LAMPIRAN 1

Daftar Pertanyaan Kuesioner Siswa Techonlogy Acceptance Model (TAM)

Kemanfaatan *(Perceived Usefulness)*

1. Saya yakin bahwa sistem MyLMS dapat membantu saya belajar dengan lebih efektif.
    1. Sangat Tidak Setuju
    2. Tidak Setuju
    3. Cukup Setuju
    4. Setuju
    5. Sangat Setuju
2. Saya yakin bahwa sistem MyLMS dapat membantu saya menghemat waktu belajar.
    1. Sangat Tidak Setuju
    2. Tidak Setuju
    3. Cukup Setuju
    4. Setuju
    5. Sangat Setuju
3. Saya yakin Sistem My LMS mempercepat dalam kegiatan belajar saya.
    1. Sangat Tidak Setuju
    2. Tidak Setuju
    3. Cukup Setuju
    4. Setuju
    5. Sangat Setuju
4. Saya berniat untuk menggunakan sistem MyLMS untuk mendapatkan pengalaman belajar yang lebih baik.
    1. Sangat Tidak Setuju
    2. Tidak Setuju
    3. Cukup Setuju
    4. Setuju
    5. Sangat Setuju

Kemudahan *(Ease of Use)*

1. Saya yakin bahwa sistem MyLMS mudah digunakan.
    1. Sangat Tidak Setuju
    2. Tidak Setuju
    3. Cukup Setuju
    4. Setuju
    5. Sangat Setuju
2. Mudah bagi saya dalam mengoperasikan sistem My LMS dalam proses pembelajaran.
    1. Sangat Tidak Setuju
    2. Tidak Setuju
    3. Cukup Setuju
    4. Setuju
    5. Sangat Setuju
3. Saya yakin bahwa saya dapat belajar menggunakan sistem MyLMS dengan cepat.
    1. Sangat Tidak Setuju
    2. Tidak Setuju
    3. Cukup Setuju
    4. Setuju
    5. Sangat Setuju

Penerimaan *(Acceptance)*

1. Saya berniat untuk menggunakan sistem MyLMS secara rutin.
    1. Sangat Tidak Setuju
    2. Tidak Setuju
    3. Cukup Setuju
    4. Setuju
    5. Sangat Setuju

2. Saya berniat untuk menggunakan sistem MyLMS untuk belajar materi yang diberikan pengajar.
    1. Sangat Tidak Setuju
    2. Tidak Setuju
    3. Cukup Setuju
    4. Setuju
    5. Sangat Setuju
3. Saya berniat untuk menggunakan sistem MyLMS untuk berinteraksi dengan Guru dan teman sekelas saya.
    1. Sangat Tidak Setuju
    2. Tidak Setuju
    3. Cukup Setuju
    4. Setuju
    5. Sangat Setuju
4. Saya yakin bahwa sistem MyLMS dapat memenuhi kebutuhan saya.
    1. Sangat Tidak Setuju
    2. Tidak Setuju
    3. Cukup Setuju
    4. Setuju
    5. Sangat Setuju

Kualitas (Quality)

1. Saya yakin bahwa sistem MyLMS aman untuk digunakan.
    1. Sangat Tidak Setuju
    2. Tidak Setuju
    3. Cukup Setuju
    4. Setuju
    5. Sangat Setuju
2. Saya yakin bahwa sistem MyLMS dapat diandalkan.
    1. Sangat Tidak Setuju
    2. Tidak Setuju
    3. Cukup Setuju
    4. Setuju
    5. Sangat Setuju
3. Saya yakin bahwa sistem MyLMS dapat melindungi privasi saya.
    1. Sangat Tidak Setuju
    2. Tidak Setuju
    3. Cukup Setuju
    4. Setuju
    5. Sangat Setuju
4. Saya yakin bahwa sistem MyLMS dapat menjadi sumber belajar yang berharga bagi saya.
    1. Sangat Tidak Setuju
    2. Tidak Setuju
    3. Cukup Setuju
    4. Setuju
    5. Sangat Setuju

Daftar Pertanyaan Kuesioner Guru Techonlogy Acceptance Model (TAM)

