SATUAN KERJA SEMENTARA
PELAKSANA KEGIATAN USAHA HULU MINYAK DAN GAS BUMI
(SKMIGAS)

PEDOMAN TATA KERJA

Nomor : 053/SKO0000/2013/SO

TENTANG

PENGELOLAAN TEKNOLOGI INFORMASI KOMUNIKASI pada KONTRAKTOR KONTRAK KERJA SAMA(KKKS)

JAKARTA

KEMENTERIAN ENERGI DAN SUMBER DAYA MINERAL
SATUAN KERJA SEMENTARA
PELAKSANA KEGIATAN USAHA HULU MINYAK DAN GAS BUMI
(SKMIGAS)

SURAT KEPUTUSAN
Nomor: KEP-0008./SKO0000/2013/S0

TENTANG
PEDOMAN TATA KERJA PENGELOLAAN TEKNOLOGI INFORMASI DAN KOMUNIKASI PADA KONTRAKTOR KONTRAK KERJA SAMA

KEPALA SKMIGAS

Menimbang:

a. Bahwa pemanfaatan Teknologi Informasi dan Komunikasi (TIK) oleh Kontraktor Kontrak Kerja Sama (Kontraktor KKS) dapat lebih meningkatkan efisiensi operasional dan dapat menghasilkan informasi yang akurat, yang memungkinkan pengguna informasi dapat mengambil keputusan yang tepat; yang dimana jika pemanfaatan TIK tidak dikelola dengan baik dapat menimbulkan risiko;

b. bahwa TIK yang digunakan Kontraktor merupakan aset yang sangat berharga bagi Negara Republik Indonesia yang dalam hal ini diwakilkan oleh SKMIGAS, untuk itu pemanfaatannya perlu dikelola dengan optimal;

c. bahwa untuk memudahkan pengelolaan TIK diperlukan suatu pedoman yang menyeluruh sebagai acuan bagi Kontraktor KKS dalam pelaksanaan pengelolaan TIK tersebut;

d. bahwa untuk memastikan agar informasi yang dikelola terjaga kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaannya (*availability*) diperlukan suatu pedoman sebagai acuan dan ketentuan dalam pelaksanaan TIK secara efektif dan efisien;

e. bahwa sehubungan dengan pertimbangan sebagaimana dimaksud pada huruf a, huruf b, huruf c, dan huruf d perlu ditetapkan ketentuan yang mengatur tentang tata kelola pemanfaatan aset TIK yang baik oleh Kontraktor dalam peraturan SKMIGAS.

Mengingat:

1. Pasal 5 ayat (2) Undang-Undang Dasar 1945 sebagaimana telah diubah dengan Perubahan Ketiga Undang Undang Dasar 1945;
2. Peraturan Pemerintah Republik Indonesia No. 17 Tahun 1974 tentang Pengawasan Pelaksanaan Eksplorasi dan Eksploitasi Minyak dan Gas Bumi di Daerah Lepas Pantai;
3. Undang-Undang Republik Indonesia Nomor 22 Tahun 2001 tentang Minyak dan Gas Bumi (Lembaran Negara Tahun 2001 Nomor 136, Tambahan Lembaran Negara Nomor 4152);
4. Peraturan Presiden No. 95 Tahun 2012 tentang Pengalihan dan Pelaksanaan Tugas dan Fungsi Kegiatan Usaha Hulu Minyak dan Gas;

5. Keputusan .....

5. Keputusan Menteri Energi dan Sumber Daya Mineral Nomor 3135 W08/MEM/2012 tanggal 13 November 2012 tentang Pengalihan Tugas, Fungsi dan Organisasi dalam Pelaksanaan Kegiatan Usaha Hulu Minyak dan Gas;
6. Keputusan Menteri Energi dan Sumber Daya Mineral Nornor 3136 K/73/MEM/2012 tanggal13 November 2012 yang menetapkan antara lain bahwa Menteri Energi dan Sumber Daya Mineral mengalihkan pelaksanaan tugas, fungsi dan organisasi dari Badan Pelaksana Kegiatan Usaha Hulu Minyak dan Gas Bumi ("BPMIGAS") kepada Satuan Kerja Sementara Pelaksana Kegiatan Usaha Hulu Minyak dan Gas Bumi ("SKSPMIGAS") yang berada di bawah dan bertanggung jawab kepada Menteri Enegi dan Sumber Daya Mineral;
7. Peraturan Menteri Energi dan Sumber Daya Mineral Nomor 01 Tahun 2008 tentang Pedoman Pengusahaan Pertambangan Minyak Bumi Pada Sumur Tua;
8. Peraturan Menteri Energi dan Sumber Daya Mineral Nomor 27 Tahun 2008 tentang kegiatan Usaha Penunjang Minyak dan Gas Bumi;
9. Peraturan Menteri Energi dan Sumber Daya Mineral Nomor 35 Tahun 2008 tentang Tata Cara Penetapan dan Penawaran Wilayah Kerja Minyak dan Gas Bumi;
10. Peraturan Pemerintah Republik Indonesia Nomor 55 Tahun 2009 tentang Perubahan Kedua Atas Peraturan Pemerintah Nomor 35 Tahun 2004 Tentang Kegiatan Usaha Hulu Minyak dan Gas Bumi;Peraturan Pemerintah Republik Indonesia No.79 Tahun 2010 tentang Biaya Operasi yang Dapat Dikembalikan dan Perlakuan Pajak Penghasilan di Bidang Usaha Hulu Minyak dan Gas Bumi;
11. Undang-Undang Republik Indonesia No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

MEMUTUSKAN

Menetapkan :

PERTAMA : Memberlakukan Pedoman Tata Kerja Pengelolaan Teknologi Informasi pada Kontraktor Kontrak Kerja Sama (PTK Pengelolaan TIK pada Kontraktor KKS) untuk seluruh Kontraktor KKS di lingkungan Usaha Hulu Minyak dan Gas Bumi; dimana penerapannya wajib disesuaikan dengan kebijakan, usaha, ukuran dan kompleksitas pemanfaatan TIK.

KEDUA.....

KEDUA : Menugaskan kepada Kepala Divisi Evaluasi, Pelaporan dan Teknologi Informasi sebagai penanggung jawab yang secara berkesinambungan mengadakan penyempurnaan terhadap Pedoman Tata Kerja yang mengatur pemanfaatan TIK di Kontraktor KKS.

Ketentuan lain yang belum diatur atau belum cukup diatur dalam Pedoman Tata Kerja ini akan ditetapkan kemudian dan menjadi satu kesatuan yang tak terpisahkan dengan Pedoman Tata Kerja ini.

Surat Keputusan ini berlaku terhitung mulai tanggal ditetapkan.

Ditetapkan di : Jakarta
Pada tanggal : 10 Januari 2013

Menteri Energi dan Sumber Daya Mineral
selaku
Kepala Satuan Kerja Sementara
Pelaksana Kegiatan Usaha Hulu
Minyak dan Gas Bumi

SATUAN KERJA SEMENTARA PELAKSANA KEGIATAN USAHA HULU MINYAK DAN GAS BUMI
KEMENTERIAN ESDM
KEPALA

Ir. Jero Wacik, S.E.

DAFTAR ISI

BAB I
PENDAHULUAN

A. Latar Belakang

Dalam pelaksanaan kegiatan usaha hulu minyak dan gas bumi, Kontraktor Kontrak Kerja Sama (KKKS) menggunakan fasilitas Teknologi Informasi dan Komunikasi (TIK) untuk menunjang kegiatannya. Penggunaan TIK memiliki dampak yang dapat menimbulkan risiko terhadap terganggunya operasional Perusahaan, reputasi serta kerahasiaan, integritas dan ketersediaan data dan informasi. Untuk memitigasi hal tersebut, diperlukan suatu proses pengendalian dan pengawasan yang dituangkan dalam suatu Pedoman Tata Kerja yang mengatur penerapan TIK dalam kegiatan usaha hulu minyak dan gas bumi.

Oleh karena itu, SKMIGAS sebagai badan hukum yang bertugas sebagai pengawas dan pengendali kegiatan usaha hulu minyak dan gas bumi berdasarkan Peraturan Pemerintah Nomor 42 Tahun 2002, mengeluarkan dan menerapkan pedoman yang terkait penggunaan fasilitas TIK dan Manajemen Risiko TIK oleh KKKS dalam kegiatan usaha hulu minyak dan gas bumi.

B. Maksud dan Tujuan

Pedoman Tata Kerja ini dimaksudkan untuk memberikan suatu pedoman bagi KKKS dalam pengelolaan sumber daya TIK untuk kegiatan usaha hulu minyak dan gas bumi serta menciptakan keselarasan dengan kerangka tata kelola yang akan dituangkan dalam Pedoman Tata Kerja ini. Implementasi atas PTK ini dan pengendalian yang tercakup di dalamnya harus disesuaikan dengan kebutuhan, proses TIK, serta karakteristik risiko KKKS.

Pedoman Tata Kerja ini bertujuan untuk optimalisasi sumber daya TIK yang digunakan atau dimiliki KKKS dalam kegiatan usaha hulu minyak dan gas bumi yang terkait dengan kerahasiaan, integritas, dan ketersediaan data atau informasi.

C. Ruang Lingkup

Pedoman Tata Kerja ini mengatur keseluruhan aspek kegiatan pengelolaan TIK di Kontraktor Kontrak Kerja Sama (KKKS). Ruang lingkup Pedoman Tata Kerja ini mencakup seluruh kegiatan yang menggunakan fasilitas TIK, baik dalam lingkup strategis, administratif, dan operasional di lapangan yang terbagi atas penemuan cadangan (*finding*), pengembangan lapangan (*development*) dan produksi (*lifting*).

D. Dasar Hukum

1. Peraturan Presiden No. 95 Tahun 2012 tentang Pengalihan dan Pelaksanaan Tugas dan Fungsi Kegiatan Usaha Hulu Minyak dan Gas;
2. Peraturan Pemerintah Nomor 35 Tahun 2004 Tentang Kegiatan Usaha Hulu Minyak dan Gas Bumi sebagaimana terakhir diubah dengan Peraturan Pemerintah Republik Indonesia Nomor 55 Tahun 2009 tentang Perubahan Kedua atas Peraturan Pemerintah Nomor 35 Tahun 2004 tentang Kegiatan Usaha Hulu Minyak dan Gas Bumi;
3. *Production Sharing Contract* (PSC).

E. Referensi Hukum

1. Undang-Undang Republik Indonesia Nomor 12 Tahun 1997 tentang Perubahan Atas Undang-Undang Nomor 6 tahun 1982 tentang Hak Cipta sebagaimana telah diubah dengan Undang-Undang Nomor 7 Tahun 1987;
2. Undang-Undang Republik Indonesia Nomor 14 Tahun 2001 tentang Paten;
3. Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik;
4. Peraturan Pemerintah Republik Indonesia Nomor 17 Tahun 1974 tentang Pengawasan Pelaksanaan Eksplorasi dan Eksploitasi Minyak dan Gas Bumi di Daerah Lepas Pantai;
5. Peraturan Pemerintah Republik Indonesia Nomor 79 Tahun 2010 tentang Biaya Operasi yang Dapat Dikembalikan dan Perlakuan Pajak Penghasilan di Bidang Usaha Hulu Minyak dan Gas Bumi;
6. Instruksi Presiden No. 17 tahun 2011 tentang Aksi Pencegahan dan Pemberantasan Korupsi tahun 2012;

7. Peraturan Menteri Energi dan Sumber Daya Mineral Nomor 27 Tahun 2006 tentang Pengelolaan dan Pemanfaatan Data yang Diperoleh dari Survey Umum, Eksplorasi dan Eksploitasi Minyak dan Gas Bumi;
8. Peraturan Menteri Energi dan Sumber Daya Mineral Nomor 27 Tahun 2008 tentang Kegiatan Usaha Penunjang Minyak dan Gas Bumi;
9. Peraturan Menteri Energi dan Sumber Daya Mineral Nomor 35 Tahun 2008 tentang Tata Cara Penetapan dan Penawaran Wilayah Kerja Minyak dan Gas Bumi.

F. Pedoman Tata Kerja Terkait

1. Pedoman Tata Kerja No. 007 tentang Pedoman Pengelolaan Rantai Suplai Kontraktor Kontrak Kerja Sama;
2. Pedoman Tata Kerja No.018 Pengelolaan tentang Sumber Daya Manusia Kontraktor Kontrak Kerja Sama;
3. Petunjuk Umum No. 0051 tentang Permohonan Perijinan Sarana Komunikasi Radio Kontraktor Kontrak Kerja Sama;
4. Petunjuk Teknis Pedoman Tata Kerja Telemetering dan Telecontroling SKMIGAS – Kontraktor KKS;
5. Pedoman Tata Kerja No. XXX tentang Sistem Operasi Terpadu sebagai turunan dari PTK ini.

G. Pengertian Istilah

1. ***Agility*** TIK adalah keadaan atau perkembangan TIK yang cepat, radikal, dan kompetitif.
2. **Akses** adalah jalan masuk, yaitu suatu usaha untuk membuka suatu saluran komunikasi dengan perangkat *hardware* atau *software* tertentu, seperti modem yang digunakan untuk membuka akses internet.
3. **Audit *ad hoc*** dikenal juga sebagai audit khusus (*special audit*), yaitu audit non-reguler yang dapat dilakukan sewaktu-waktu untuk memeriksa objek yang dipandang bermasalah.
4. ***Auditee*** adalah orang atau organisasi yang diaudit.
5. **Auditor** adalah orang atau organisasi yang melakukan audit.

6. ***Backup*** adalah salinan dari dokumen asli atau cadangan dari mesin utama yang dapat digunakan apabila terjadi gangguan pada mesin utama.
7. ***Bandwidth*** adalah besaran lalu lintas data yang diperbolehkan melalui jaringan.
8. ***Business Impact Analysis* (BIA)** adalah proses untuk memastikan akibat yang ditimbulkan dari ketidaktersediaannya dukungan semua *resource*. Pada fase ini mencakup identifikasi beragam kejadian yang dapat mengakibatkan kelangsungan kegiatan operasional dan *financial*, sumber daya manusia dan dampak terhadap reputasi perusahaan. BIA merupakan langkah kritikal dalam pengembangan DRP.
9. **Cetak Biru TIK (ICT *Blueprint*)** adalah dokumen yang menggambarkan visi dan misi TIK KKKS yang merupakan acuan dalam pemanfaatan TIK untuk memenuhi kebutuhan bisnis dan mendukung rencana bisnis.
10. ***Computing Infrastructure*** adalah infrastruktur TIK yang digunakan untuk mendukung proses komputasi.
11. ***Data Center* (DC)** adalah fasilitas utama pemerosesan data KKKS yang terdiri dari *hardware* dan *software* untuk mendukung kegiatan operasional KKKS secara berkesinambungan.
12. **Data** menurut Peraturan Pemerintah Nomor 35 Tahun 2004 adalah semua fakta, petunjuk, indikasi, dan informasi baik dalam bentuk tulisan (karakter), angka (digital), gambar (analog), media magnetik, dokumen, percontohan batuan, fluida, dan bentuk lain yang didapat dari hasil survey umum, eksplorasi dan eksploitasi minyak dan gas bumi.
13. ***Database*** (basis data) adalah representasi kumpulan fakta yang saling berhubungan disimpan secara bersama sedemikian rupa dan tanpa pengulangan (redundansi) yang tidak perlu untuk memenuhi berbagai kebutuhan.
14. ***Disaster Recovery Center* (DRC)** adalah suatu lokasi alternatif yang dapat digunakan pada saat Pusat Data (*Data Center*) mengalami gangguan atau tidak dapat berfungsi akibat adanya *disaster* antara lain karena tidak adanya aliran listrik ke ruang komputer, kebakaran, ledakan atau kerusakan pada komputer, yang digunakan sementara waktu selama dilakukannya pemulihan Pusat Data (*Data Center*) KKKS untuk menjaga kelangsungan kegiatan usaha (*business continuity*).
15. ***Disaster Recovery Plan* (DRP)** adalah dokumen yang berisikan rencana dan langkah-langkah mendapatkan kembali akses data, *hardware* dan *software* yang

diperlukan agar KKKS dapat menjalankan kegiatan operasional bisnis yang kritikal setelah adanya *disaster*.

16. ***Disposal*** adalah proses penghancuran/penghapusan sistem, aplikasi, aset atau proses dari lingkungan produksi karena sudah tidak digunakan.
17. ***Downtime*** adalah lamanya sistem tidak dapat berfungsi dan digunakan oleh pengguna karena adanya gangguan *hardware, software* dan komunikasi.
18. **Enkripsi** adalah alat untuk mencapai keamanan data dengan menerjemahkan data tersebut menggunakan sebuah *key* (*password*).
19. ***Firewall*** adalah peralatan untuk menjaga keamanan jaringan yang melakukan pengawasan dan penyeleksian atas lalu lintas data/informasi melalui jaringan serta memisahkan jaringan pribadi dan publik.
20. ***Full System Back up*** adalah sistem *backup* yang mencakup keseluruhan sistem yang digunakan.
21. ***Hardcopy*** adalah salinan data/informasi komputer dalam bentuk tercetak atau dikenal dengan *printout*.
22. ***Hardening*** adalah proses/metode untuk mengamankan sistem dari berbagai ancaman atau gangguan.
23. ***Informasi*** adalah data yang telah diolah dengan metodologi tertentu sehingga dapat dipahami dan digunakan untuk suatu tujuan tertentu.
24. ***Interface/Integration Testing*** adalah uji coba oleh *Quality Assurance (QA)* dan pengguna akhir untuk menguji antar muka/*interface* komponen perangkat lunak yang terintegrasi, termasuk keterhubungannya dengan sistem lain.
25. **Integritas (*Integrity*)** adalah prinsip pengamanan informasi yang menjamin keutuhan dan keaslian data dan informasi, dimana data dan informasi tidak berubah tanpa izin dari pihak yang memiliki otorisasi dengan tujuan untuk memastikan keakuratan dan kelengkapan informasi tersebut.
26. ***Interoperability*** adalah:
    a. Kemampuan perangkat lunak atau perangkat keras pada berbagai jenis mesin dari banyak vendor untuk saling berkomunikasi;
    b. Kemampuan untuk saling bertukar dan menggunakan informasi (biasanya dalam suatu jaringan besar yang terdiri beberapa jaringan lokal yang bervariasi).

