnya; dan
e. Tidak sama dengan 3 kata sandi *(password)* terakhir yang telah diganti.

13. Pengguna hak akses tidak boleh membagi atau memberitahukan kata sandi *(password);*
14. Kata sandi *(password)* tidak boleh dituliskan di tempat yang mudah terlihat;
15. Kata sandi *(password)* default harus segera diganti.
16. Hak akses semua pengguna harus dilakukan peninjauan secara berkala;
17. Hak akses pengguna yang telah tidak berwenang harus segera ditutup atau dihapus;
18. Pengguna hak akses tidak boleh memilih mengingat kata sandi *(remember password)* dalam tampilan *login*;
19. Setiap personil wajib menjaga perangkat (komputer dan gawai) tetap aman dengan melakukan hal-hal sebagai berikut :
    a. Menginstal dan melakukan pembaruan Antivirus;
    b. Memastikan media yang bisa dipindahkan (*removable media*) seperti Flashdisk tetap aman;
    c. Menggunakan aplikasi resmi dan berlisensi;
    d. Menggunakan enkripsi;
    e. Melakukan pencadangan data secara rutin.
20. Selalu mengunci perangkat (komputer dan gawai) jika sedang tidak digunakan;
21. Melakukan pengamanan pada koneksi jaringan internet di lingkungan satuan kerja (satker) dengan melakukan hal – hal sebagai berikut :
    a. Mengaktifkan fungsi *firewall* pada *router*;
    b. Gunakan protokol WPA2 pada kata sandi WiFi.
22. Akses internet WiFi *(wireless)* disediakan kepada pegawai untuk melakukan akses informasi yang berkaitan dengan operasional dan kompetensi dalam pelayanan jasa teknologi;
23. Pemasangan perangkat akses internet WiFi *(wireless)* harus mendapatkan persetujuan dari Kepala Bagian/ Sub Bagian terkait;
24. Pengguna akses internet dilarang melakukan pengunduhan informasi dengan ekstensi **".exe", ".com"**, dan ekstensi lainnya yang dapat dieksekusi karena memiliki risiko terdapat *malware (*perangkat lunak berbahaya);
25. Pengguna pesan elektronik dilarang :
    a. Menghina atau melecehkan orang atau pihak lain;
    b. Melakukan unsur SARA;
    c. Menyebarkan fitnah;
    d. Menyebarkan iklan/ urusan pribadi;
    e. Menyebarkan SPAM;
    f. Menyebarkan *Malware* (Perangkat lunak berbahaya);

g. Mengirim atau menerima lampiran informasi dengan ekstensi **".exe", ".com"**;

26. Pengguna pesan elektronik harus memastikan kebenaran alamat tujuan sebelum melakukan pengiriman pesan dengan memanfaatkan fasilitas peyimpanan alamat tujuan untuk menghindari salah kirim;
27. Pengguna pesan elektronik harus memastikan lampiran *(attachment)* pada pesan elektronik, baik yang dikirim maupun yang diterima, bahwa aman dari *malware* (perangkat lunak berbahaya) dengan melakukan pemindaian terhadap lampiran *(attachment)* terlebih dahulu;
28. Pengguna pesan elektronik dilarang membuka lampiran *(attachment)* jika tidak meminta pengirim untuk melampirkan apapun;
29. Pengguna pesan elektronik dilarang membuka dokumen/tautan yang berasal dari media sosial atau apapun yang tidak berhubungan dengan urusan kedinasan.

Demikian disampaikan untuk menjadi perhatian dan dilaksanakan dengan penuh tanggung jawab. Atas perhatian dan kerjasamanya kami ucapkan terima kasih.

Ditetapkan di Jakarta
Pada tanggal 28 Januari 2022

Ketua Komisi Pemilihan Umum
Republik Indonesia,

Ilham Saputra