Kemanfaatan *(Perceived Usefulness)*

1. Saya yakin bahwa sistem MyLMS dapat membantu saya dalam proses belajar mengejar dengan lebih efektif.
    1. Sangat Tidak Setuju
    2. Tidak Setuju
    3. Cukup Setuju
    4. Setuju
    5. Sangat Setuju
2. Saya yakin bahwa sistem MyLMS dapat membantu saya menghemat waktu mengajar.
    1. Sangat Tidak Setuju
    2. Tidak Setuju
    3. Cukup Setuju
    4. Setuju
    5. Sangat Setuju
3. Saya yakin Sistem My LMS mempercepat dalam kegiatan mengjar saya.
    1. Sangat Tidak Setuju
    2. Tidak Setuju
    3. Cukup Setuju
    4. Setuju
    5. Sangat Setuju
4. Saya berniat untuk menggunakan sistem MyLMS untuk mendapatkan pengalaman mengajar yang lebih baik.
    1. Sangat Tidak Setuju
    2. Tidak Setuju
    3. Cukup Setuju
    4. Setuju
    5. Sangat Setuju

Kemudahan *(Ease of Use)*

1. Saya yakin bahwa sistem MyLMS mudah digunakan.
    1. Sangat Tidak Setuju
    2. Tidak Setuju
    3. Cukup Setuju
    4. Setuju
    5. Sangat Setuju
2. Mudah bagi saya dalam mengoperasikan sistem My LMS dalam proses pembelajaran.
    1. Sangat Tidak Setuju
    2. Tidak Setuju
    3. Cukup Setuju
    4. Setuju
    5. Sangat Setuju
3. Saya yakin bahwa saya dapat mengjar menggunakan sistem MyLMS dengan cepat.
    1. Sangat Tidak Setuju
    2. Tidak Setuju
    3. Cukup Setuju
    4. Setuju
    5. Sangat Setuju

Penerimaan *(Acceptance)*

1. Saya berniat untuk menggunakan sistem MyLMS secara rutin.
    1. Sangat Tidak Setuju
    2. Tidak Setuju
    3. Cukup Setuju
    4. Setuju
    5. Sangat Setuju
2. Saya berniat untuk menggunakan sistem MyLMS untuk memberikan materi belajar siswa.
    1. Sangat Tidak Setuju
    2. Tidak Setuju
    3. Cukup Setuju
    4. Setuju
    5. Sangat Setuju
3. Saya berniat untuk menggunakan sistem MyLMS untuk berinteraksi dengan siswa dikelas.
    1. Sangat Tidak Setuju
    2. Tidak Setuju
    3. Cukup Setuju
    4. Setuju
    5. Sangat Setuju
4. Saya yakin bahwa sistem MyLMS dapat memenuhi kebutuhan saya.
    1. Sangat Tidak Setuju
    2. Tidak Setuju
    3. Cukup Setuju
    4. Setuju
    5. Sangat Setuju

Kualitas (Quality)

1. Saya yakin bahwa sistem MyLMS aman untuk digunakan.
    1. Sangat Tidak Setuju
    2. Tidak Setuju
    3. Cukup Setuju
    4. Setuju
    5. Sangat Setuju
2. Saya yakin bahwa sistem MyLMS dapat diandalkan.
    1. Sangat Tidak Setuju
    2. Tidak Setuju
    3. Cukup Setuju
    4. Setuju
    5. Sangat Setuju
3. Saya yakin bahwa sistem MyLMS dapat melindungi privasi saya.
    1. Sangat Tidak Setuju
    2. Tidak Setuju
    3. Cukup Setuju
    4. Setuju
    5. Sangat Setuju
4. Saya yakin bahwa sistem MyLMS dapat menjadi sumber materi ajar yang berharga bagi siswa.
    1. Sangat Tidak Setuju
    2. Tidak Setuju
    3. Cukup Setuju
    4. Setuju
    5. Sangat Setuju

Daftar Pertanyaan Indeks Keamanan Informasi (KAMI)

Bagian I: Kategori Sistem Elektronik

No	Karakteristik Instansi
1	Nilai investasi sistem elektronik yang terpasang
2	Total anggaran operasional tahunan yang dialokasikan untuk pengelolaan Sistem Elektronik
3	Memiliki kewajiban kepatuhan terhadap Peraturan atau Standar tertentu
4	Menggunakan algoritma khusus untuk keamanan informasi dalam Sistem Elektronik
5	Jumlah pengguna Sistem Elektronik
6	Data pribadi yang dikelola Sistem Elektronik
7	Tingkat klasifikasi/kekritisan Data yang ada dalam Sistem Elektronik, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi.
8	Tingkat kekritisan proses yang ada dalam Sistem Elektronik, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi
9	Dampak dari kegagalan Sistem Elektronik
10	Potensi kerugian atau dampak negatif dari insiden ditembusnya keamanan informasi Sistem Elektronik (sabotase, terorisme)