27. ***IT Librarian*** adalah pihak yang bertugas melakukan inventarisasi dan menyimpan seluruh *software*, data, dan informasi dalam berbagai media, serta *copy* dari seluruh kebijakan dan prosedur.
28. ***IT Library*** adalah kumpulan perangkat lunak atau data yang memiliki fungsi tertentu dan disimpan serta siap untuk digunakan.
29. **Kerahasiaan (*Confidentiality*)** adalah prinsip pengamanan informasi yang menjamin terjaganya informasi dari kebocoran dimana akses terhadap data dan informasi hanya dapat dilakukan oleh pihak yang memiliki otorisasi.
30. **Ketersediaan (*Availability*)** adalah prinsip pengamanan informasi yang menjamin diperolehnya informasi yang benar dan dapat diakses bila dibutuhkan oleh pihak yang memiliki otorisasi.
31. **Kontraktor Kontrak Kerja Sama (KKKS)** adalah pihak/Badan Usaha yang melakukan kegiatan usaha hulu minyak dan gas bumi yang berintikan kegiatan eksplorasi dan eksploitasi minyak dan gas bumi sebagaimana dimaksud dalam Undang-Undang Republik Indonesia Nomor 22 Tahun 2001 tentang Minyak dan Gas Bumi.
32. ***License* (Lisensi)** adalah izin yang diberikan oleh pemegang paten kepada pihak lain berdasarkan perjanjian pemberian hak untuk menikmati manfaat ekonomi dari suatu paten yang diberikan perlindungan dalam jangka waktu dan syarat tertentu.
33. ***Mobile Device*** adalah perangkat komputasi yang dapat digunakan berpindah tempat seperti *smartphone* dan PDA.
34. ***Non-Disclosure Agreement*** adalah perjanjian untuk menjaga kerahasiaan informasi.
35. ***Password*** adalah kode atau simbol khusus untuk mengamankan sistem komputer yaitu untuk mengidentifikasi pihak yang mengakses data, program atau aplikasi komputer dan digunakan.
36. ***Patch*** adalah sekumpulan kode yang ditambahkan pada perangkat lunak untuk memperbaiki suatu kesalahan, biasanya merupakan koreksi yang bersifat sementara di antara dua keluaran versi *software*.
37. ***Patch Management*** adalah manajemen sistem yang meliputi proses memperoleh, pengujian dan instalasi berbagai *patch* yang digunakan untuk memperbaiki suatu program.

38. **Paten** menurut Undang-Undang Republik Indonesia Nomor 14 Tahun 2001 adalah hak eksklusif yang diberikan oleh Negara kepada Investor atas hasil investasinya di bidang teknologi untuk selama waktu tertentu melaksanakan sendiri investasinya tersebut atau memberikan persetujuannya kepada pihak lain untuk melaksanakannya.
39. **Pengamanan Fisik** adalah suatu sistem pengamanan untuk mencegah akses oleh pihak-pihak yang tidak berwenang terhadap area komputerisasi serta peralatan/fasilitas pendukung.
40. **Pengamanan Logik** adalah suatu sistem pengamanan untuk mencegah akses oleh pihak-pihak yang tidak berwenang terhadap sistem komputer dan informasi yang tersimpan di dalamnya yang meliputi penggunaan *user* ID, *password* dan lain-lain.
41. **Pengguna** (atau *user*) adalah pihak yang menggunakan suatu aplikasi atau layanan.
42. **Pengelolaan Data** meliputi perolehan, pengadministrasian, pengolahan, penataan, penyimpanan, pemeliharaan, dan pemusnahan data formasi.
43. **Penyedia Barang dan Jasa** adalah badan usaha atau perseorangan yang melaksanakan pengadaan barang/jasa yang terdiri dari sub kontraktor, pemasok, konsultan, usaha kecil, koperasidan lain-lain.
44. ***Power User*** adalah *user* ID yang memiliki kewenangan sangat luas.
45. ***Quality Assurance*** adalah aktivitas yang merupakan standar pengembangan yang akan digunakan untuk pengawasan proyek, pengendalian sistem dan kendali mutu.
46. ***Restore*** adalah tindakan untuk mengembalikan pada fungsi atau kondisi semula sebelum terjadi *disaster*.
47. ***Restricted Area*** adalah suatu area yang hanya dapat dimasuki oleh orang yang telah mendapatkan hak akses.
48. ***Risk Appetite*** adalah tingkat risiko yang siap diterima oleh organisasi sebelum suatu tindakan pengendalian diimplementasi untuk memitigasi risiko tersebut.
49. ***Service Level Agreement*** **(SLA)** adalah bagian dari kontrak perjanjian dimana tingkat penyediaan layanan yang diharapkan para pihak ditetapkan biasanya mencakup pula standar kinerja seperti tingkat pelayanan yang diperjanjikan (*service level*) atau target waktu penyediaan layanan.
50. ***Source Code*** adalah instruksi program perangkat lunak yang ditulis dalam suatu format (bahasa) dan dapat dibaca oleh manusia.

51. **Teknologi Informasi dan Komunikasi (TIK)** adalah teknologi terkait sarana komputer, telekomunikasi dan sarana elektronis lainnya yang digunakan dalam pengelolaan data KKKS.
52. ***Virus*** adalah program yang bersifat merusak dan akan aktif dengan bantuan orang (dieksekusi) dan tidak dapat mereplikasi sendiri, penyebarannya karena dilakukan oleh orang, seperti *copy*, biasanya melalui *attachement e-mail*, *game*, program bajakan dan lain-lain.

BAB II

PEMBINAAN DAN PENGAWASAN

A. Umum

Berdasarkan Peraturan Pemerintah Republik Indonesia Nomor 42 Tahun 2002, SKMIGAS sebagai Badan Pelaksana memiliki fungsi pengawasan terhadap Kegiatan Usaha Hulu agar pengambilan sumber daya alam Minyak dan Gas Bumi milik Negara Republik Indonesia dapat memberikan manfaat dan penerimaan yang maksimal untuk kemakmuran rakyat.

Kegiatan usaha Hulu Minyak dan Gas tersebut terbagi kedalam 3 proses utama, yaitu proses Penemuan Cadangan (*Finding)*, Pengembangan Lapangan (*Development)* dan Produksi (*Lifting)*. Berikut adalah penjelasan dari masing-masing proses:

1. Penemuan Cadangan (*Finding)*
   Merupakan proses yang dilakukan untuk menemukan potensi ekonomi yang bersifat prospek terhadap tersedianya cadangan minyak atau *hypothetical*.
2. Pengembangan Lapangan (*Development)*
   Merupakan proses pegembangan terhadap penemuan cadangan minyak yang telah dilakukan pada proses *finding.*
3. Produksi (*Lifting)*
   Merupakan proses produksi untuk menghasilkan minyak dari sumur hingga proses penjualan minyak hasil produksi.

Ketiga proses tersebut saling berhubungan satu sama lain dan terintegrasi mulai dari proses awal penemuan cadangan (*Finding*) hingga proses produksi (*Lifting*).

B. Pembinaan dan Pengawasan

Dalam menjalankan tugasnya sebagai fungsi pengawasan dan pembinaan terhadap aktivitas terkait dengan Teknologi Informasi dan Komunikasi (TIK) dalam Kegiatan Usaha Hulu Minyak dan Gas Bumi, SKMIGAS memiliki wewenang, yaitu:

1. Membina kegiatan terkait TIK yang dilakukan oleh KKKS berdasarkan kontrak kerja sama dalam rangka terwujudnya integrasi dan sinkronisasi kegiatan operasional KKKS;
2. Merumuskan kebijakan atas anggaran dan program kerja KKKS terkait TIK;
3. Mengawasi pelaksanaan kegiatan TIK serta data dan informasi KKKS;
4. Membina seluruh aset (termasuk data dan informasi) terkait TIK yang digunakan oleh KKKS dan diperoleh berdasarkan persetujuan SKMIGAS.

Berikut adalah penjelasan dari masing-masing wewenang di atas:

1. Pembinaan kegiatan tekait TIK.

   Pembinaan sebagaimana dimaksud dalam PTK ini meliputi:

   a. Penerapan TIK di KKKS untuk mewujudkan integrasi dan sinkronisasi kegiatan operasional KKKS sesuai dengan kompleksitas usaha dan karakteristik risiko KKKS;
   b. Pengadaan sistem/infrastruktur TIK dalam rangka meningkatkan optimalisasi kegiatan operasional KKKS.

2. Perumusan kebijakan atas anggaran dan program kerja KKKS terkait TIK

   Dalam hal ini, SKMIGAS memiliki hak untuk menentukan dan menyetujui anggaran program kerja TIK yang diajukan oleh KKKS.

3. Pengawasan kegiatan TIK serta data dan informasi terkait Usaha Hulu Minyak dan Gas

   SKMIGAS melakukan pengawasan terhadap KKKS atas penerapan PTK terkait TIK yang berlaku. SKMIGAS juga melakukan pengawasan dan pengendalian terhadap pemanfaatan aset TIK, termasuk di dalamnya adalah data dan informasi Kegiatan Usaha Hulu Minyak dan Gas. Dalam menjalankan perannya sebagai fungsi pengawasan, SKMIGAS memiliki akses terhadap perangkat TIK termasuk data dan informasi KKKS. Data dan informasi tersebut mencakup semua data dan informasi yang terkait dalam 3 proses utama Usaha Hulu Minyak dan Gas, yaitu data dan informasi proses Penemuan Cadangan (*Finding)*, Pengembangan Lapangan (*Development*) dan proses Produksi (*Lifting*).

Untuk memudahkan SKMIGAS dalam memperoleh data dan informasi tersebut, SKMIGAS telah memberlakukan inisiatif sistem informasi terkait kegiatan operasional KKKS, yaitu Sistem Operasi Terpadu (SOT). SOT merupakan sistem dengan arsitektur yang dirancang untuk mengintegrasikan kemampuan sistem informasi agar mempermudah pengelolaan dan pengolahan data dan informasi yang dapat mendukung proses bisnis SKMIGAS. Pedoman untuk penerapan dan pengelolaan SOT di KKKS akan diatur dalam PTK lainnya.

4. Pembinaan aset (termasuk data dan informasi) terkait TIK

   Sesuai dengan Peraturan Pemerintah Nomor 35 Tahun 2004 Pasal 78, aset TIK yang digunakan dalam kegiatan Usaha Hulu Minyak dan Gas Bumi oleh KKKS menjadi milik Negara Republik Indonesia, yang dikelola oleh SKMIGAS. Oleh karena itu, SKMIGAS juga memiliki tanggung jawab untuk melakukan pembinaan dan pengawasan terhadap pengelolaan aset TIK KKKS.

   Pelaksanaan pembinaan dan pengawasan dalam pengelolaan aset TIK KKKS dilakukan oleh SKMIGAS melalui pengendalian manajemen atas penerapan PTK TIK oleh KKKS.

Audit Sebagai Salah Satu Bentuk Pengawasan

Salah satu bentuk pengawasan SKMIGAS terhadap penerapan TIK di KKKS adalah dengan melakukan audit terhadap KKKS. Penerapan TIK di KKKS, termasuk di dalamnya penerapan kegiatan terkait TIK, penerapan kebijakan dan prosedur TIK, pengelolaan aset serta data dan informasi dapat menjadi objek audit TIK. Audit TIK dapat dilaksanakan secara regular dan *ad hoc* sesuai dengan kebutuhan SKMIGAS.

Dalam pelaksanaan audit, hal-hal yang harus diperhatikan adalah:

1. Jika terdapat keterbatasan dalam pelaksanaan audit TIK dari segi kualitas ataupun sumber daya, maka pelaksanaan fungsi audit dapat diwakilkan oleh auditor independen yang ditunjuk oleh SKMIGAS;
2. Pelaksanaan audit penerapan TIK memperhatikan kepatuhan terhadap Peraturan dan Perundangan yang berlaku;
3. Hasil kegiatan audit berupa tindak lanjut perbaikan wajib diselesaikan dalam jangka waktu yang telah disepakati;

4. Jika diperlukan, SKMIGAS dapat melakukan audit forensik atas persetujuan Kepala SKMIGAS;
5. Penyedia Barang dan Jasa yang menyimpan maupun mengelola data milik Negara Republik Indonesia harus bersedia diaudit oleh internal KKKS, SKMIGAS, atau pihak eksternal yang ditunjuk oleh KKKS maupun SKMIGAS. Penyedia Barang dan Jasa tersebut harus menyediakan informasi untuk keperluan pemeriksaan, termasuk hak akses, baik secara logik maupun fisik terhadap data dan informasi yang dikelola oleh Penyedia Barang dan Jasa.

D. Manajemen Risiko Dalam Pengelolaan Teknologi Informasi dan Komunikasi

Dalam upaya meningkatkan efektivitas penerapan TIK di usaha hulu minyak dan gas bumi, KKKS harus menerapkan manajemen risiko guna menjaga integritas informasi dan melindungi aset TIK. Penerapan manajemen risiko dalam pengelolaan TIK disesuaikan dengan kerangka manajemen risiko yang dimiliki KKKS dengan memperhatikan:

1. Penilaian Risiko (*Risk Assessment*)

   KKKS harus memiliki panduan dalam melakukan penilaian risiko yang meliputi identifikasi risiko di dalam proses bisnis KKKS. Hasil identifikasi risiko dapat menjadi masukan bagi proses lainnya, seperti perencanaan internal audit TIK, pemutakhiran DRP, dan dapat digunakan untuk meningkatkan pengendalian internal KKKS. Berikut adalah alternatif kategori risiko yang dapat digunakan oleh KKKS dalam melakukan identifikasi risiko:

   a. Risiko gangguan bisnis

      Merupakan risiko yang timbul dari ketidakmampuan KKKS untuk dapat melanjutkan kegiatan operasional jika sistem TIK atau informasi kritikal tidak tersedia. Risiko gangguan bisnis meliputi:

      i. Risiko kelangsungan bisnis;
      ii. Risiko pengamanan TIK;
      iii. Risiko *online*;
      iv. Risiko informasi.

b. Risiko relasional

Merupakan risiko yang timbul dari ketergantungan KKKS terhadap pihak eksternal, dan dampaknya dapat dirasakan oleh para *stakeholders*. Risiko relasional meliputi:

i. Risiko pengelolaan pihak penyedia barang dan jasa (*vendor management*);
ii. Risiko pihak ketiga dan mitra kerja;
iii. Risiko reputasi atau kepuasan pelanggan.

c. Risiko teknologi

Merupakan risiko yang timbul dari ketidakmampuan KKKS untuk mengikuti perkembangan teknologi, mengelola proyek-proyek TIK yang sesuai dengan kebutuhan operasional, dan mempertahankan standar infrakstruktur TIK di dalam KKKS. Risiko teknologi meliputi:

i. Risiko *agility* TIK;
ii. Risiko arsitektur TIK;
iii. Risiko pelaksanaan perubahan TIK;
iv. Risiko manajemen proyek.

d. Risiko tata kelola TIK

Merupakan risiko yang timbul dari lemahnya tata kelola TIK yang berakibat langsung terhadap domain risiko lainnya, sehingga akan menganggu tujuan strategis KKKS dan tujuan penerapan TIK di KKKS. Risiko tata kelola TIK meliputi:

i. Risiko strategis TIK;
ii. Risiko sumber daya TIK;
iii. Risiko kepatuhan atau legal.

2. *Risk Appetite*

Setiap tingkatan dalam organisasi TIK KKKS harus menetapkan batasan risiko yang dapat diterima terkait penggunaan dan pemanfaatan TIK dalam proses bisnisnya. *Risk appetite* tidak selalu dapat dihitung (kuantitatif), melainkan

disesuaikan dengan tujuan bisnis dan risiko yang dapat diterima oleh masing-masing unit bisnis untuk mencapai tujuan tersebut. Agar *risk appetite* dapat dipertimbangkan dan dikelola dengan baik, KKKS harus memiliki panduan dalam menentukan tingkat risiko yang dapat diterima oleh bisnis.

3. Evaluasi Risiko dan Pengendalian

Penerapan manajemen risiko yang efektif membutuhkan evaluasi atas risiko dan pengendalian yang diterapkan secara berkesinambungan. Evaluasi risiko dan penerapan pengendalian harus dilakukan secara periodik dan hasilnya dapat menjadi masukan untuk meningkatkan pengendalian internal KKKS.

Agar penerapan manajemen risiko dalam pengelolaan TIK berjalan dengan optimal, KKKS harus menerapkan pengendalian TIK berdasarkan manajemen risiko yang akan dibahas pada bab-bab selanjutnya dalam PTK TIK ini.

BAB III
PENGAMANAN INFORMASI

A. Pendahuluan

Data dan Informasi Minyak dan Gas Bumi sebagaimana diatur dalam peraturan dan perundangan merupakan aset yang penting bagi Negara Republik Indonesia. Setiap kebocoran, kerusakan, ketidaktersediaan, atau ancaman lainnya dapat menimbulkan dampak yang siginifikan bagi Negara Republik Indonesia. Oleh karena itu, KKKS bertanggung jawab untuk melindungi seluruh data dan informasi tersebut dengan menerapkan pengendalian terkait keamanan informasi yang mengacu pada prinsip-prinsip dasar keamanan, yaitu kerahasiaan (*confidentiality*), integritas (*integrity*) dan ketersediaan (*availability*).

Dalam menerapkan pengendalian untuk melindungi data dan informasi Negara Republik Indonesia, KKKS harus memiliki kebijakan dan prosedur pengamanan informasi yang meliputi pengamanan akses logik, pengamanan akses fisik, pengamanan operasional TIK, kebijakan anti virus, pengamanan jalur komunikasi data, fungsi pengamanan Informasi dalam manajemen dan organisasi, pengamanan pengembangan TIK, pengamanan dalam pengelolaan sumber daya manusia, serta pengamanan dalam pertukaran informasi.

1. Maksud dan Tujuan

a. Maksud

Pedoman ini dimaksudkan untuk memberikan panduan mengenai pengendalian utama yang perlu diterapkan KKKS dalam melakukan perlindungan serta pengamanan data dan informasi.

b. Tujuan

Pedoman pengamanan data dan informasi ditujukan untuk melindungi data dan informasi di KKKS dari penggunaan, pengungkapan, gangguan, pengubahan, atau pengerusakan yang dilakukan oleh pihak tidak berkepentingan. Pedoman ini merupakan salah satu panduan untuk mendefinisikan pengendalian keamanan yang dibutuhkan KKKS dalam rangka melindungi data dan informasi yang merupakan aset Negara.

Hasil yang diharapkan dari implementasi pedoman ini adalah tercapainya tiga prinsip keamanan data, yaitu kerahasiaan, integritas dan ketersediaan. Setiap data dan informasi harus dapat dijaga untuk memenuhi kepentingan Negara dan dapat bermanfaat secara optimal bagi operasional KKKS.

B. Penerapan Pengendalian dalam Pengamanan Informasi

KKKS harus memiliki kebijakan dan prosedur formal dan tertulis yang berisi penerapan pengendalian pengamanan informasi, yang mengatur hal-hal berikut ini:

1. Penerapan Klasifikasi Data

Penerapan pengendalian dalam pengamanan informasi harus dijalankan dengan memenuhi ketentuan peraturan dan perundangan yang berlaku di Indonesia, dan dijalankan sesuai dengan klasifikasi kerahasiaan data. KKKS harus menerapkan klasifikasi kerahasiaan pada setiap data yang digunakan dan disimpan, baik dalam bentuk *hardcopy* maupun dalam bentuk *softcopy*.

2. Pengamanan Akses Logik terhadap Informasi

Akses logik adalah pintu masuk untuk memperoleh data dan informasi yang ada di dalam sistem TIK. Akses ke dalam sistem internal KKKS yang di dalamnya mengandung data dan informasi harus diatur dan dikelola sesuai dengan tingkat klasifikasi kerahasiaan data, sehingga dapat mencegah terjadinya kebocoran informasi.

Penerapan pengamanan akses logik harus diterapkan oleh KKKS dengan prosedur yang baku dan dijalankan dengan benar dengan memenuhi hal-hal sebagai berikut, yaitu:

a. Proses pengajuan dan persetujuan hak akses pengguna dengan adanya administrasi hak akses pengguna yang meliputi pendaftaran, perubahan, dan penghapusan pengguna di dalam sistem, baik untuk pengguna internal KKKS, pengguna eksternal (Penyedia Barang dan Jasa, pegawai kontrak) maupun pihak Pemerintah;
b. Pembagian hak akses pengguna (*user privilege*), dimana terdapat pembedaan hak akses terhadap data dan informasi yang diijinkan untuk dikelola oleh masing-masing pengguna dalam TIK;
c. Penerapan manajemen kunci akses pengguna untuk memasuki sistem TIK. Kunci akses pengguna ini dapat berupa *password*, penggunaan token ataupun teknologi lainnya. Setiap kunci akses yang disimpan dalam sistem TIK harus menggunakan enkripsi untuk mencegah penyalahgunaan oleh pihak yang tidak berwenang;
d. Pelaksanaan *review* berkala terhadap hak akses pengguna. *Review* perlu dilakukan minimal setahun sekali untuk memastikan akses yang diberikan kepada setiap pengguna sesuai wewenangnya dan apakah diperlukan penyesuaian/*update* terhadap pemberian hak akses pengguna;
e. Penerapan *session timeout*. Untuk menjaga kerahasiaan informasi dan mencegah akses informasi dari pihak yang tidak berwenang, KKKS harus menerapkan *session timeout* saat penggunaan TIK;
f. Penerapan log aktivitas pengguna terhadap penggunaan TIK. Setiap aktivitas yang dilakukan oleh pengguna saat mengakses aplikasi maupun data dan informasi harus tercatat dalam log dan tersimpan di sistem. Log ini harus terjaga terhadap perubahan, dan hanya petugas yang berwenang yang dapat mengakses ataupun menghapus log tersebut;
g. Data yang bersifat rahasia dan tersimpan dalam sistem TIK maupun media penyimpanan lainnya, harus memiliki pembatasan akses dengan penerapan kunci akses dan menggunakan enkripsi/kriptografi, sehingga tidak dapat terbaca oleh pihak yang tidak berwenang;

h. KKKS wajib menetapkan prosedur penanganan *power user* agar penggunaannya tidak disalahgunakan. Prosedur tersebut harus mengatur hal-hal berikut:
    i. Penetapan siapa saja yang memiliki hak akses *power user* termasuk penerapan *dual custody* (pemecahan *password* kepada lebih dari 1 orang);
    ii. Prosedur penyimpanan *password power user*;
    iii. Prosedur *break ID power user* pada keadaan darurat;
    iv. Prosedur penggantian *password power user* setelah digunakan.

3. Pengamanan Akses Fisik terhadap Informasi

KKKS harus memiliki kebijakan dan prosedur yang baku terkait dengan pengendalian keamanan fisik dan lingkungan dalam rangka menjaga kerahasiaan, integritas dan ketersediaan data dan informasi. Penerapan pengendalian ini berlaku untuk lingkungan fisik dimana terdapat akses untuk memperoleh data dan informasi, seperti lingkungan *Data Center*, tempat penyimpanan data pada media eksternal, ataupun tempat penyimpanan dokumen *hardcopy*.

Penerapan pengendalian akses fisik harus memperhatikan hal-hal berikut ini:

a. Pembatasan akses fisik pada area *Data Center*

    KKKS harus melakukan pengamanan secara fisik pada lingkungan *Data Center* untuk memitigasi risiko pihak-pihak yang tidak berwewenang dapat memasuki *Data Center*.

b. Pengamanan akses terhadap media penyimpanan

    Apabila data disimpan dalam media penyimpanan (*softcopy*) ataupun dalam bentuk hasil cetak (*hardcopy*), maka penggunaan media perlu dikendalikan dengan menerapkan:

    i. Media penyimpanan harus disimpan dalam tempat yang terkunci dan aman dari akses oleh pihak yang tidak berwenang;

Penerapan pengamanan akses logik harus diterapkan oleh KKKS dengan prosedur yang baku dan dijalankan dengan benar dengan memenuhi hal-hal sebagai berikut, yaitu:

a. Proses pengajuan dan persetujuan hak akses pengguna dengan adanya administrasi hak akses pengguna yang meliputi pendaftaran, perubahan, dan penghapusan pengguna di dalam sistem, baik untuk pengguna internal KKKS, pengguna eksternal (Penyedia Barang dan Jasa, pegawai kontrak) maupun pihak Pemerintah;
b. Pembagian hak akses pengguna (*user privilege*), dimana terdapat pembedaan hak akses terhadap data dan informasi yang diijinkan untuk dikelola oleh masing-masing pengguna dalam TIK;
c. Penerapan manajemen kunci akses pengguna untuk memasuki sistem TIK. Kunci akses pengguna ini dapat berupa *password*, penggunaan token ataupun teknologi lainnya. Setiap kunci akses yang disimpan dalam sistem TIK harus menggunakan enkripsi untuk mencegah penyalahgunaan oleh pihak yang tidak berwenang;
d. Pelaksanaan *review* berkala terhadap hak akses pengguna. *Review* perlu dilakukan minimal setahun sekali untuk memastikan akses yang diberikan kepada setiap pengguna sesuai wewenangnya dan apakah diperlukan penyesuaian/*update* terhadap pemberian hak akses pengguna;
e. Penerapan *session timeout*. Untuk menjaga kerahasiaan informasi dan mencegah akses informasi dari pihak yang tidak berwenang, KKKS harus menerapkan *session timeout* saat penggunaan TIK;
f. Penerapan log aktivitas pengguna terhadap penggunaan TIK. Setiap aktivitas yang dilakukan oleh pengguna saat mengakses aplikasi maupun data dan informasi harus tercatat dalam log dan tersimpan di sistem. Log ini harus terjaga terhadap perubahan, dan hanya petugas yang berwenang yang dapat mengakses ataupun menghapus log tersebut;
g. Data yang bersifat rahasia dan tersimpan dalam sistem TIK maupun media penyimpanan lainnya, harus memiliki pembatasan akses dengan penerapan kunci akses dan menggunakan enkripsi/kriptografi, sehingga tidak dapat terbaca oleh pihak yang tidak berwenang;

h. KKKS wajib menetapkan prosedur penanganan *power user* agar penggunaannya tidak disalahgunakan. Prosedur tersebut harus mengatur hal-hal berikut:
   i. Penetapan siapa saja yang memiliki hak akses *power user* termasuk penerapan *dual custody* (pemecahan *password* kepada lebih dari 1 orang);
   ii. Prosedur penyimpanan *password power user*;
   iii. Prosedur *break ID power user* pada keadaan darurat;
   iv. Prosedur penggantian *password power user* setelah digunakan.

3. Pengamanan Akses Fisik terhadap Informasi

KKKS harus memiliki kebijakan dan prosedur yang baku terkait dengan pengendalian keamanan fisik dan lingkungan dalam rangka menjaga kerahasiaan, integritas dan ketersediaan data dan informasi. Penerapan pengendalian ini berlaku untuk lingkungan fisik dimana terdapat akses untuk memperoleh data dan informasi, seperti lingkungan *Data Center*, tempat penyimpanan data pada media eksternal, ataupun tempat penyimpanan dokumen *hardcopy*.

Penerapan pengendalian akses fisik harus memperhatikan hal-hal berikut ini:

a. Pembatasan akses fisik pada area *Data Center*

   KKKS harus melakukan pengamanan secara fisik pada lingkungan *Data Center* untuk memitigasi risiko pihak-pihak yang tidak berwewenang dapat memasuki *Data Center*.

b. Pengamanan akses terhadap media penyimpanan

   Apabila data disimpan dalam media penyimpanan (*softcopy*) ataupun dalam bentuk hasil cetak (*hardcopy*), maka penggunaan media perlu dikendalikan dengan menerapkan:

   i. Media penyimpanan harus disimpan dalam tempat yang terkunci dan aman dari akses oleh pihak yang tidak berwenang;

ii. Media penyimpanan harus disimpan dalam lingkungan yang dapat menjaga ketahanan media dalam dalam waktu yang dibutuhkan.

c. Pengamanan informasi pada pelaksanaan *disposal* data, sistem, infrastruktur TIK, dan/atau media penyimpanan.

Pemusnahan (*disposal*) merupakan penghapusan data, sistem, infrastruktur TIK, dan/atau media penyimpanan yang sudah tidak digunakan lagi atau masa retensinya telah habis. Data atau sistem versi lama yang sudah tidak dipakai lagi harus disimpan dengan keterangan yang jelas mengenai tanggal, waktu, dan informasi lainnya. Kegiatan yang dilakukan meliputi antara lain:

i. Memindahkan data dari sistem produksi ke media *backup* dengan mekanisme sesuai prosedur, termasuk prosedur uji coba dan *backup*;

ii. Menyimpan dokumentasi sistem sebagai persiapan jika diperlukan untuk menginstal ulang suatu sistem ke server produksi;

iii. Mengelola arsip data sesuai masa retensi;

iv. Menghancurkan data yang habis masa retensinya.

Apabila KKKS melakukan *disposal* infrastruktur TIK ataupun media penyimpanan yang sudah tidak digunakan lagi, maka KKKS perlu melakukan pengendalian untuk mencegah terjadinya kebocoran data. Hal-hal minimum yang harus dilakukan saat proses *disposal* adalah:

i. Memastikan bahwa data yang akan dihapus dari media penyimpanan adalah data yang sudah tidak terpakai dan penghapusannya tidak melanggar ketentuan yang berlaku di Negara Republik Indonesia;

ii. Setelah dilakukan penghapusan data, maka harus dipastikan bahwa seluruh data dalam infrastruktur TIK ataupun media tersebut sudah tidak terbaca atau tidak dapat digunakan lagi oleh pihak manapun;

iii. Mengelola arsip pelaksanaan *disposal* yang terdokumentasi dan dapat ditelusuri.

4. Pengamanan dalam Proses Operasional Teknologi Informasi dan Komunikasi

Penerapan pengamanan informasi dalam pelaksanaan operasional TIK tidak hanya terkonsentrasi pada layanan *Data Center*, namun juga pada aktivitas penggunaan aplikasi yang terintegrasi dan penggunaan komunikasi data. Dalam menjalankan operasional TIK, KKKS memiliki risiko terganggunya kerahasiaan, integritas dan ketersediaan informasi. Oleh karena itu, untuk meminimalisasi terjadinya risiko tersebut diperlukan pengendalian yang memadai atas operasional TIK dengan menerapkan hal-hal berikut ini:

a. Pengelolaan data dan informasi eksplorasi hulu minyak dan gas bumi tidak boleh keluar dari wilayah Republik Indonesia tanpa izin dari Kementerian Energi dan Sumber Daya Mineral;

b. Standar keamanan informasi (*security baseline*) yang berisi kebijakan yang harus diterapkan oleh KKKS dalam rangka menerapkan pengamanan informasi;

c. Penerapan respon darurat terhadap insiden kebocoran informasi, untuk mengambil langkah-langkah yang diperlukan dalam membatasi kemungkinan meluasnya kebocoran informasi;

d. Penerapan sistem pengaman TIK, dapat berupa *software* maupun *hardware* untuk mencegah kerusakan data maupun kebocoran akses TIK. Sistem pengamanan ini harus dapat melindungi data dari ancaman serangan program (*malicious software*) seperti virus, *spyware, firewall*, IDS, trojan dan sejenisnya. Penerapan sistem pengamanan TIK tersebut harus selalu dalam kondisi terkini.

5. Pengamanan Jalur Komunikasi Data

Penyelenggaraan jalur komunikasi data (jaringan komunikasi) memiliki risiko terbukanya suatu informasi dan/atau dokumen elektronik yang bersifat rahasia. Oleh karena itu, KKKS perlu menerapkan pengendalian keamanan jalur komunikasi data agar data dan informasi tidak terganggu oleh pihak-pihak yang tidak berwenang.

Keamanan jaringan komunikasi data merupakan tanggung jawab seluruh pihak dalam KKKS. Dalam pelaksanaannya, KKKS harus memiliki petugas/fungsi yang menangani jaringan komunikasi data. Petugas/fungsi tersebut harus melakukan koordinasi dengan fungsi pengelola pengamanan TIK. Beberapa hal yang harus diperhatikan oleh KKKS dalam pengamanan jaringan komunikasi data:

a. Pembatasan hak akses pengguna yang menggunakan jalur komunikasi data

Pengamanan akses ke jaringan komunikasi data di internal KKKS maupun ke luar KKKS harus dilakukan untuk memitigasi risiko terjadinya kebocoran informasi. Penerapan pembatasan akses pada jalur komunikasi data harus dilakukan dengan, namun tidak terbatas pada:

i. Pengamanan fisik dan logik, yaitu dengan:

a) Melakukan penyimpanan perangkat jaringan di lokasi yang aman terhadap gangguan lingkungan dan akses oleh orang yang tidak berhak;

b) Melakukan pengaturan parameter sistem perangkat jaringan untuk membatasi akses pengguna dalam jaringan;

ii. Penggunaan perangkat pengamanan jaringan komunikasi data untuk mencegah terganggunya jaringan dan terbukanya akses kepada pihak yang tidak berwenang;

iii. Jalur komunikasi data yang berisi berisi data rahasia yang terhubung dengan pihak eksternal dan/atau menggunakan jalur publik dan harus diamankan dengan menggunakan mekanisme enkripsi/kriptografi yang memadai.

b. Manajemen konfigurasi dan pemeliharaan perangkat jaringan komunikasi data

Untuk menjaga kelangsungan pengamanan informasi dalam pemakaian jalur komunikasi data, KKKS perlu melakukan pengelolaan dan pemeliharaan konfigurasi perangkat jaringan komunikasi data yang digunakan. Pengelolaan dan pemeliharaan perangkat jaringan komunikasi data harus dilakukan dengan menerapkan hal-hal berikut, namun tidak terbatas pada:

i. Penerapan identifikasi dan otentikasi pada setiap perangkat yang terhubung dengan jaringan;

ii. Penggunaan perangkat *monitor* jaringan Komunikasi Data (*network management system*) untuk memonitor kinerja perangkat dan jalur komunikasi, serta mendeteksi terjadinya gangguan;

iii. Pengujian secara berkala (minimal setahun sekali) terhadap keamanan dan konfigurasi jaringan komunikasi data, misalnya dengan *penetration testing, vulnerability assessment*, dan lain-lain;

iv. Melakukan proses *security hardening* terhadap *hardware* dan *software*, seperti proses *patching* dilakukan secara rutin untuk meyakinkan bahwa kelemahan-kelemahan telah diperbaiki.

6. Penerapan Fungsi Pengamanan Informasi dalam Manajemen dan Organisasi

Dalam menerapkan pengamanan informasi, KKKS harus memiliki kebijakan pengamanan informasi dan petugas yang bertanggung jawab untuk melakukan pengawasan terhadap pengamanan informasi, dengan menerapkan:

a. Petugas yang bertanggung jawab terhadap penerapan pengamanan informasi (*Information Security Officer*).

Harus terdapat fungsi atau petugas khusus dalam manajemen KKKS yang bertanggung jawab terhadap berjalannya penerapan pengamanan informasi. Tanggung jawab dari fungsi ataupun petugas pengamanan informasi sekurang-kurangnya adalah sebagai berikut:

i. Memimpin pengembangan kebijakan dan prosedur pengamanan informasi, agar sesuai dengan ketentuan yang ditetapkan oleh SKMIGAS dan kebutuhan KKKS;

ii. Melakukan pengawasan dan pengendalian terhadap penerapan kebijakan dan prosedur pengamanan informasi yang terdapat di KKKS;

iii. Memimpin pelaksanaan sosialisasi pengamanan informasi kepada seluruh karyawan dan manajemen KKKS untuk meminimalisir kemungkinan terjadinya kebocoran informasi;

iv. Menerapkan pengelolaan insiden pengamanan informasi, yang meliputi prosedur pelaporan, penanganan, pendokumentasian dan tidak lanjut terjadinya insiden pengamanan informasi.

b. Fungsi dalam organisasi yang spesifik menggambarkan garis kewenangan, pelaporan dan tanggung jawab terhadap pengamanan informasi.

Di dalam organisasi KKKS, dalam fungsi pengamanan informasi harus terdapat garis kewenangan, tanggung jawab dan mekanisme pelaporan yang jelas terhadap penerapan pengamanan informasi.

SKMIGAS dapat bekerjasama dengan pejabat yang bertanggung jawab terhadap pengamanan informasi di KKKS dalam rangka melakukan koordinasi dan pengawasan penerapan pengamanan informasi.