Bagian II: Tata Kelola Keamanan Informasi

No	Fungsi/Instansi Keamanan Informasi
1	Apakah pimpinan Instansi anda secara prinsip dan resmi bertanggungjawab terhadap pelaksanaan program keamanan informasi (misal yang tercantum dalam ITSP), termasuk penetapan kebijakan terkait?
2	Apakah Instansi anda memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab mengelola keamanan informasi dan menjaga kepatuhannya?
3	Apakah pejabat/petugas pelaksana pengamanan informasi mempunyai wewenang yang sesuai untuk menerapkan dan menjamin kepatuhan program keamanan informasi?
4	Apakah penanggungjawab pelaksanaan pengamanan informasi diberikan alokasi sumber daya yang sesuai untuk mengelola dan menjamin kepatuhan program keamanan informasi?
5	Apakah peran pelaksana pengamanan informasi yang mencakup semua keperluan dipetakan dengan lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan?
6	Apakah Instansi anda sudah mendefinisikan persyaratan/standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi?
7	Apakah semua pelaksana pengamanan informasi di Instansi anda memiliki kompetensi dan keahlian yang memadai sesuai persyaratan/standar yang berlaku?
8	Apakah instansi anda sudah menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi, termasuk kepentingan kepatuhannya bagi semua pihak yang terkait?
9	Apakah Instansi anda menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi?

10	Apakah instansi anda sudah mengintegrasikan keperluan/persyaratan keamanan informasi dalam proses kerja yang ada?
11	Apakah instansi anda sudah mengidentifikasikan data pribadi yang digunakan dalam proses kerja dan menerapkan pengamanan sesuai dengan peraturan perundangan yang berlaku?
12	Apakah tanggungjawab pengelolaan keamanan informasi mencakup koordinasi dengan pihak pengelola/pengguna aset informasi internal dan eksternal maupun pihak lain yang berkepentingan, untuk mengidentifikasikan persyaratan/kebutuhan pengamanan (misal: pertukaran informasi atau kerjasama yang melibatkan informasi penting) dan menyelesaikan permasalahan yang ada?
13	Apakah pengelola keamanan informasi secara proaktif berkoordinasi dengan satker terkait (SDM, Legal/Hukum, Umum, Keuangan dll) dan pihak eksternal yang berkepentingan (misal: regulator, aparat keamanan) untuk menerapkan dan menjamin kepatuhan pengamanan informasi terkait proses kerja yang melibatkan berbagai pihak?
14	Apakah tanggungjawab untuk memutuskan, merancang, melaksanakan dan mengelola langkah kelangsungan layanan TIK (business continuity dan disaster recovery plans) sudah didefinisikan dan dialokasikan?
15	Apakah penanggungjawab pengelolaan keamanan informasi melaporkan kondisi, kinerja/efektivitas dan kepatuhan program keamanan informasi kepada pimpinan Instansi secara rutin dan resmi?
16	Apakah kondisi dan permasalahan keamanan informasi di Instansi anda menjadi konsideran atau bagian dari proses pengambilan keputusan strategis di Instansi anda?

17	Apakah pimpinan satuan kerja di Instansi anda menerapkan program khusus untuk mematuhi tujuan dan sasaran kepatuhan pengamanan informasi, khususnya yang mencakup aset informasi yang menjadi tanggungjawabnya?
18	Apakah Instansi anda sudah mendefinisikan metrik, paramater dan proses pengukuran kinerja pengelolaan keamanan informasi yang mencakup mekanisme, waktu pengukuran, pelaksananya, pemantauannya dan eskalasi pelaporannya?
19	Apakah Instansi anda sudah menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi individu (pejabat & petugas) pelaksananya?
20	Apakah Instansi anda sudah menerapkan target dan sasaran pengelolaan keamanan informasi untuk berbagai area yang relevan, mengevaluasi pencapaiannya secara rutin, menerapkan langkah perbaikan untuk mencapai sasaran yang ada, termasuk pelaporan statusnya kepada pimpinan Instansi?
21	Apakah Instansi anda sudah mengidentifikasi legislasi, perangkat hukum dan standar lainnya terkait keamanan informasi yang harus dipatuhi dan menganalisa tingkat kepatuhannya?
22	Apakah Instansi anda sudah mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata)?

Bagian III: Pengelolaan Risiko Keamanan Informasi

No	Kajian Risiko Keamanan Informasi
1	Apakah Instansi anda mempunyai program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?
2	Apakah Instansi anda sudah menetapkan penanggung jawab manajemen risiko dan eskalasi pelaporan status pengelolaan risiko keamanan informasi sampai ke tingkat pimpinan?
3	Apakah Instansi anda mempunyai kerangka kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?
4	Apakah kerangka kerja pengelolaan risiko ini mencakup definisi dan hubungan tingkat klasifikasi aset informasi, tingkat ancaman, kemungkinan terjadinya ancaman tersebut dan dampak kerugian terhadap Instansi anda?
5	Apakah Instansi anda sudah menetapkan ambang batas tingkat risiko yang dapat diterima?
6	Apakah Instansi anda sudah mendefinisikan kepemilikan dan pihak pengelola (custodian) aset informasi yang ada, termasuk aset utama/penting dan proses kerja utama yang menggunakan aset tersebut?
7	Apakah ancaman dan kelemahan yang terkait dengan aset informasi, terutama untuk setiap aset utama sudah teridentifikasi?
8	Apakah dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi aset utama sudah ditetapkan sesuai dengan definisi yang ada?
9	Apakah Instansi anda sudah menjalankan inisiatif analisa/kajian risiko keamanan informasi secara terstruktur terhadap aset informasi yang ada (untuk nantinya digunakan dalam

	mengidentifikasi langkah mitigasi atau penanggulangan yang menjadi bagian dari program pengelolaan keamanan informasi)?
10	Apakah Instansi anda sudah menyusun langkah mitigasi dan penanggulangan risiko yang ada?
11	Apakah langkah mitigasi risiko disusun sesuai tingkat prioritas dengan target penyelesaiannya dan penanggungjawabnya, dengan memastikan efektivitas penggunaan sumber daya yang dapat menurunkan tingkat risiko ke ambang batas yang bisa diterima dengan meminimalisir dampak terhadap operasional layanan TIK?
12	Apakah status penyelesaian langkah mitigasi risiko dipantau secara berkala, untuk memastikan penyelesaian atau kemajuan kerjanya?persyaratan/kebutuhan pengamanan (misal: pertukaran informasi atau kerjasama yang melibatkan informasi penting) dan menyelesaikan permasalahan yang ada?
13	Apakah penyelesaian langkah mitigasi yang sudah diterapkan dievaluasi, melalui proses yang obyektif/terukur untuk memastikan konsistensi dan efektivitasnya?
14	Apakah profil risiko berikut bentuk mitigasinya secara berkala dikaji ulang untuk memastikan akurasi dan validitasnya, termasuk merevisi profil terebut apabila ada perubahan kondisi yang signifikan atau keperluan penerapan bentuk pengamanan baru?
15	Apakah kerangka kerja pengelolaan risiko secara berkala dikaji untuk memastikan/meningkatkan efektivitasnya?
16	Apakah pengelolaan risiko menjadi bagian dari kriteria proses penilaian obyektif kinerja efektivitas pengamanan?

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi

No	Penyusunan dan Pengelolaan Kebijakan dan Prosedur Keamanan Informasi
1	Apakah kebijakan dan prosedur maupun dokumen lainnya yang diperlukan terkait keamanan informasi sudah disusun dan dituliskan dengan jelas, dengan mencantumkan peran dan tanggungjawab pihak-pihak yang diberikan wewenang untuk menerapkannya?
2	Apakah kebijakan keamanan informasi sudah ditetapkan secara formal, dipublikasikan kepada semua staf/karyawan termasuk pihak terkait dan dengan mudah diakses oleh pihak yang membutuhkannya?
3	Apakah tersedia mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi, termasuk penggunaan daftar induk, distribusi, penarikan dari peredaran dan penyimpanannya?
4	Apakah tersedia proses (mencakup pelaksana, mekanisme, jadwal, materi, dan sasarannya) untuk mengkomunikasikan kebijakan keamanan informasi (dan perubahannya) kepada semua pihak terkait, termasuk pihak ketiga?
5	Apakah keseluruhan kebijakan dan prosedur keamanan informasi yang ada merefleksikan kebutuhan mitigasi dari hasil kajian risiko keamanan informasi, maupun sasaran/obyetif tertentu yang ditetapkan oleh pimpinan Instansi?
6	Apakah tersedia proses untuk mengidentifikasi kondisi yang membahayakan keamanan infomasi dan menetapkannya sebagai insiden keamanan informasi untuk ditindak lanjuti sesuai prosedur yang diberlakukan?
7	Apakah aspek keamanan informasi yang mencakup pelaporan insiden, menjaga kerahasiaan, HAKI, tata tertib penggunaan dan