7. Pengamanan Informasi dalam Proses Pengembangan TIK

Dalam melaksanakan pengembangan TIK, KKKS harus menerapkan hal-hal berikut ini, sehingga hasil dari pengembangan TIK sudah menunjang pelaksanaan pengamanan informasi:

a. Penentuan kebutuhan dalam pengembangan sesuai kebutuhan pengamanan informasi

Dalam proses pengembangan TIK, spesifikasi sistem penunjang dan spesifikasi TIK yang akan dikembangkan harus memenuhi prinsip pengamanan informasi dengan menerapkan:

i. Pengendalian akses terhadap layanan TIK

Memastikan bahwa dapat dilakukan pembatasan terhadap akses logik dan fisik ke dalam TIK yang akan dikembangkan, sehingga data dan informasi dapat dikelola hanya oleh pihak yang berwenang.

ii. Enkripsi untuk penyimpanan data dan informasi yang bersifat rahasia.

Memastikan sistem mengelola informasi secara aman dengan menyimpan data dan informasi dalam format yang terenkripsi, sehingga meminimalisir kemungkinan terjadinya kebocoran informasi.

b. Perlindungan terhadap program asli dan *source code* aplikasi

KKKS harus menerapkan pengendalian keamanan terhadap program asli ataupun *source code,* baik untuk pengembangan aplikasi yang dilakukan secara internal maupun yang dilakukan secara *outsource* kepada Vendor dengan metode pembelian aplikasi. *Source code* tersebut harus disimpan pada tempat yang aman dengan menerapkan pembatasan akses logik maupun fisik untuk melindungi dari pihak yang tidak berwenang.

8. Pengamanan Informasi dalam Pengelolaan Sumber Daya Manusia

Pengamanan informasi juga harus diterapkan dalam pengelolaan sumber daya manusia yang memiliki akses terhadap sistem TIK, dengan menerapkan :

a. Pembatasan akses informasi bagi pegawai dan pihak eksternal (Penyedia Barang, Konsultan, dan Pihak Eksternal Lainnya)

Hilang, rusak, atau bocornya data dan informasi dapat terjadi karena kelalaian atau pelanggaran yang dilakukan oleh manusia, baik itu pihak internal KKKS ataupun pihak lainnya yang secara sah maupun tidak sah memiliki akses ke dalam sistem TIK. Oleh karena itu, pengamanan informasi perlu diterapkan dalam proses Sumber Daya Manusia di KKKS yang meliputi:

i. Pegawai KKKS dan Pihak Eksternal yang memiliki akses terhadap informasi harus memahami tanggung jawabnya terhadap pengamanan informasi;
ii. Peran dan tanggung jawab seluruh pihak yang memiliki akses terhadap informasi harus didefinisikan dan didokumentasikan sesuai dengan kebijakan pengamanan informasi;
iii. Perjanjian atau kontrak dengan Pegawai KKKS dan Pihak Eksternal harus mencantumkan ketentuan-ketentuan mengenai pengamanan TIK yang sesuai dengan kebijakan pengamanan informasi KKKS dan SKMIGAS;
iv. Pegawai KKKS dan Pihak Eksternal harus menandatangani perjanjian menjaga kerahasiaan informasi (*Non-Disclosure Agreement*);
v. KKKS harus menetapkan sanksi atas pelanggaran terhadap kebijakan pengamanan informasi;
vi. KKKS harus menetapkan prosedur yang mengatur tentang keharusan untuk mengembalikan aset dan pengubahan/penutupan hak akses pihak terkait yang disebabkan karena perubahan tugas atau selesainya masa kerja atau kontrak.

b. Pelaksanaan sosialisasi kepada seluruh personel dalam rangka meningkatkan kesadaran terhadap pengamanan informasi.

KKKS harus melakukan sosialisasi dalam rangka meningkatkan kesadaran pengamanan informasi dalam kegiatan pekerjaan sehari-hari.Pemahaman terhadap peran dan tanggung jawab setiap pengguna dalam menjaga keamanan akses informasi sangat penting untuk mencegah terjadinya penyalahgunaan akses.

Sosialisasi tentang pengamanan informasi harus diberikan kepada jajaran manajemen organisasi, pegawai KKKS, dan Pihak Eksternal.Pelaksanaan sosialisasi ini harus dilakukan secara berkala dan memiliki mekanisme pengukuran untuk mengetahui kesuksesan tingkat pemahaman peserta sosialisasi terhadap kesadaran pengamanan informasi.

9. Pengamanan pada Pelaksanaan Pertukaran Informasi

Dalam pelaksanaan pertukaran informasi dari KKKS kepada Pihak Eksternal selain SKMIGAS sebagai Badan Pelaksana, maka KKKS harus memiliki kebijakan dan prosedur yang baku. Kebijakan dan prosedur tersebut mencakup pengendalian terhadap pengiriman informasi secara *online* maupun melalui media penyimpan eksternal (seperti *tape, disk*, dan lain-lain). Hal-hal yang harus diatur dalam Kebijakan dan Prosedur Pertukaran Informasi adalah sebagai berikut, namun tidak terbatas pada:

a. Penerapan kesepakatan kerahasiaan informasi

Setiap kegiatan yang terkait dengan pertukaran informasi dengan pihak eksternal harus diawali dengan kesepakatan kerahasiaan informasi antara kedua belah pihak, yang ditandatangani oleh pejabat tertinggi yang bertanggung jawab terhadap informasi.

b. Manajemen pertukaran informasi

Setiap pelaksanaan pertukaran informasi harus melalui prosedur yang baku, melalui permintaan secara formal, dan mendapatkan persetujuan dari pejabat yang bertanggung jawab terhadap pengamanan informasi di KKKS. Setiap data dan informasi yang diberikan oleh KKKS harus tercatat dan terdokumentasi serta dapat ditelusuri mengenai data dan informasi apa saja yang telah diberikan dan siapa yang menerima data dan informasi tersebut.

10. Pengamanan Informasi pada Penggunaan *Mobile Device*

KKKS harus mengelola penggunaan mobile device untuk dapat mengakses data dan informasi dengan menggunakan jaringan karena memiliki risiko tinggi. Perangkat *mobile device* yang dimaksud adalah laptop, *Personal Digital Assistance* (PDA), *smartphone* (antara lain I Phone dan Blackberry), tablet, dan sebagainya, yang memiliki kemampuan untuk push *e-mail*, *web browser*, dan menggunakan jaringan komunikasi *service provider*. Berikut adalah hal-hal minimum yang harus diperhatikan oleh KKKS dalam penggunaan *mobile device*:

a. KKKS memiliki wewenang dan kemampuan untuk melaksanakan syarat-syarat keamanan tertentu terhadap *mobile device*;
b. Adanya mekanisme yang memastikan konfigurasi keamanan mobile device tidak berubah sesuai dengan kebijakan yang telah ditetapkan oleh KKKS;
c. Hak akses harus sesuai kebutuhan dan adanya petunjuk pelaksanaan bagi *user* untuk dapat mengakses sistem informasi;
d. Adanya mekanisme keamanan seperti *password* untuk dapat mengakses data di *mobile device;*
e. Adanya mekanisme untuk menghapus data yang berada di *mobile device* ketika terjadi kehilangan.

BAB IV
JARINGAN KOMUNIKASI

A. Pendahuluan

Jaringan komunikasi mencakup *hardware*, *software*, dan media yang digunakan untuk mentransmisikan informasi berupa data, suara (*voice*), gambar (*image*) dan video.

Penyelenggaraan jaringan komunikasi memiliki risiko: 1) diakses oleh pihak yang tidak berwewenang (*unauthorized access*), 2) terbukanya suatu informasi elektronik dan/atau dokumen elektronik yang bersifat rahasia kepada publik (*exposures*), 3) keberlangsungan layanan TIK (*continuity*) dan 4) kinerja (*performance*). Oleh karena itu, KKKS harus memiliki kebijakan dan prosedur sebagai pedoman dalam menerapkan teknologi jaringan komunikasi untuk meyakinkan bahwa kelangsungan operasional dan keamanan jaringan komunikasi tetap terjaga. Dalam menerapkan pengendalian pada jaringan komunikasi untuk melindungi integritas data dan informasi Negara Republik Indonesia, KKKS harus memiliki pengelolaan pada jaringan komunikasi meliputi:

a. Pengukuran kinerja dan kapasitas jaringan komunikasi;
b. *Backup* jaringan komunikasi;
c. Pengendalian akses terhadap jaringan komunikasi;
d. Penggunaan jaringan internet;
e. Penggunaan jaringan nirkabel;
f. Penggunaan *dial up;*
g. Penggunaan sarana komunikasi radio;
h. Penggunaan *Process Control Network* (PCN).

1. Maksud dan Tujuan

a. Maksud

Pedoman ini dimaksudkan untuk memberikan acuan kepada KKKS dalam melakukan pengelolaan terhadap jaringan komunikasi, sehingga memperkecil

risiko timbulnya celah keamanan yang dapat membahayakan data dan sistem informasi KKKS.

b. Tujuan

Pedoman jaringan komunikasi ditujukan untuk membangun kerangka kerja bagi KKKS dalam melakukan pengelolaan jaringan komunikasi agar dapat memenuhi aspek operasional, serta tetap tunduk pada prinsip keamanan informasi. Melalui implementasi pengendalian jaringan, KKKS dapat menerapkan mekanisme pengendalian jaringan komunikasi untuk menjamin ketersediaan kapasitas jaringan, serta untuk menjaga integritas data pada saat melakukan pengiriman data.

B. Penerapan Pengendalian Jaringan Komunikasi

1. Pengukuran Kinerja dan Kapasitas Jaringan Komunikasi

Dalam pengelolaan jaringan komunikasi dibutuhkan pengukuran kinerja dan kapasitas. KKKS harus mendesain jaringan komunikasi yang efisien serta dinamis untuk mengantisipasi perkembangan di masa yang akan datang. Selain itu, KKKS juga harus memastikan ketersediaan dan kecukupan kapasitas layanan jaringan komunikasi yang dikelola oleh Penyedia Barang atau Jasa.

Untuk memastikan jaringan komunikasi berfungsi sesuai dengan kebutuhan strategis, maka KKKS harus menetapkan kebijakan dan prosedur terkait dengan pengukuran kinerja dan kapasitas jaringan, serta menunjuk personel yang bertanggung jawab. Hal-hal umum yang harus diperhatikan dalam pengukuran kinerja dan kapasitas jaringan komunikasi adalah:

a. Menentukan topologi dan protokol jaringan komunikasi;
b. Memilih media jaringan komunikasi sesuai dengan kebutuhan;
c. Adanya kontrak dengan Penyedia Barang dan Jasa,serta tersedianya SLA yang sesuai dengan kebutuhan bisnis;
d. Melakukan kaji ulang atas penggunaan jaringan komunikasi minimal setahun sekali;

e. Melakukan pengukuran terhadap kapasitas jaringan komunikasi berdasarkan tingkat ketersediaan dan kecukupan kapasitas minimal 1 (satu) tahun sekali;
f. Pengelolaan kapasitas *bandwidth* diterapkan untuk membatasi maksimum penggunaan-nya pada masing-masing *workstation*;
g. Melakukan perencanaan kapasitas (*capacity planning*) terhadap jaringan komunikasi;
h. Pemantauan kebutuhan kapasitas, yaitu membandingkan kapasitas yang direncanakan dengan yang digunakan. Pemantauan kapasitas harus dilakukan secara periodik oleh KKKS untuk menjaga ketersediaan layanan TIK.

2. Backup Jaringan Komunikasi

Jaringan komunikasi sangat rentan terhadap gangguan baik dari eksternal maupun internal KKKS. Oleh karena itu, KKKS menerapkan *backup* jaringan komunikasi untuk menjaga ketersediaan layanan komunikasi. Dalam menerapkan *backup* jaringan komunikasi, KKKS harus memperhatikan hal-hal berikut:

a. Tersedianya *alternative routing* (jalur alternatif) dan/atau Penyedia Barang dan Jasa alternatif dalam penyediaan layanan jaringan komunikasi;
b. Tersedianya *backup* perangkat jaringan komunikasi;
c. Memiliki *incident response plan* terhadap gangguan akses yang tidak berwenang pada jaringan komunikasi;
d. Tersedianya prosedur penanganan masalah (*problem handling*).

3. Pengendalian Akses terhadap Jaringan Komunikasi

Pengendalian akses terhadap jaringan komunikasi adalah suatu upaya untuk mengendalikan akses masuk serta aktivitas yang dilakukan untuk memperoleh data atau informasi. Pengendalian akses di jaringan komunikasi sangat penting dan harus diperhatikan karena memiliki risiko perubahan data dari pihak yang tidak berwenang dan terbukanya suatu informasi elektronik dan/atau dokumen elektronik yang bersifat rahasia kepada publik.

Dalam menerapkan pengendalian akses, terdapat beberapa hal yang harus diperhatikan oleh KKKS, yaitu:

a. Akses ke jaringan komunikasi didasarkan pada kebutuhan dengan memperhatikan aspek keamanan informasi;
b. Akses jaringan komunikasi dari lingkungan kerja di wilayah Indonesia ke luar wilayah Indonesia harus melalui izin SKMIGAS;
c. Melakukan pemisahan jaringan komunikasi berdasarkan segmen, baik secara logis maupun fisik sesuai dengan kebutuhan;
d. Akses ke jaringan komunikasi harus dipantau;
e. Konfigurasi perangkat jaringan komunikasi harus diatur dengan baik. *Port* dan *services* yang tidak dibutuhkan harus dinonaktifkan;
f. Melakukan kaji ulang pemberian akses ke pengguna secara berkala dan sesuai dengan kebutuhan untuk meyakinkan bahwa akses yang diberikan masih sesuai dengan tugas dan wewenangnya;
g. Penggunaan perangkat pengamanan jaringan komunikasi, seperti *firewall, Intrusion Detection System,* dan *Intrusion Prevention System.*

C. Penggunaan Jaringan Komunikasi

1. Penggunaan Jaringan Internet

Penggunaan jaringan internet untuk dapat mengakses data atau informasi, memiliki risiko tinggi yang harus diantisipasi oleh KKKS. Pengendalian yang memadai terhadap penggunaan internet harus dikelola agar dampak kehilangan data dapat diminimalkan. Oleh karena itu, terdapat beberapa hal minimum yang harus diperhatikan oleh KKKS, yaitu:

a. Jaringan internet yang digunakan harus menggunakan mekanisme VPN (*virtual private network*);
b. Lalu lintas data melalui jaringan internet harus dienkripsi;
c. Adanya mekanisme otentifikasi keamanan seperti *username* dan *password*.

2. Penggunaan Jaringan Nirkabel

Penggunaan jaringan nirkabel untuk mengakses data dan informasi memiliki risiko tinggi. Oleh karena itu, penggunaan jaringan nirkabel di lingkungan KKKS diperbolehkan selama pengendaliannya memadai. Berikut adalah hal-hal minimum yang harus diperhatikan oleh KKKS dalam penggunaan jaringan nirkabel:

a. Adanya metode enkripsi data, otentikasi dan otorisasi terhadap penggunaan jaringan nirkabel dalam mengakses sistem informasi;
b. Melakukan *monitoring* atas penggunaan koneksi jaringan nirkabel;
c. KKKS memiliki mekanisme untuk melakukan konfigurasi perangkat jaringan nirkabel.

3. Penggunaan *Dial Up*

Penggunaan jaringan komunikasi dengan mekanisme *dial up* dalam mengakses data dan informasi memiliki risiko tinggi. Oleh sebab itu, dalam penggunaan jaringan *dial up,* terdapat beberapa hal minimum yang harus diperhatikan oleh KKKS, yaitu:

a. Adanya penentuan pengguna yang berhak melakukan *outgoing call* dan *incoming call*, serta jalur yang dilalui;
b. Adanya mekanisme keamanan seperti *user name* dan *password*;
c. Adanya mekanisme verfikasi *call back* dari *server* sistem informasi yang diakses untuk memastikan akses telah sesuai dengan yang diberikan;
d. Lalu lintas data harus dienkripsi.

4. Penggunaan Sarana Komunikasi Radio

Sarana komunikasi radio yang digunakan untuk kegiatan usaha hulu minyak dan gas bumi oleh KKKS harus sesuai dengan peraturan dan perundang-undangan yang berlaku, dimana dalam menggunakan sarana telekomunikasi radio harus memiliki perizinan sesuai peruntukkannya. Sistem dan sarana komunikasi radio yang akan digunakan harus mendapatkan persetujuan dari SKMIGAS. Pengurusan legalitas sarana komunikasi radio untuk KKKS dengan instansi

pemerintah akan difasilitasi oleh SKMIGAS. Selain itu, operator komunikasi radio di KKKS harus memiliki sertifikasi yang sesuai dan masih berlaku.

Berikut beberapa hal yang harus diperhatikan oleh KKKS dalam penggunaan sarana komunikasi radio, yaitu:

a. Penggunaan sarana telekomunikasi radio harus mendapatkan izin dari Direktorat Jenderal Pos dan Telekomunikasi melalui SKMIGAS;
b. KKKS harus melakukan koordinasi dengan SKMIGAS terkait dengan stasiun radio untuk:
   i. Permohonan baru ;
   ii. Pergantian dan penambahan frekuensi;
   iii. Perpanjangan;
   iv. Pengembalian izin stasiun radio.
c. Peralatan yang digunakan harus sesuai dengan peruntukkannya.

5. Penggunaan *Process Control Network* (PCN)

Dalam menjalankan Kegiatan Usaha Hulu Minyak dan Gas Bumi penggunaan teknologi *Process Control Network* (PCN) oleh KKKS harus dikelola dengan optimal untuk memastikan ketersediaan dan integritas data. PCN harus mampu untuk mengambil dan menampilkan data sesuai dengan keluaran dari perangkat lapangan (*field device*) dan atau mengirimkan data kendali (perintah) kepada perangkat lapangan (*field device*) sesuai dengan konfigurasi atau aksi kendali yang ditetapkan.

Dalam upaya untuk memastikan hal tersebut, terdapat beberapa hal dalam pengelolaan jaringan komunikasi yang harus diperhatikan oleh KKKS, yaitu:

a. Terdapat kebijakan dan prosedur yang dapat memastikan integritas data pada jaringan komunikasi PCN;
b. Menerapkan topologi jaringan yang memiliki keamanan yang dapat diandalkan;
c. Memisahkan jaringan komunikasi antara sistem PCN dan sistem KKKS;
d. Membatasi akses fisik pada jaringan komunikasi dan perangkat sistem PCN;

e. Menyediakan *backup* jaringan komunikasi pada sistem PCN;
f. Adanya mekanisme yang memastikan bahwa data yang diiinput baik dari *field* maupun dari *control room* telah valid, baik dalam bentuk pengendalian, pengawasan, maupun audit secara periodik.

BAB V
PENGEMBANGAN SISTEM/INFRASTRUKTUR TEKNOLOGI INFORMASI DAN KOMUNIKASI

A. Pendahuluan

Pengembangan sistem/infrastruktur TIK di lingkungan KKKS meliputi proses pengidentifikasian kebutuhan pengguna dan pelaksanaan pengembangan yang mencakup *software* dan infrastruktur TIK. Untuk memenuhi kebutuhannya, KKKS didorong untuk menggunakan program *open source*. Hal ini dapat menghindari ketergantungan KKKS terhadap satu vendor penyedia program/aplikasi.

Dalam pelaksanaan pengembangan sistem/infrastruktur TIK terdapat risiko bahwa pengembangan yang dilakukan tidak memberikan kontribusi yang optimal pada proses operasional KKKS. Oleh karena itu, KKKS perlu menerapkan pengendalian dalam proses pengembangan sistem/infrastruktur TIK dengan memiliki kebijakan dan prosedur tentang manajemen proyek, serta metodologi pengembangan sistem/infrastruktur TIK.

1. Maksud dan Tujuan

a. Maksud

Pedoman ini dimaksudkan untuk memberikan panduan mengenai pengendalian utama yang perlu diterapkan oleh KKKS dalam melakukan pengembangan sistem/infrastruktur TIK.

b. Tujuan

Pedoman pengembangan sistem/infrastruktur TIK ditujukan untuk memberikan panduan pengendalian bagi KKKS dalam melakukan pengembangan, instalasi, implementasi, serta perubahan pada sistem/infrastruktur TIK. Dalam hal ini, pengendalian yang diterapkan tidak hanya merupakan pengendalian preventif,

namun juga pengendalian detektif dan korektif agar sistem/infrastruktur TIK dapat digunakan dengan baik serta memberikan kontribusi yang optimal bagi kegiatan KKKS.

Melalui implementasi pengendalian ini, diharapkan KKKS dapat memperoleh dan mendayagunakan sistem TIK yang dibutuhkan dalam jumlah, kualitas, harga, waktu, tempat yang efektif dan efisien, dapat dipertanggungjawabkan sesuai ketentuan dan prosedur yang berlaku, serta memenuhi prinsip-prinsip keamanan TIK.

B. Penerapan Pengendalian dalam Pengembangan Sistem/Infrastruktur TIK

1. Rencana Kerja Pengembangan Sistem/Infrastruktur TIK

Dalam proses pengembangan sistem/infrastruktur TIK, KKKS harus menyiapkan rencana pengembangan berdasarkan *Work Program and Budget* (WP&B) dan harus mendapatkan persetujuan dari SKMIGAS. Proses penyusunan WP&B mengacu pada ketentuan yang telah ditetapkan SKMIGAS, sebagaimana tertuang dalam Pedoman Tata Kerja (PTK) SKMIGAS yang mengatur mengenai WP&B.

2. Manajemen Proyek dalam Pengembangan Sistem/Infrastruktur TIK

Dalam melakukan pengembangan sistem/infrastruktur TIK, KKKS harus menerapkan Manajemen Proyek. Penerapan Manajemen Proyek bertujuan untuk memastikan bahwa sistem/infrastruktur TIK telah dikembangkan sesuai tujuan pengembangan, waktu yang telah ditentukan, dan biaya yang dianggarkan. Selain itu, penerapan manajemen proyek dapat memastikan bahwa proses pengembangan sistem/infrastruktur TIK telah memenuhi kebutuhan pengguna.

Dalam menerapkan Manajemen Proyek pada proses pengembangan sistem/ infrastruktur TIK, KKKS ataupun pihak penyedia barang dan jasa harus menerapkan beberapa hal, yaitu:

a. Metodologi

Metodologi pengembangan sistem/infrastruktur TIK yang digunakan oleh KKKS harus sesuai dengan karakteristik dan risiko proyek. Terdapat

beberapa metodologi pengembangan yang dapat digunakan, namun tidak terbatas pada:

i. *Agile Software Development*;

Merupakan kerangka pengembangan sistem yang berbasis pada pengembangan secara iterasi/berulang-ulang dalam siklus proyek untuk merespon kebutuhan dan solusi pengembangan yang berubah atau berkembang terus menerus.

ii. *Rapid Application Development*;

Merupakan metodologi pengembangan dimana *working model* sistem dikonstruksikan diawal tahap pengembangan dengan tujuan menetapkan kebutuhan pengguna.RAD menekankan pada siklus pembangunan pendek, singkat, dan cepat.

iii. *System Development Life Cycle (SDLC)*;

Merupakan metodologi pengembangan yang pada umumnya sering digunakan.Adapun tahapan yang diperlukan adalah perencanaan, pengadaan (dilakukan apabila KKKS menggunakan pihak penyedia barang dan jasa), perancangan, pemrograman, pengujian, implementasi, kaji ulang paska implementasi dan pemeliharaan.

b. *IT Quality Assurance*

Dalam pelaksanaan pengembangan sistem/infrastruktur TIK dibutuhkan aktivitas *quality assurance* untuk memastikan bahwa tahapan pengembangan dilakukan sesuai dengan metodologi yang diterapkan.*IT Quality Assurance* juga membantu Tim Proyek dalam memastikan *deliverables* setiap tahapan pekerjaan telah sesuai dengan TOR.

3. Pengendalian Pengembangan Sistem/Infrastruktur TIK

Metodologi SDLC merupakan metodologi yang pada umumnya digunakan dalam melakukan pengembangan sistem/infrastruktur TIK. Berikut pengendalian yang dapat diterapkan dalam pengembangan sistem/infrastruktur TIK dengan menggunakan metodologi SDLC.

a. Perencanaan

KKKS harus melakukan proses identifikasi kebutuhan pengembangan sistem/ infrastruktur TIK dan melakukan perencanaan untuk melaksanakan proyek. Proses ini didokumentasikan dalam sebuah dokumen proposal dan studi kelayakan yang sekurang-kurangnya mencakup hal-hal berikut:

i. Tujuan pelaksanaan pengembangan sistem/infrastruktur TIK;
ii. Ruang lingkup proyek;
iii. Manfaat yang diharapkan dari sistem/infrastruktur TIK yang akan dikembangkan, khususnya menjelaskan manfaat bagi efisiensi biaya (*cost efficiency*) dan peningkatan produksi;
iv. Analisa untuk menentukan pengembangan dilakukan oleh internal KKKS atau menggunakan pihak penyedia barang dan jasa, termasuk pengajuan apabila KKKS akan melakukan *direct charges*;
v. Jadwal proyek;
vi. Struktur Tim Proyek.

Proposal dan hasil dari studi kelayakan harus diajukan kepada SKMIGAS.

b. Pengadaan

Pelaksanaan pengadaan dilakukan apabila KKKS menggunakan pihak penyedia barang dan jasa dalam melakukan pengembangan sistem/infrastruktur TIK. Proses pengadaan ini harus mengacu kepada Pedoman Tata Kerja - Nomor 007 REVISI II/PTK/I/2011 tentang Pedoman Pengelolaan Rantai Suplai Kontraktor Kontrak Kerja Sama (PTK 007) serta perubahannya. Penyedia barang dan jasa yang akan bekerja sama dengan KKKS harus memiliki SKT (Surat Keterangan Terdaftar) dari SKMIGAS.

PTK 007 telah mengatur isi kontrak terkait dengan pelaksanaan pengadaan barang dan jasa. Namun khusus terkait dengan pengembangan sistem/infrastruktur TIK, KKKS harus memastikan bahwa:

i. Penyedia barang dan jasa yang ditugaskan di KKKS menandatangani NDA (*Non-Disclosure Agreement*);

ii. Penyedia barang dan jasa memberikan SLA dan laporan hasil pemantauan kinerja. SLA tersebut tetap berlaku apabila terjadi perubahan kepemilikan baik pada KKKS maupun penyedia barang dan jasa;

iii. Terdapat garansi kepada SKMIGAS diantaranya adalah:

a) Garansi untuk barang dan jasa yang diberikan kepada SKMIGAS selama periode tertentu setelah implementasi;

b) Garansi bahwa sistem yang dikembangkan tidak mengandung *back door* yang memungkinkan akses oleh pihak yang tidak berwenang ke dalam sistem tersebut.

iv. Jika KKKS melakukan pembelian lisensi terhadap *software* yang dibuat atau disediakan oleh penyedia barang dan jasa, maka:

a) Penyedia barang dan jasa harus melindungi kepemilikan dan kerahasiaan sumber daya dan data KKKS;

b) Penyedia barang dan jasa tidak diperkenankan menggunakan atau mengungkapkan informasi yang dimiliki KKKS tanpa persetujuan KKKS;

c) Secara eksplisit menyatakan bahwa penyedia barang dan jasa tidak akan menggunakan fitur *software* yang dapat mengakibatkan *software* tersebut tidak berfungsi dengan baik.

v. Terdapat batasan risiko yang ditanggung oleh KKKS, dan penyedia barang dan jasa, diantaranya adalah:

a) Risiko perubahan ruang lingkup kontrak;

b) Perubahan ruang lingkup bisnis dan organisasi KKKS dan penyedia barang dan jasa;

c) Perubahan aspek hukum serta regulasi;

d) Aspek hukum yang meliputi hak cipta, paten dan *trade mark*.

vi. Jika KKKS menggunakan layanan penyedia barang dan jasa dan terdapat data yang disimpan dan diolah oleh penyedia barang dan jasa, maka KKKS memiliki wewenang untuk melakukan audit terhadap penyedia barang dan jasa tersebut;

vii. Jika penyelenggaraan *Data Center* dan *Disaster Recovery Center* dikelola oleh pihak penyedia barang dan jasa, maka hal-hal yang harus diperhatikan adalah:

a) Tersedianya sarana komunikasi *on-line*, pengamanan terhadap aksesdan transmisi data, dari dan ke *Data Center*, *Disaster Recovery Center*, dan pengelolaan data berbasis TIK;

b) Pengaturan yang jelas mengenai *backup*, *contingency*, *record protection* termasuk *hardware*, *equipment*, *software* dan *data files*, untuk menjamin kelangsungan penyelenggaraan TIK;

c) Pengaturan mengenai pengamanan dalam pengiriman *source document* yang diperlukan dari dan *ke Data Center, Disaster Recovery Center*, dan pengelolaan data berbasis TIK.

viii. Penyedia barang dan jasa yang terikat kerja sama dengan KKKS bersedia diaudit oleh SKMIGAS apabila dibutuhkan.

c. Perancangan

Aktivitas yang dilakukan pada tahap ini yaitu dengan melakukan perancangan sistem/infrastruktur TIK berdasarkan identifikasi kebutuhan. Semua kebutuhan pengguna yang telah teridentifikasi dikonversikan menjadi rancangan sistem yang akan menghasilkan suatu dokumen teknis. Dokumen tersebut harus dikaji oleh personel Auditor, *Information Security Officer* dan *IT Quality Assurance* sebelum digunakan oleh *Programmer*.

Hal-hal yang harus diperhatikan dalam proses perancangan sistem adalah sebagai berikut, namun tidak terbatas pada:

i. Deskripsi detil sistem/infrastruktur TIK;

ii. Diagram alur data dalam sistem/infrastruktur TIK yang dikembangkan;

iii. Rincian spesifikasi rancangan sistem/infrastruktur TIK yang akan dikembangkan harus sesuai dengan kebutuhan;

iv. Kebutuhan keamanan (*security requirement*) yang mengacu kepada *Security Baseline* milik KKKS.

Selain itu dalam aktivitas perancangan sistem diperlukan suatu standar pengendalian terkait aktivitas pengguna pada sistem. Standar sistem aplikasi tersebut dapat meningkatkan keamanan, integritas dan kehandalan sistem dengan memastikan *input*, proses dan *output* yang akurat, lengkap dan aman.

Pengendalian yang harus dilakukan paling kurang meliputi:

i. Pengendalian *input*

Memastikan pengguna memasukkan informasi secara akurat agar dapat mengurangi kesalahan *input/human error.* Pengendalian *input* minimal dapat mencakup pengecekan terhadap validitas/kebenaran data, *range* data/parameter dan duplikasi data yang di-*input*.

ii. Pengendalian proses

Memastikan proses bekerja secara akurat dan dapat menyimpan informasi atau menolaknya. Pengendalian proses yang dapat dilakukan secara otomatis oleh sistem mencakup paling kurang *Error Reporting, Transaction Log,* pengecekan urutan dan *backup file*.

iii. Pengendalian output

Memastikan sistem mengelola informasi dengan aman dan mendistribusikan informasi hasil proses dengan tepat serta menghapus informasi yang telah melewati masa retensi.

d. Pemrograman

Pada tahap pemrograman, hasil spesifikasi desain dikonversikan menjadi sebuah program yang dapat dijalankanoleh *Programmer*. Pada saat pemrograman, Manajer Proyek harus memahami secara keseluruhan proses pemrograman untuk memastikan tanggung jawab seorang *Programmer* terhadap data, program, dan sistem telah dibatasi untuk menjaga integritas dan keamanan data.

Pada pengembangan sistem/infrastruktur TIK diperlukan pengujian internal untuk meminimalkan terjadinya kesalahan pada sistem yang dikembangkan dan memastikan sistem telah berjalan dengan baik.Pengujian internal yang dilakukan adalah dengan melakukan *Unit Testing.* Pengujian ini dilakukan untuk menilai fungsionalitas dari sebagian kecil modul pada sistem.

Dokumentasi teknis pemrograman, data, dan program hasil pengembangan harus disimpan dalam media penyimpanan dengan baik oleh KKKS.

e. Pengujian

Pada tahap pengujian, pengguna melakukan beberapa rangkaian uji coba untuk memastikan keakuratan dan berfungsinya sistem/infrastruktur TIK sesuai dengan kebutuhan. Pengujian yang dapat dilakukan antara lain, namun tidak terbatas pada:

i. *System Integration Testing*, dilakukan untuk menilai fungsionalitas seluruh sistem dan integrasi antar modul di dalam sistem;

ii. *Stress Testing*, dilakukan dalam rangka menilai kinerja sistem pada kondisi penggunaan maksimal untuk mendapatkan batasan kemampuan maksimal dari sistem yang dikembangkan;

iii. *User Acceptance Testing* (UAT), dilakukan untuk menguji fungsionalitas keseluruhan sistem apakah telah sesuai dengan kebutuhan pengguna, baik dari sisi akurasi, maupun hubungan dengan sistem lain (*interoperability*). Pada saat UAT, terdapat 2 macam pengujian yang dapat dilakukan dengan menggunakan skenario pengujian, yaitu:

a) *Positive Test*

Merupakan suatu pengujian yang sengaja dirancang untuk menunjukan bahwa sistem/infrastruktur TIK akan menghasilkan *output* yang sesuai jika informasi yang diinput oleh *user* adalah benar. Pengujian ini dilakukan berdasarkan skenario yang telah disusun sebelumnya.

b) *Negative Test*

Merupakan suatu pengujian yang sengaja dirancang untuk menunjukan bahwa sistem/infrastruktur TIK akan menghasilkan *output* yang tidak sesuai atau tidak diharapkan jika informasi yang diinput oleh *user* adalah salah. Pengujian ini dilakukan berdasarkan skenario yang telah disusun sebelumnya.

UAT merupakan uji coba akhir yang dilakukan oleh pengguna akhir terhadap sistem yang dikembangkan. Selain pengguna, UAT ini dapat melibatkan Fungsi Internal Audit TIK untuk memastikan ketersediaan, kecukupan dan keefektifan pengendalian yang ada di sistem, dengan tetap menjaga tingkat independensinya.

UAT dilakukan dengan menggunakan skenario pengujian yang sebelumnya disusun dan didokumentasikan oleh pengguna. Hasil dari pelaksanaan UAT harus didokumentasikan dalam Berita Acara dan disetujui oleh pengguna, Manajer Proyek, Internal Audit TIK, dan *IT Quality Assurance*.

f. Implementasi

KKKS harus menerapkan pengendalian pada tahap implementasi sistem/ infrastruktur TIK ke lingkungan produksi. Hal-hal yang harus diperhatikan pada tahap implementasi adalah:

i. Terdapat rencana *release* sistem/infrastruktur TIK untuk menentukan jadwal dan tahapan *release* sistem/infrastruktur TIK ke lingkungan produksi;
ii. Terdapat rencana *rollback* untuk mengatasi jika sistem/infrastruktur TIK yang diimplementasikan mengalami kegagalan fungsional atau menyebabkan kinerja aplikasi kritikal lainnya terganggu, sehingga sistem lama harus digunakan kembali;
iii. Terdapat rencana migrasi data apabila sistem yang akan diimplementasikan menggantikan sistem lama di lingkungan produksi dan di dalamnya terdapat data yang masih digunakan, yang mencakup:

a) Pengecekan integritas program, berupa pengendalian yang memadai terhadap konversi *source code* ke *object code* yang akan diimplementasikan;

b) Pengecekan akurasi dan keamanan data hasil migrasi perlu dilakukan untuk memastikan integrasi dan validitas data.

iv. Terdapat rencana pelatihan penggunaan sistem/infrastruktur TIK untuk pengguna setelah implementasi dilakukan;
v. Terdapat dokumentasi hasil pelaksanaan implementasi dalam suatu Berita Acara. Berita Acara tersebut harus disetujui oleh personel operasional TIK yang melakukan implementasi, pengguna, manajer proyek, serta *IT Quality Assurance* atau Internal Audit.

g. Kaji Ulang Paska Implementasi

Kaji ulang paska implementasi dilakukan untuk memastikan bahwa seluruh aktivitas proyek telah dilaksanakan dan tujuan proyek tersebut telah tercapai. Untuk menilai efektivitas pelaksanaan proyek, KKKS melakukan analisa terhadap rencana dan realisasi biaya, manfaat yang diperoleh dan ketepatan jadwal proyek. Kaji ulang paska implementasi dilakukan oleh pihak yang independen.

h. Pemeliharaan

KKKS harus melakukan pemeliharaan terhadap sistem/infrastruktur TIK dan dokumentasi untuk mendukung terciptanya efektivitas operasional TIK. Hal tersebut dilakukan untuk meningkatkan kinerja sistem, memperbaiki masalah pada sistem/infrastruktur TIK, meningkatkan keamanan, dan menyediakan kebutuhan pengguna.Dengan demikian, KKKS harus memiliki metodologi pemeliharaan yang sesuai dengan karakteristik dan risiko sistem/infrastruktur TIK yang ada.

4. Manajemen Perubahan

Manajemen Perubahan atau *Change Management* adalah prosedur yang mengatur penambahan, penggantian, maupun penghapusan objek di lingkungan

produksi. Objek yang dimaksud dapat berupa data, program, menu, aplikasi, perangkat komputer, perangkat jaringan, dan proses.

Hal-hal yang perlu diperhatikan dalam melakukan manajemen perubahan adalah sebagai berikut, namun tidak terbatas pada:

a. Pengajuan perubahan dilakukan oleh pengguna dan disetujui oleh pihak yang memiliki otorisasi di dalam KKKS;
b. *Programmer* melakukan pengujian untuk memastikan integrasi antar modul pada saat melakukan perubahan;
c. Pengguna melakukan pengujian hasil perubahan untuk memastikan perubahan dilakukan sesuai dengan kebutuhan;
d. Pengujian dilakukan di lingkungan pengembangan yang terpisah dari lingkungan produksi dan data yang digunakan bukan data asli. Jika menggunakan data asli, data tersebut harus disamarkan;
e. Pengujian dilakukan berdasarkan skenario yang telah dibuat pengguna;
f. Hasil perubahan yang akan diimplementasikan, harus mendapatkan persetujuan fungsi *IT Quality Assurance*;
g. Dokumentasi perubahan harus disimpan dan dikelola dengan baik untuk mempermudah KKKS dalam melakukan penelusuran kembali jika terjadi gangguan pada sistem/infrastruktur TIK.

5. *Patch Management*

Untuk memperbaiki permasalahan, meningkatkan kinerja dan meningkatkan keamanan pada *software*, penyedia barang dan jasa secara rutin mengembangkan dan mengeluarkan *patches*. Jika terdapat *patch* baru, KKKS harus melakukan analisa dampak dari aspek teknis dan keamanan informasi atas instalasi *patch* terhadap operasional TIK. Oleh karena itu, KKKS harus memiliki kebijakan dan prosedur terkait *patch management* yang mencakup prosedur identifikasi, evaluasi, persetujuan, pengujian, instalasi, dan dokumentasi *patches*.

6. Kepemilikan Sistem/Infrastruktur TIK

Semua aset yang berwujud maupun tidak berwujud, termasuk di dalamnya sistem/infrastruktur TIK seperti lisensi dan *software*, berpindah menjadi milik

Negara yang dikelola oleh SKMIGAS pada saat dibeli dan berpindah tangan ke dalam penguasaan KKKS sebagaimana tertuang di dalam PTK 007

BAB VI
OPERASIONAL TEKNOLOGI INFORMASI DAN KOMUNIKASI

A. Pendahuluan

Operasional TIK tidak hanya terkonsentrasi pada layanan *Data Center*, namun juga pada aktivitas penggunaan aplikasi yang terintegrasi dan penggunaan komunikasi, PC, dan peralatan lain yang digunakan oleh *user*. Dalam menjalankan operasional TIK, KKKS memiliki risiko yang dapat menghambat operasional bisnis. Adapun risiko yang dapat timbul dalam pelaksanaan operasional TIK adalah risiko terganggunya kerahasiaan, integritas dan ketersediaan informasi, serta terganggunya layanan TIK yang diberikan. Oleh karena itu, untuk meminimalisasi terjadinya risiko tersebut diperlukan pengendalian yang memadai atas operasional TIK. KKKS juga perlu mempertimbangkan penerapan "*Go Green*" atau "*Green Computing*" dalam operasional TIK. Tujuan penerapan *Go Green* ini adalah sebagai upaya untuk meminimalisir dampak pada lingkungan, seperti penggunaan infrastruktur TIK yang hemat energi, pengurangan penggunaan material yang berbahaya, serta pengamanan pada disposal infrastruktur TIK.

Dalam pengendalian operasional TIK, KKKS bertanggung jawab kepada SKMIGAS sebagai lembaga hukum yang melakukan fungsi operasional usaha hulu minyak dan gas bumi di Indonesia.

1. Maksud dan Tujuan

a. Maksud

Pedoman ini dimaksudkan untuk memberikan arahan bagi KKKS dalam aktivitas operasional TIK, serta sebagai acuan dalam melakukan pengukuran kinerja proses operasional TIK.

b. Tujuan

Pedoman pengendalian dalam operasional TIK ditujukan untuk memberikan acuan bagi KKKS dalam membangun kebijakan, prosedur, proses, serta tata kerja operasional TIK yang sesuai dengan strategi bisnis dan kebutuhan KKKS. Pedoman ini juga menyajikan panduan untuk menjaga ketersediaan layanan TIK di lingkungan KKKS agar dapat digunakan sebaik-baiknya oleh pengguna.

Hasil yang diharapkan melalui implementasi pengendalian operasional TIK adalah keselarasan antara Cetak Biru TIK dengan strategi bisnis KKKS, tercapainya efisiensi dan efektivitas penggunaan sumber daya TIK, serta optimalisasi layanan TIK bagi bisnis.

B. Pengendalian Manajemen Teknologi Informasi dan Komunikasi

Dalam rangka menerapkan pengedalian manajemen TIK, KKKS harus memiliki suatu mekanisme atau kerangka manajemen risiko untuk melakukan proses identifikasi, pengukuran, pemantauan dan pengendalian risiko TIK. Kerangka manajemen risiko yang harus diterapkan dapat disesuaikan dengan fungsi dan organisasi TIK di masing-masing KKKS.

1. Organisasi Teknologi Informasi dan Komunikasi

KKKS perlu memiliki struktur organisasi TIK yang sesuai dengan kebutuhan penyelenggaraan dan pemanfaatan TIK. Hal-hal yang harus diperhatikan dalam struktur organisasi TIK adalah sebagai berikut, namun tidak terbatas pada:

a. Penyelenggara TIK merupakan satuan kerja yang terpisah dari fungsi operasional lainnya;
b. Struktur organisasi TIK harus menggambarkan garis kewenangan, pelaporan dan tanggung jawab untuk setiap fungsi yang harus dimiliki secara spesifik;
c. Terdapat prinsip pemisahan tugas dan tanggung jawab (*segregation of duties*). Prinsip tersebut bertujuan untuk mencegah kewenangan berlebih

sehingga menyebabkan kemungkinan kesalahan yang tidak mudah terdeteksi atau *fraud*;

d. Menerapkan pengendalian tambahan atau *compensanting controls* apabila tidak bisa menerapkan prinsip pemisahan tugas dan tanggung jawab yang memadai (*segregation of incompatible duties*) baik secara keseluruhan maupun sebagian. Dalam menentukan *compensating controls*, KKKS harus memperhatikan kepemilikan data, tanggung jawab dan hak akses ke data;
e. Mempertimbangkan *job specification* yang sesuai dengan posisi/jabatan pada saat melakukan penempatan personel.

2. Pengendalian Personel

KKKS harus menerapkan pengendalian personel untuk mendukung pelaksanaan operasional TIK secara maksimal. Hal-hal yang harus diperhatikan dalam pengendalian personel adalah sebagai berikut, namun tidak terbatas pada:

a. KKKS menetapkan prosedur untuk pengelolaan Sumber Daya Manusia (SDM), yang meliputi penerimaan pegawai baru, mutasi, promosi dan pemberhentian pegawai TIK;
b. Menetapkan tugas, tanggung jawab, harapan/target secara transparan;
c. Menetapkan standar penilaian kinerja, upah/gaji dan tunjangan, serta pensiun;
d. Program pendidikan atau pelatihan dan penilaian kinerja untuk mempertahankan dan meningkatkan kualitas para pegawai.

Dalam pelaksanaan pengendalian tersebut, KKKS harus mangacu PTK No.018/2008 tentang Pengelolaan Sumber Daya Manusia KKKS.

3. Cetak Biru Teknologi Informasi dan Komunikasi

KKKS harus memiliki rencana strategis dalam pemanfaatan TIK untuk mendukung visi, misi, dan kebutuhan bisnis KKKS. Strategi dalam penggunaan TIK harus tergambarkan dan terdokumentasikan dalam sebuah Cetak Biru TIK baik jangka pendek maupun jangka panjang. Cetak Biru TIK merupakan salah satu bentuk penerapan pengendalian dalam perencanaan dan organisasi TIK.

Dalam penyusunan Cetak Biru TIK, KKKS harus memperhatikan prinsip-prinsip penyusunan Cetak Biru TIK sebagai berikut, namun tidak terbatas pada:

a. Mempertimbangkan regulasi yang berlaku di wilayah Republik Indonesia, standar dan tren teknologi serta hasil penilaian kondisi lingkungan TIK;
b. Peranan TIK dalam mendukung pelaksanaan kegiatan KKKS;
c. Hubungan antara sumber daya TIK yang digunakan saat ini dan perencanaan kedepan;
d. Mempertimbangkan manfaat yang akan diperoleh dengan biaya yang akan dikeluarkan.

Hal-hal yang harus tercakup dalam dokumen Cetak Biru TIK adalah sebagai berikut, namun tidak terbatas pada:

a. Target perkembangan usaha KKKS;
b. Standar-standar teknologi yang digunakan;
c. Ketentuan perundangan yang mendasari (antara lain mengenai kerahasiaan data dan pengamanan data);
d. Rencana kebutuhan akan infrastruktur TIK dan sistem informasi dalam usaha meningkatkan produksi dan aktivitas baru;
e. Proses bisnis yang dibutuhkan dalam rangka efisiensi;
f. Road map implementasi Cetak Biru TIK;
g. Analisis kemampuan sumber daya TIK yang dimiliki KKKS;
h. Kemampuan untuk menyesuaikan dan mengintegrasikan dengan perkembangan teknologi baru; dan
i. Kemampuan bisnis untuk menyesuaikan dengan iklim perkembangan ekonomi Indonesia (secara makro).

Pengendalian Operasional Teknologi Informasi dan Komunikasi

Operasional TIK merupakan proses yang kritikal dalam penyelenggaraan layanan TIK unit bisnis, oleh karena itu KKKS harus memiliki suatu panduan berupa kebijakan dan prosedur untuk menjalankan operasional TIK. Kebijakan dan Prosedur Operasional TIK yang harus dimiliki oleh KKKS sekurang-kurangnya mencakup:

1. Operasional *Data Center*;

2. Pemeliharaan perangkat *Data Center*;
3. Pengendalian keamanan fisik dan lingkungan *Data Center*;
4. Pengelolaan *Computing Infrastructure*,
5. Pengelolaan kapasitas;
6. Pengelolaan konfigurasi infrastruktur TIK;
7. Penanganan insiden dan masalah;
8. *Management Information System*;
9. *Service Level Management*.

Penjelasan pengendalian pada masing-masing kebijakan dan prosedur akan dibahas pada sub bab berikutnya.

1. Operasional *Data Center*

Kebijakan dan prosedur operasional *Data Center* TIK harus didefinisikan dan diterapkan untuk mendukung proses dan keamanan informasi pada *Data Center*. Kebijakan dan prosedur operasional *Data Center* diperlukan sebagai standar panduan dalam melaksanakan aktivitas operasional *Data Center*, baik aktivitasrutin maupun non rutin. Hal-hal minimum yang harus diatur dan diterapkan pada operasional *Data Center* antara lain:

a. Lokasi *Data Center*

KKKS harus memperhatikan kondisi geografis untuk menetapkan posisi *Data Center.Data Center* wajib berada di wilayah hukum Negara Republik Indonesia.

b. Aktivitas Operasional *Data Center*

KKKS wajib memastikan semua aktivitas operasional *Data Center* dijalankan sesuai jadwal secara efektif dan efisien.

c. Proses *Backup*

KKKS harus memiliki kebijakan dan prosedur terkait dengan proses *backup* dan *restore* yang mencakup proses *on-site* dan *off-site*. Hal-hal yang harus diatur dalam kebijakan dan prosedur ini, namun tidak terbatas pada:

i. Data harus di *backup* secara periodik sesuai dengan kebutuhan;

ii. Data *backup* harus disimpan di lokasi terpisah dari lokasi *Data Center;*
iii. Media *backup* data harus disimpan di lokasi yang memiliki sistem pengamanan;
iv. *Full system backup* harus dilakukan secara berkala sesuai dengan kebutuhan. Apabila terjadi perubahan pada *operating system*, aplikasi dan *database* maka *full system backup* harus dilakukan sesegera mungkin;
v. Seluruh media *backup* perlu menggunakan penamaan agar mempermudah proses penggunaan, waktu dan jadwal retensi;
vi. Seluruh media *backup*harus dikaji secara berkala untuk memastikan dapat digunakan pada saat dibutuhkan;
vii. Proses *restore* harus melalui persetujuan dari pemilik data/*database* yang terkait.

d. Pengaktifan *Audit Trail*

Audit trail harus diaktifkan, didokumentasikan dan dikaji secara berkala untuk memastikan dapat dilakukan penelusuran balik pada saat dibutuhkan.

e. Pengawasan Kinerja *Hardware* dan *Software* pada *Data Center*

KKKS harus melakukan pengawasan atas kinerja *hardware* dan *software* secara rutin. Pengawasan kinerja tersebut bertujuan untuk memberikan informasi mengenai kinerja *hardware* dan *software* sebagai bahan acuan dalam melakukan perbaikan terhadap kinerja *hardware* dan *software* pada *Data Center*.

2. Pemeliharaan Perangkat *Data Center*

KKKS perlu melaksanakan pemeliharaan terhadap perangkat *Data Center.* Hal-hal yang harus dilakukan dalam melakukan pemeliharaan perangkat *Data Center* adalah sebagai berikut, namun tidak terbatas:

a. Melakukan perawatan secara berkala terhadap perangkat *Data Center*. Hal ini perlu dilakukan untuk meminimalkan kegagalan pengoperasian peralatan dan untuk mendeteksi permasalahan yang terjadi;

b. Merencanakan jadwal pemeliharaan agar proses pemeliharaan dan perawatan dapat terlaksana dengan baik;
c. Seluruh proses pemeliharaan dan perawatan harus terdokumentasikan dan dilakukan pemeriksaan secara berkala;
d. Perangkat *Data Center* harus diasuransikan.

3. Pengendalian Keamanan Fisik dan Lingkungan *Data Center*

KKKS perlu memiliki kebijakan dan prosedur terkait dengan pengendalian keamanan fisik dan lingkungan *Data Center*. Kebijakan dan prosedur tersebut harus selaras dengan kebijakan keamanan informasi yang dijelaskan pada bagian keamanan informasi. Hal ini untuk memitigasi risiko akses data oleh pihak-pihak yang tidak berwewenang. Hal-hal yang harus dipenuhi dalam pengendalian keamanan fisik *Data Center* adalah sebagai berikut, namun tidak terbatas pada:

a. Akses fisik ke *Data Center* harus dibatasi dan dikendalikan sesuai dengan kebijakan pengamanan informasi yang dimiliki oleh KKKS.
b. Perangkat pengendalian lingkungan *Data Center* seperti AC, *termometer, higrometer, water leak detection system, pest control*, alat pendeteksi asap/api/panas dan lain-lain harus dimonitor untuk memastikan fungsinya dapat mendukung operasional TIK.
c. Terdapat pemisahan jalur antara jalur data dan jalur listrik.

4. Pengelolaan *Computing Infrastructure*

Perangkat komputerisasi (*computing infrastructure*) yang digunakan oleh para pekerja KKKS baik berupa *Personal Computer* (PC), Laptop, Tablet dan lain-lainnya, harus dikelola dengan baik untuk menjamin keamanan dan kontinuitas perangkat tersebut. Dalam pengelolaan perangkat komputerisasi yang digunakan oleh *user*, KKKS harus memiliki kebijakan dan prosedur yang menjamin setiap berlangsungnya operasional penggunaan *computing infrastructure*. Hal-hal yang harus diperhatikan dalam pengelolaan perangkat komputerisasi adalah sebagai berikut, namun tidak terbatas pada;

a. Terdapat kebijakan yang menjelaskan pembagian dan penggunaan perangkat, serta peran dan tanggung jawab atas keamanan perangkat yang digunakan oleh pengguna;
b. Terdapatnya kebijakan dan prosedur yang mengatur *support* baik dari aspek *software*, *hardware* dan konfigurasi dari perangkat yang digunakan oleh *user*.

5. Pengelolaan Kapasitas

KKKS perlu memiliki kebijakan dan prosedur pengelolaan kapasitas. Kebijakan dan prosedur tersebut bertujuan sebagai pedoman untuk memastikan bahwa *hardware* dan *software* yang digunakan KKKS telah sesuai dengan kebutuhan operasional dan dapat mengantisipasi pertumbuhan data. Hal-hal yang harus dipenuhi dalam proses pengelolaan kapasitas adalah sebagai berikut, namun tidak terbatas pada:

a. Pemantauan dan pengukuran kapasitas infrastruktur TIK dilakukan secara rutin pada waktu yang telah ditentukan;
b. Hasil pemantauan dan pengukuran kapasitas infrastruktur TIK dijadikan dasar untuk memprediksi kebutuhan di masa yang akan datang.

6. Pengelolaan Konfigurasi TIK

KKKS perlu memiliki kebijakan dan prosedur terkait dengan pengelolaan konfigurasi TIK. Pengelolaan konfigurasi TIK bertujuan untuk mengoptimalkan sumber daya dan kemampuan infrastruktur TIK dalam memfasilitasi ketersediaan sistem yang lebih besar, terutama untuk menjaga tingkat interoperabilitas, keterpaduan, ketahanan dan integritas sistem untuk meminimalkan terjadinya masalah pada lingkungan produksi, serta dapat membantu menyelesaikan masalah dengan cepat. Hal-hal yang diatur dalam pengelolaan konfigurasi TIK adalah sebagai berikut, namun tidak terbatas pada:

a. Instalasi *hardware, software,* dan *network;*
b. Pengaturan parameter (*hardening*) *hardware*, *software* dan *network*;
c. Inventarisasi dan pemutakhiran dokumentasi konfigurasi *hardware, software,network*, media penyimpan dan perangkat pendukung lainnya.

7. Penanganan Insiden dan Masalah

KKKS *w*ajib memiliki kebijakan dan prosedur terkait dengan penanganan kejadian dan masalah. Kebijakan dan prosedur tersebut harus meliputi penanganan *hardware*, sistem aplikasi, perangkat jaringan dan keamanan informasi. Dalam penanganan insiden dan masalah hendaknya terdapat suatu fungsi atau personel yang ditunjuk bertanggung jawab terhadap proses tersebut, Insiden dan permasalahan yang terjadi harus didokumentasikan dan dilaporkan kepada pihak-pihak terkait.

8. *Management Information System*

KKKS yang telah menerapkan *management information system* (MIS) harus mempertimbangkan aspek-aspek *Confidentiality*, *Availability*, dan *Integrity*, yaitu dengan melakukan pembatasan hak akses logik MIS berdasarkan hak akses *user* serta pembatasan fisik. KKKS yang telah menerapkan MIS harus memiliki kebijakan dan prosedur yang mengatur penerapan MIS.

9. *Service Level Management*

Kerja sama dengan Penyedia Barang dan Jasa TIK memiliki risiko terhadap operasional, hukum, kepatuhan, dan reputasi yang dapat timbul karena kegagalan Penyedia Barang dan Jasa TIK dalam menyediakan jasa, pelanggaran terhadap pengamanan atau ketidakmampuan untuk memenuhi hukum dan peraturan yang berlaku. Untuk memastikan adanya pengendalian yang memadai terhadap layanan Penyedia Barang dan Jasa TIK, KKKS perlu menerapkan *Service Level Management* (SLM). Tujuan penerapan SLM untuk meyakinkan bahwa pemantauan layanan, pelaporan permasalahan dan dokumentasi terkait dengan layanan Penyedia Barang dan Jasa TIK dapat berjalan dengan baik. Oleh sebab itu KKKS harus menunjuk personel yang bertanggung jawab dalam memantau dan mengevaluasi kehandalan pihak Penyedia Barang dan Jasa TIK dalam menyediakan layanan secara berkala.

BAB VII

DISASTER RECOVERY PLAN

A. Pendahuluan

Kemajuan Teknologi Informasi dan Komunikasi (TIK) dapat meningkatkan efisiensi dan efektivitas kegiatan usaha hulu minyak dan gas bumi. Penggunaan TIK memiliki ketergantungan yang tinggi terhadap ketersediaan layanan TIK agar dapat menunjang operasional. Penggunaan TIK juga dapat meningkatkan risiko terganggunya kerahasiaan, integritas, dan ketersediaan informasi yang harus dimitigasi oleh setiap pengguna.

Kegiatan operasional TIK tidak terlepas dari adanya bencana yang diakibatkan oleh kejadian alam (*force majeure*), manusia (*human error*) dan teknologi. Bencana perlu diantisipasi sedini mungkin dengan mempersiapkan rencana yang berkesinambungan atas layanan TIK dan langkah-langkah pemulihan untuk sistem informasi yang kritikal. Oleh sebab itu KKKS perlu memiliki *Disaster Recovery Plan* (DRP). DRP merupakan suatu rencana pemulihan yang fokus pada pemulihan layanan TIK.

1. Maksud dan Tujuan

a. Maksud

Pedoman ini dimaksudkan untuk memberikan arahan kepada KKKS agar memiliki suatu mekanisme pemulihan layanan TIK yang memadai dan sesuai dengan karakteristik operasional KKKS. *Disaster Recovery Plan* berfokus pada pemulihat layanan TIK saat terjadi bencana.

b. Tujuan

Pedoman *Disaster Recovery Plan* ditujukan sebagai panduan implementasi pengendalian dalam meminimalkan dampak bencana bagi KKKS. Implementasi dari pedoman ini diupayakan sebagai salah satu upaya pemulihan layanan TIK di KKKS pasca terjadinya bencana.

Melalui implementasi pedoman ini, diharapkan KKKS dapat menjaga keberlangsungan usahanya, sehingga terjadinya bencana tidak berdampak signifikan pada operasional KKKS.

B. Penerapan Pengendalian dalam *Disaster Recovery Plan*

1. Penyusunan *Disaster Recovery Plan* (DRP)

Dalam penyusunan *Disaster Recovery Plan* perlu dilakukan identifikasi terhadap sistem yang kritikal serta penentuan rencana pemulihan melalui proses Penilaian Risiko dan *Business Impact Analysis* (BIA). KKKS harus menerapkan prinsip-prinsip DRP, yaitu:

a. Penyusunan DRP harus melibatkan seluruh satuan kerja dan fungsi bisnis yang terdapat pada KKKS;
b. DRP harus didukung dan memperoleh komitmen dari pihak Top Manajemen;
c. DRP disusun berdasarkan proses penilaian risiko dan BIA;
d. DRP bersifat menyeluruh agar dapat merespon berbagai macam skenario bencana yang tidak terduga;
e. DRP bersifat spesifik agar mudah diimplementasikan jika terjadi bencana;
f. Pengujian DRP harus dilakukan secara berkala;
g. DRP dan hasil pengujian DRP harus dikaji ulang secara berkala.

Proses Penilaian Risiko dan BIA akan dibahas pada sub bab selanjutnya.

a. Penilaian Risiko

Penilaian Risiko *(Risk Assessment)* merupakan proses analisa risiko terhadap bencana dan dampaknya yang mungkin terjadi pada kegiatan operasional KKKS.

Berikut adalah hal-hal yang harus diperhatikan dalam melakukan penilaian risiko, namun tidak terbatas pada:

i. Tingkatan potensi bencana bisnis berdasarkan tingkat kerusakan *(severity)* dan kemungkinan terjadinya bencana;
ii. Analisa dampak bencana terhadap KKKS;

iii. *Gap analysis,* yaitu membandingkan kondisi saat ini dengan langkah atau mitigasi yang seharusnya diterapkan.

Dalam pelaksanaannya tidak tertutup kemungkinanan adanya aspek lain yang ikut dalam penilaian risiko.

b. *Business Impact Analysis*

Business Impact Analysis (BIA) harus dilakukan secara sistematis untuk menentukan prioritas pemulihan berdasarkan besarnya dampak terhadap operasional KKKS. BIA merupakan kajian menyeluruh terhadap dampak yang akan dialami oleh KKKS apabila sebuah bencana terjadi.

Penyusunan BIA harus dilakukan melalui analisa terhadap aspek-aspek berikut, namun tidak terbatas pada:

i. Tingkat kepentingan kritikal pada ketersediaan data dan aplikasi di masing-masing proses bisnis, dan ketergantungan antar proses bisnis, serta penentuan tingkat prioritas;
ii. Terdapat faktor-faktor finansial yang dijadikan dasar penentuan estimasi besarnya kerugian terhadap KKKS akibat adanya bencana;
iii. Tingkat ketergantungan terhadap ketersediaan layanan Penyedia Barang dan Jasa;
iv. Estimasi *maximum downtime* yang dapat ditoleransi atas kehilangan data dan terhentinya proses bisnis, yang meliputi seperti di bawah ini:
    a) *Recovery Time Objective* (RTO);

    RTO merupakan waktu yang dibutuhkan untuk memulihkan sistem dan sumber daya yang mengalami bencana agar dapat berfungsi kembali, atau dapat disebut sebagai sasaran waktu pemulihan;

    b) Analisa tingkat*Recovery Point Objective* (RPO);

    RPO merupakan tingkat maksimum waktu kehilangan data yang dapat ditoleransi oleh masing-masing proses bisnis;

v. Dampak bencana terhadap seluruh fungsi di KKKS;

vi. Alternatif jaringan komunikasi yang dibutuhkan untuk berjalannya pemulihan;

vii. Dampak hukum dan pemenuhan ketentuan yang terkait, seperti ketentuan kerahasiaan data;

viii. Penentuan strategi pemulihan DRC (*hot site, warm site* atau *cold site*).

2. *Disaster Recovery Plan* (DRP)

DRP terdiri dari kebijakan, strategi, skenario, prosedur dan kriteria bencana yang diperlukan untuk dapat memastikan kelangsungan proses bisnis pada saat terjadinya bencana. Strategi pemulihan disusun berdasarkan hasil BIA, penilaian risiko, sumber daya yang dimiliki, serta kapasitas dan teknologi informasi KKKS. DRP harus menjadi bagian dalam *Business Continuity Management* (BCM).

Berikut adalah hal-hal yang harus diperhatikan dalam penyusunan DRP, namun tidak terbatas pada:

a. Jenis-jenisProsedur dalam DRP

Hal-hal yang harus diperhatikan dalam prosedur DRP, namun tidak terbatas pada:

i. Prosedur tanggap darurat

Prosedur yang mengendalikan krisis pada saat terjadi bencana, menentukan perlu tidaknya mendeklarasikan keadaan bencana serta menjalankan prosedur pemulihan sistem.

ii. Prosedur pemulihan sistem

Prosedur yang mengatur proses pemulihan sistem informasi untuk kembali normal.

iii. Prosedur sinkronisasi data

Prosedur yang digunakan untuk memastikan kesamaan antara data produksi dengan data yang ada di DRC, serta untuk memastikan semua data hasil pemrosesan bisnis selama masa pemulihan telah masuk ke dalam sistem.

b. Komponen Prosedur DRP

Hal-hal yang harus diperhatikan dalam komponen prosedur DRP adalah sebagai berikut, namun tidak terbatas pada:

i. Personel;

Memiliki struktur organisasi DRP yang bertanggung jawab untuk melakukan koordinasi, prosedur tanggap darurat, pemulihan sistem, dan sinkronisasi data terhadap proses pemulihan.

ii. Infrastruktur TIK;

Memiliki infrastruktur TIK yang dapat menunjang ketersediaan layanan TIK pada kegiatan operasional KKKS.

iii. *Disaster Recovery Center* (DRC);

Memiliki DRC sebagai *backup Data Center* yang dapat digunakan pada saat terjadinya bencana.

iv. *Backup* Dokumentasi, Data, Aplikasi, dan Alat Komunikasi;

Memiliki *backup* dokumentasi, data, aplikasi, dan alat komunikasi yang dapat digunakan pada saat terjadinya bencana.

c. Struktur Organisasi DRP

KKKS harus membentuk struktur organisasi DRP yang bertanggung jawab terhadap pengelolaan DRP ketika kondisi normal dan terjadi bencana. Peran dan tanggung jawab struktur organisasi DRP harus ditetapkan dan disahkan oleh pihak manajemen KKKS. Struktur Organisasi DRP, minimal terdiri dari:

i. Koordinator;
ii. Tim pemulihan yang meliputi:
   a) Infrastruktur dan Telekomunikasi;
   b) *Software* TIK;
   c) Satuan Pendukung Kerja lainnya.

d. Rencana Alur Komunikasi

KKKS harus memiliki suatu rencana atau mekanisme komunikasi yang digunakan ketika terjadi bencana untuk menginformasikan kondisi darurat. Hal-hal yang harus diperhatikan dalam rencana komunikasi adalah sebagai berikut, namun tidak terbatas pada:

i. Informasi mengenai siapa yang harus dihubungi;
ii. Apa yang dikomunikasikan;
iii. Seberapa sering komunikasi dilakukan;
iv. Media komunikasi yang digunakan.

Anggota dalam struktur organisasi DRP harus memiliki daftar orang-orang yang harus dihubungi apabila suatu bencana terjadi.

Ketika terjadi bencana, KKKS wajib melaporkan kondisi tersebut kepada (*Emergency Response Center*) di SKMIGAS.

e. Kriteria Bencana

Penyusunan DRP tidak saja untuk total *disaster*, namun untuk berbagai kemungkinan situasi bencana yang dapat saja terjadi. Oleh karena itu KKKS harus memiliki suatu kriteria bencana serta dampaknya terhadap layanan TIK. Setiap kriteria bencana yang ditetapkan harus dilengkapi dengan tindakan penyelesaian yang dilakukan.

3. *Disaster Recovery Center* (DRC)

Disaster Recovery Center adalah suatu lokasi alternatif yang digunakan sementara waktu ketika *Data Center* tidak dapat berfungsi akibat bencana untuk menjaga kelangsungan kegiatan usaha.

DRC sekurang-kurangnya memenuhi ketentuan berikut:

a. DRC harus merupakan *restricted area* yang ditempatkan pada lokasi terpisah dari *Data Center*, dan berada di wilayah Republik Indonesia;
b. DRC harus memiliki keamanan fisik yang minimal sama dengan *Data Center*;
c. DRC harus memiliki sarana listrik dan telekomunikasi yang dapat menjamin kelangsungan operasionalnya dan dapat menggantikan fungsi operasional *Data Center;*
d. Sistem DRC harus disesuaikan dengan sistem yang digunakan pada *Data Center* dan harus disesuaikan jika terjadi perubahan pada *Data Center.*

4. Pengujian DRP

DRP harus diuji secara berkala untuk memastikan kesiapan personel, dan infrastruktur TIK yang akan digunakan ketika terjadi bencana. Pengujian tersebut minimum dilakukan 1 tahun sekali. Skenario pengujian yang ditetapkan harus mengacu pada strategi, kebijakan dan prosedur yang ada di dalam DRP.

a. Ruang lingkup Pengujian

Hal-hal yang harus diperhatikan dalam ruang lingkup pengujian adalah sebagai berikut, namun tidak terbatas pada:

i. Prosedur komunikasi yang telah ditetapkan (*calling tree*);
ii. Prosedur penetapan kondisi bencana;
iii. Kesiapan fasilitas D*isaster Recovery Center;*
iv. Prosedur pemulihan sistem informasi yang kritikal;
v. Pengembalian kegiatan operasional TIK dan pengaktifan kembali *Data Center*

b. Jenis Pengujian DRP

Pengujian DRP dapat dilakukan dengan menggunakan salah satu metode pengujian yang ada di bawah ini.

i. *Checklist Testing*

i. Koordinator;
ii. Tim pemulihan yang meliputi:
   a) Infrastruktur dan Telekomunikasi;
   b) *Software* TIK;
   c) Satuan Pendukung Kerja lainnya.

d. Rencana Alur Komunikasi

KKKS harus memiliki suatu rencana atau mekanisme komunikasi yang digunakan ketika terjadi bencana untuk menginformasikan kondisi darurat. Hal-hal yang harus diperhatikan dalam rencana komunikasi adalah sebagai berikut, namun tidak terbatas pada:

i. Informasi mengenai siapa yang harus dihubungi;
ii. Apa yang dikomunikasikan;
iii. Seberapa sering komunikasi dilakukan;
iv. Media komunikasi yang digunakan.

Anggota dalam struktur organisasi DRP harus memiliki daftar orang-orang yang harus dihubungi apabila suatu bencana terjadi.

Ketika terjadi bencana, KKKS wajib melaporkan kondisi tersebut kepada (*Emergency Response Center*) di SKMIGAS.

e. Kriteria Bencana

Penyusunan DRP tidak saja untuk total *disaster*, namun untuk berbagai kemungkinan situasi bencana yang dapat saja terjadi. Oleh karena itu KKKS harus memiliki suatu kriteria bencana serta dampaknya terhadap layanan TIK. Setiap kriteria bencana yang ditetapkan harus dilengkapi dengan tindakan penyelesaian yang dilakukan.

3. *Disaster Recovery Center* (DRC)

Disaster Recovery Center adalah suatu lokasi alternatif yang digunakan sementara waktu ketika *Data Center* tidak dapat berfungsi akibat bencana untuk menjaga kelangsungan kegiatan usaha.

DRC sekurang-kurangnya memenuhi ketentuan berikut:

a. DRC harus merupakan *restricted area* yang ditempatkan pada lokasi terpisah dari *Data Center*, dan berada di wilayah Republik Indonesia;
b. DRC harus memiliki keamanan fisik yang minimal sama dengan *Data Center*;
c. DRC harus memiliki sarana listrik dan telekomunikasi yang dapat menjamin kelangsungan operasionalnya dan dapat menggantikan fungsi operasional *Data Center;*
d. Sistem DRC harus disesuaikan dengan sistem yang digunakan pada *Data Center* dan harus disesuaikan jika terjadi perubahan pada *Data Center*.

4. Pengujian DRP

DRP harus diuji secara berkala untuk memastikan kesiapan personel, dan infrastruktur TIK yang akan digunakan ketika terjadi bencana. Pengujian tersebut minimum dilakukan 1 tahun sekali. Skenario pengujian yang ditetapkan harus mengacu pada strategi, kebijakan dan prosedur yang ada di dalam DRP.

a. Ruang lingkup Pengujian

Hal-hal yang harus diperhatikan dalam ruang lingkup pengujian adalah sebagai berikut, namun tidak terbatas pada:

i. Prosedur komunikasi yang telah ditetapkan (*calling tree*);
ii. Prosedur penetapan kondisi bencana;
iii. Kesiapan fasilitas D*isaster Recovery Center;*
iv. Prosedur pemulihan sistem informasi yang kritikal;
v. Pengembalian kegiatan operasional TIK dan pengaktifan kembali *Data Center*

b. Jenis Pengujian DRP

Pengujian DRP dapat dilakukan dengan menggunakan salah satu metode pengujian yang ada di bawah ini.

i. *Checklist Testing*

Merupakan pengujian yang memastikan ketersediaan komponen-komponen DRP, meliputi antara lain:

a) Verifikasi jalur komunikasi darurat;
b) Validasi prosedur utama;
c) Dokumentasi konfigurasi *hardware* dan *software* yang terbaru dan terlengkap;
d) Ketersediaan sumber daya;
e) Rencana pemulihan dan manual operasional yang diperlukan.

ii. *Walk-Through Testing*

Merupakan pengujian yang dilakukan berdasarkan prosedur-prosedur yang ada di dalam DRP. *Walk-Through Testing* bertujuan untuk memastikan efektivitas, identifikasi gap atau kelemahan pada DRP. Pengujian ini sebaiknya dilakukan bersamaan dengan *Check list Testing*.

iii. *Simulation Testing*

Merupakan pengujian dengan melakukan simulasi berdasarkan skenario yang telah dirancang. Pengujian simulasi ini bertujuan untuk melihat kesiapan personel dalam menghadapi bencana.

iv. *Full-Interuption Testing*

Merupakan pengujian yang mengkondisikan KKKS dalam keadaan bencana sesungguhnya dengan mematikan seluruh sistem. Pengujian ini bertujuan untuk menguji akurasi rencana pemulihan.

c. Analisis dan Pelaporan Hasil Pengujian DRP

Hasil pengujian DRP harus didokumentasikan dan dilaporkan kepada SKMIGAS. Hal-hal yang harus diperhatikan dalam laporan analisa hasil pengujian DRP, namun tidak terbatas pada:

i. Penilaian terhadap tercapainya tujuan pengujian;
ii. Penilaian terhadap validitas pengujian pemrosesan data;
iii. Tindakan perbaikan dalam mengatasi permasalahan yang terjadi;

iv. Deskripsi mengenai kesenjangan antara DRP dan hasil pengujian serta usulan perubahannya;
v. Rekomendasi yang diajukan untuk pengujian selanjutnya.

d. Pemeliharaan Dokumen DRP

Pemeliharaan dokumen DRP dilakukan untuk memastikan dan menjaga agar dokumen dapat tetap digunakan untuk mempertahankan kelangsungan layanan TIK dan meminimalisir dampak yang timbul dari bencana. Proses pemeliharaan mencakup proses evaluasi serta pemutakhiran dokumen jika diperlukan. Pemutakhiran dokumen DRP dapat dilakukan berdasarkan hasil pengujian dan ketika terjadi perubahan pada lingkungan KKKS, baik perubahan pada proses bisnis, organisasi, kebijakan, dan prosedur yang mempengaruhi dokumen DRP. Proses pemutakhiran dokumen DRP harus disetujui oleh pihak manajemen KKKS.

BAB VIII

AUDIT INTERNAL TEKNOLOGI INFORMASI DAN KOMUNIKASI

A. Pendahuluan

Pengawasan atas penerapan TIK di KKKS perlu dilakukan untuk menilai efisiensi dan efektivitas pengendalian TIK. Untuk memastikan kegiatan operasional dan pengendalian internal tersebut berjalan efektif sesuai dengan peraturan dan kebijakan yang telah ditetapkan oleh SKMIGAS, KKKS harus melakukan suatu kegiatan audit TIK sebagai bentuk pengawasan dan pengendalian internal.

Dalam melakukan penyelenggaraan audit TIK, KKKS harus menetapkan suatu fungsi dan pedoman audit TIK dengan mengacu kepada PTK ini. Penyelenggaraan audit TIK juga dapat dilakukan dengan menggunakan jasa auditor eksternal.

1. Maksud dan Tujuan

a. Maksud

Pedoman ini dimaksudkan sebagai panduan bagi KKKS dalam melaksanakan pemeriksaan terhadap efektivitas dari pengendalian internal TIK.

b. Tujuan

Pedoman audit internal TIK ditujukan untuk memberikan acuan bagi KKKS dalam melaksanakan audit TIK yang sesuai dengan kaidah audit berbasis risiko. Pedoman ini menjabarkan fungsi audit TIK, serta pedoman dan prosedur audit TIK yang perlu diterapkan oleh KKKS sesuai dengan karakteristik kegiatan dan besarnya layanan TIK yang diberikan pada bisnis.

Hasil yang diharapkan dari implementasi pedoman ini adalah meningkatnya efisiensi dan efektivitas pengendalian dalam penerapan fungsi pengawasan operasional TIK dan memastikan ketaatan KKKS pada aturan dan prosedur yang berlaku.

B. Penerapan Pengendalian dalam Audit TIK

1. Pedoman Audit Internal TIK

Pedoman audit internal TIK adalah kebijakan, prosedur, dan standar yang dapat dijadikan acuan oleh Auditor TIK, baik itu Auditor Internal TIK atau auditor eksternal yang ditunjuk oleh KKKS. Pedoman ini harus disetujui oleh Komite Audit dan dapat digunakan untuk setiap tahap dalam siklus audit. Secara umum, pedoman audit TIK harus mengatur proses penyusunan *Audit Charter*, penilaian risiko, perencanaan audit TIK, pelaksanaan audit, laporan audit, dan tindak lanjut audit TIK.

a. Penyusunan *Audit Charter*

Penyusunan *Audit Charter* ditujukan untuk menetapkan keberadaan dan berfungsinya suatu Auditor Internal TIK dalam KKKS. *Audit Charter* merupakan landasan pelaksanaan kegiatan audit bagi Auditor Internal TIK. Oleh karena itu, KKKS harus memiliki *Audit Charter* dan memastikan audit TIK tercakup dalam ruang lingkup audit.

Audit Charter harus ditinjau secara periodik untuk menilai apakah hal-hal minimum yang tercakup di dalamnya tetap memadai dan memungkinkan aktivitas audit internal TIK mencapai tujuannya.

b. Penilaian Risiko

Dalam melakukan audit, KKKS perlu melakukan penilaian risiko. Tujuan penilaian risiko adalah mengidentifikasi risiko yang terdapat di dalam proses bisnis KKKS. Penilaian risiko tersebut dijadikan dasar untuk perencanaan audit internal TIK dan penentuan prosedur pengendalian.

Hal-hal minimum yang harus dilakukan dalam penilaian risiko adalah sebagai berikut:

i. Menerapkan rencana audit yang meliputi pelaksanaan, pelaporan, dan tindak lanjut, pemantauan, dan pembaharuan penilaian risiko secara rutin minimal 1 (satu) tahun sekali untuk seluruh unit bisnis, departemen, produk atau sistem yang kritikal;

ii. Mengidentifikasi data, aplikasi, sistem operasi, teknologi, fasilitas, dan personel KKKS;
iii. Mengidentifikasi aktivitas dan proses bisnis yang menggunakan TIK;
iv. Mengidentifikasi profil dari unit bisnis, departemen, dan lini produk, atau sistem kritikal;
v. Menggunakan pengukuran atau sistem penilaian yang menggolongkan dan mengevaluasi risiko operasional dan pengendalian risiko terhadap unit bisnis, departemen, dan produk (misal: data, aplikasi, proses bisnis) kritikal;
vi. Mendapatkan persetujuan untuk melakukan penilaian risiko dan rencana audit berbasis risiko tahunan dari Manajemen dan Komite Audit dengan menetapkan jadwal, siklus, ruang lingkup program kerja, dan alokasi sumber daya untuk setiap area yang diaudit.

c. Pelaksanaan Audit TIK

Secara umum, pelaksanaan audit internal TIK terdiri atas tahapan-tahapan sebagai berikut:

i. Perencanaan Audit TIK

Perencanaan audit ditetapkan berdasarkan penilaian risiko yang telah dilakukan. Secara umum, perencanaan audit TIK harus mencakup hal-hal berikut:

a) Organisasi, kewenangan dan tanggung jawab Auditor Internal TIK;
b) Tujuan, jadwal, sumber daya (staf dan anggaran) yang dibutuhkan, serta pelaporan audit TIK;
c) Ruang lingkup audit TIK yang ditetapkan;
d) Prosedur audit dan langkah teknis.

Terdapat 2 jenis audit yang dapat dilakukan, yaitu Audit Regular dan Audit *Ad Hoc*. Audit Regular dan Audit *Ad Hoc* dapat dilakukan oleh fungsi Auditor Internal TIK atau auditor eksternal. Audit Regular terhadap penyelenggaraan TIK harus dilaksanakan sekurang-kurangnya 1 (satu) kali dalam setahun, sedangkan Audit *Ad Hoc* dapat dilakukan sewaktu-waktu untuk memeriksa objek yang dipandang bermasalah. Contoh Audit *Ad Hoc* adalah:

i) Audit forensik dan/atau investigatif

Audit ini dapat dilakukan sebagai langkah pemeriksaan untuk mendukung proses hukum apabila terdapat dugaan penyimpangan atau kecurangan dalam pemanfaatan sistem TIK di KKKS yang dapat merugikan KKKS maupun Negara Republik Indonesia;

ii) Audit atas Permintaan *Auditee*

Audit ini dapat dilakukan apabila manajemen atau kepala unit memerlukan input dari Auditor Internal TIK untuk mengevaluasi kelayakan dan keefektifan pengendalian internal serta pengaruhnya terhadap operasi yang berada di bawah supervisinya.

ii. Pelaksanaan Audit TIK

Pelaksanaan audit TIK dilakukan berdasarkan perencanaan dan prosedur yang telah ditetapkan sebelumnya. Dalam setiap pelaksanaan audit TIK, *audit working program* (AWP) harus disusun dan dilengkapi berdasarkan pada perencanaan audit yang telah disusun sebelumnya. Semua bukti-bukti, AWP dan kertas kerja harus didokumentasikan.

iii. Laporan Audit TIK

Laporan hasil audit TIK KKKS harus mencakup informasi sekurang-kurangnya:

a) Hasil *review* terhadap efektivitas pengendalian;
b) *Audit rating* (*low, medium, high*);
c) Analisis sebab akibat;
d) Tanggapan dari pihak Manajemen;
e) Rekomendasi perbaikan;
f) Target perbaikan;
g) Tindak lanjut hasil audit.

Salinan laporan hasil audit TIK disampaikan kepada SKMIGAS atas permintaan dari SKMIGAS.

iv. Tindak lanjut Audit TIK

Beberapa hal yang perlu diperhatikan oleh *auditee* pada saat melakukan tindak lanjut audit TIK adalah sebagai berikut:

a) Tanggapan terhadap hasil pemeriksaan dan target waktu penyelesaian perbaikan;
b) Pemantauan, pemeriksaan secara berkala, serta verifikasi terhadap tindakan perbaikan yang sudah dilakukan.

Salinan tindak lanjut audit disampaikan kepada SKMIGAS atas permintaan dari SKMIGAS.

d. Objek Audit TIK

Audit TIK merupakan bentuk pengawasan dan pengendalian secara menyeluruh terhadap kegiatan operasional dan infrastruktur TIK. Objek audit TIK mencakup antara lain:

i. Sistem dan Aplikasi;
ii. Operasional;
iii. Kepatuhan;
iv. Penyedia barang dan jasa.

2. Fungsi Auditor Internal TIK

Auditor internal TIK berperan sebagai fungsi penilai yang independen dengan tujuan untuk menguji dan mengevaluasi kegiatan TIK dalam KKKS. Auditor internal TIK terdiri dari fungsi, metode, dan *tools* yang digunakan di dalam KKKS dengan tujuan untuk:

a. Menjamin pelaksanaan keamanan data dan informasi berjalan efektif;
b. Memberikan rekomendasi yang diperlukan atas hasil audit TIK;
c. Mendorong efisiensi penerapan pengendalian TIK di internal KKKS;
d. Mendorong dipatuhinya PTK TIK yang telah ditetapkan.

Pelaksanaan audit TIK melibatkan Komite Audit dan Auditor Internal TIK di KKKS dimana masing-masing pihak telah memiliki peran dan tanggung jawab yang melekat dalam *Audit Charter*. Komite Audit dan Fungsi Auditor Internal TIK KKKS merupakan unit independen di dalam struktur organisasi KKKS yang harus disahkan dan memiliki *job*. Auditor Internal TIK bertanggung jawab kepada Komite Audit. Berikut adalah contoh peran dan tanggung jawab Komite Audit dan Auditor Internal TIK:

a. Komite Audit

Peran dan tanggung jawab utama dari Komite Audit mencakup hal-hal sebagai berikut, namun tidak terbatas pada:

i. Melakukan pemantauan dan evaluasi atas perencanaan dan pelaksanaan audit TIK;
ii. Memantau tindak lanjut atas hasil temuan dari audit TIK.

b. Auditor Internal TIK

Peran dan tanggung jawab Auditor Internal TIK mencakup hal-hal sebagai berikut, namun tidak terbatas pada:

i. Menyusun dan memperbaharui pedoman kerja yang sekurang-kurangnya mencakup standar baku prosedur pemeriksaan, kertas kerja, dan pelaporan hasil pemeriksaan;
ii. Mengidentifikasi ruang lingkup yang akan menjadi fokus audit;

iii. Memastikan penerapan prinsip kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) TIK;
iv. Melakukan evaluasi terhadap fungsi dan kecukupan pengendalian internal TIK;
v. Mengevaluasi efisiensi dan efektivitas perencanaan dan pengawasan penyelenggaraan TIK;
vi. Mengevaluasi kepatuhan terhadap ketentuan perundang-undangan, peraturan SKMIGAS, peraturan internal KKKS, dan kesesuaian dengan standar internasional terkait TIK (seperti ISO, IEC, COBIT, IT-IL);
vii. Menyampaikan rekomendasi untuk perbaikan atas kekurangan aspek-aspek TIK sesuai dengan hasil audit;
viii. Melakukan pemantauan terhadap tindak lanjut atas hasil audit;
ix. Melakukan pelaporan terkait hasil audit kepada SKMIGAS.

3. Audit TIK oleh Pihak Ketiga (Auditor Eksternal)

Dalam hal audit TIK dilakukan oleh pihak ketiga karena kebutuhan independensi ataupun keterbatasan kemampuan Auditor Internal TIK dari aspek kualitas, maupun dari aspek sumber daya yang dibutuhkan dalam pelaksanaan audit internal TIK, KKKS harus mempertimbangkan hal-hal berikut:

a. Auditor Eksternal yang ditunjuk memiliki pengetahuan dan pengalaman yang memadai serta mampu menjaga independensi dan objektivitasnya selama penugasan audit berlangsung;
b. Prosedur audit yang digunakan oleh Auditor Eksternal harus mengacu pada kebijakan dan prosedur audit TIK yang telah ditetapkan KKKS dan tidak bertentangan dengan ketentuan SKMIGAS;
c. Auditor Eksternal mempunyai kewenangan yang jelas mengenai akses terhadap bagian dan unit lainnya serta dokumentasi, dalam rangka mendapatkan informasi untuk kepentingan pelaksanaan tugas Auditor Internal TIK;
d. Auditor Internal TIK tetap bertanggung jawab atas temuan dan tindak lanjut audit yang dilaksanakan oleh Auditor Eksternal.

4. Audit terhadap Fungsi Audit Internal TIK KKKS

KKKS perlu memastikan kegiatan operasional dan pengendalian internal yang dilaksanakan berjalan efisien dan efektif sesuai dengan PTK TIK. Untuk itu, diperlukan suatu audit terhadap Auditor Internal TIK. Audit ini dilakukan sebagai bentuk pengawasan terhadap KKKS untuk memastikan efektivitas pelaksanaan dari Auditor Internal TIK KKKS.

Audit ini dilaksanakan sekurang-kurangnya 2 (dua) tahun sekali oleh auditor eksternal yang ditunjuk oleh KKKS. Laporan audit dan hasil tindak lanjut audit disampaikan kepada SKMIGAS atas permintaan SKMIGAS.

BAB IX
SANKSI

SKMIGAS melaksanakan pengawasan dan audit secara regular dan *ad hoc* atas kepatuhan KKKS terhadap PTK TIK ini. Apabila berdasarkan hasil pengawasan dan audit tersebut ditemukan bahwa KKKS tidak patuh, lalai atau sengaja melakukan pelanggaran terhadap PTK TIK, maka SKMIGAS akan melakukan pembinaan kepada KKKS terkait.

Kegiatan pembinaan tersebut mencakup pemberian rekomendasi serta konsultansi yang dapat membantu proses perbaikan TIK selama kurun waktu yang disepakati bersama antara SKMIGAS dan KKKS. Apabila dalam kurun waktu tersebut KKKS tidak melakukan perbaikan sesuai dengan rekomendasi, maka SKMIGAS berhak untuk menerapkan sanksi sesuai dengan mekanisme yang berlaku berdasarkan peraturan dan perundangan.

Sanksi yang dapat dikenakan kepada KKKS atas pelanggaran terhadap PTK ini adalah sebagai berikut:

1. KKKS yang bersangkutan diberi surat peringatan oleh SKMIGAS. Selanjutnya kepada pihak atau fungsi KKKS yang melakukan pelanggaran diberikan Surat Peringatan oleh Pimpinan KKKS;
2. Dalam hal penyimpangan dari ketentuan yang sejenis berulang lebih dari 2 (dua) kali, maka pihak atau fungsi KKKS yang melakukan pelanggaran diberikan sanksi administratif sesuai dengan derajat tanggungjawabnya;
3. Setiap individu yang terbukti melakukan pelanggaran terhadap PTKTIK dapat dikenakan sanksi sesuai dengan PTK Nomor 018/PTK/X/2008 Fungsi Pendayagunaan Tenaga Kerja dan Hubungan Industrial perihal Pemutusan Hubungan Kerja (PHK) dan *Mutual Agreement Termination* (MAT) dan Undang-undang Nomor 13 Tahun 2003 tentang Ketenagakerjaan;
4. KKKS yang terbukti melakukan pelanggaran atas ketentuan dalam PTK ini akan mendapatkan penundaan *placed into service* (PIS) atau penghentian sistem atau fasilitas TIK terkait yang terjadi pelanggaran. Waktu penundaan disesuaikan dengan

hasil pemeriksaan SKMIGAS dan dampak yang dapat dialami oleh Negara akibat pelanggaran tersebut;

5. Pengembalian biaya operasi yang telah dikeluarkan oleh KKKS dapat dibatalkan (*non cost recovery*) apabila KKKS terbukti melakukan kegiatan yang bertentangan dengan PTK ini.

BAB X
PENUTUP

A. Ketentuan Peralihan

1. Seluruh kegiatan KKKS yang terkait dengan TIK harus menyesuaikan kegiatannya dengan seluruh PTK ini;
2. Selama belum terdapat Pedoman Tata Kerja yang merupakan penjabaran detil dari PTK ini, maka setiap kegiatan yang terkait dengan penerapan TIK, KKKS harus berkonsultasi dengan SKMIGAS terlebih dahulu;
3. Masa penyesuaian untuk penerapan sepenuhnya PTK ini adalah 1 (satu) tahun setelah tanggal berlakunya ketentuan sebagaimana dinyatakan dalam Surat Keputusan tentang Penerapan Tata Kelola TIK;
4. Apabila terdapat ketentuan dalam PTK ini yang bertentangan dengan peraturan perundang-undangan yang berlaku di wilayah Negara Republik Indonesia, maka ketentuan tersebut tidak berlaku dan mengikuti peraturan perundang-undangan tersebut. Ketentuan lain yang tidak bertentangan tetap berlaku sebagaimana mestinya.

B. Ketentuan Lain-lain

Hal-hal yang belum atau belum cukup diatur dalam pedoman ini, akan diatur kemudian oleh SKMIGAS, berupa sisipan dan/atau penambahan lampiran pada PTK ini.

KEPALA