	pengamanan aset maupun layanan TIK tercantum dalam kontrak dengan pihak ketiga?
8	Apakah konsekuensi dari pelanggaran kebijakan keamanan informasi sudah didefinisikan, dikomunikasikan dan ditegakkan?
9	Apakah tersedia prosedur resmi untuk mengelola suatu pengecualian terhadap penerapan keamanan informasi, termasuk proses untuk menindak-lanjuti konsekuensi dari kondisi ini?
10	Apakah organisasi anda sudah menerapkan kebijakan dan prosedur operasional untuk mengelola implementasi security patch, alokasi tanggungjawab untuk memonitor adanya rilis security patch baru, memastikan pemasangannya dan melaporkannya?
11	Apakah organisasi anda sudah membahas aspek keamanan informasi dalam manajemen proyek yang terkait dengan ruang lingkup?
12	Apakah organisasi anda sudah menerapkan proses untuk mengevaluasi risiko terkait rencana pembelian (atau implementasi) sistem baru dan menanggulangi permasalahan yang muncul?
13	Apakah organisasi anda sudah menerapkan proses pengembangan sistem yang aman (Secure SDLC) dengan menggunakan prinsip atau metode sesuai standar platform teknologi yang digunakan?
14	Apabila penerapan suatu sistem mengakibatkan timbulnya risiko baru atau terjadinya ketidakpatuhan terhadap kebijakan yang ada, apakah ada proses untuk menanggulangi hal ini, termasuk penerapan pengamanan baru (compensating control) dan jadwal penyelesaiannya?
15	Apakah tersedia kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (business continuity planning) yang mendefinisikan persyaratan/konsideran keamanan informasi,

	termasuk penjadwalan uji-cobanya?
16	Apakah perencanaan pemulihan bencana terhadap layanan TIK (disaster recovery plan) sudah mendefinisikan komposisi, peran, wewenang dan tanggungjawab tim yang ditunjuk?
17	Apakah uji-coba perencanaan pemulihan bencana terhadap layanan TIK (disaster recovery plan) sudah dilakukan sesuai jadwal?
18	Apakah hasil dari perencanaan pemulihan bencana terhadap layanan TIK (disaster recovery plan) dievaluasi untuk menerapkan langkah perbaikan atau pembenahan yang diperlukan (misal, apabila hasil uji-coba menunjukkan bahwa proses pemulihan tidak bisa (gagal) memenuhi persyaratan yang ada?
19	Apakah seluruh kebijakan dan prosedur keamanan informasi dievaluasi kelayakannya secara berkala?
	Pengelolaan Strategi dan Program Keamanan Informasi
20	Apakah organisasi anda mempunyai strategi penerapan keamanan informasi sesuai hasil analisa risiko yang penerapannya dilakukan sebagai bagian dari rencana kerja organisasi?
21	Apakah organisasi anda mempunyai strategi penggunaan teknologi keamanan informasi yang penerapan dan pemutakhirannya disesuaikan dengan kebutuhan dan perubahan profil risiko?
22	Apakah strategi penerapan keamanan informasi direalisasikan sebagai bagian dari pelaksanaan program kerja organisasi anda?
23	Apakah organisasi anda memiliki dan melaksanakan program audit internal yang dilakukan oleh pihak independen dengan cakupan keseluruhan aset informasi, kebijakan dan prosedur keamanan yang ada (atau sesuai dengan standar yang berlaku)?

24	Apakah audit internal tersebut mengevaluasi tingkat kepatuhan, konsistensi dan efektivitas penerapan keamanan informasi?
25	Apakah hasil audit internal tersebut dikaji/dievaluasi untuk mengidentifikasi langkah pembenahan dan pencegahan, ataupun inisiatif peningkatan kinerja keamanan informasi?
26	Apakah hasil audit internal dilaporkan kepada pimpinan organisasi untuk menetapkan langkah perbaikan atau program peningkatan kinerja keamanan informasi?
27	Apabila ada keperluan untuk merevisi kebijakan dan prosedur yang berlaku, apakah ada analisa untuk menilai aspek finansial (dampak biaya dan keperluan anggaran) ataupun perubahan terhadap infrastruktur dan pengelolaan perubahannya, sebagai prasyaratuntuk menerapkannya?
28	Apakah organisasi anda secara periodik menguji dan mengevaluasi tingkat/status kepatuhan program keamanan informasi yang ada (mencakup pengecualian atau kondisi ketidakpatuhan lainnya) untuk memastikan bahwa keseluruhan inisiatif tersebut, termasuk langkah pembenahan yang diperlukan, telah diterapkan secara efektif?
29	Apakah organisasi anda mempunyai rencana dan program peningkatan keamanan informasi untuk jangka menengah/panjang (1-3-5 tahun) yang direalisasikan secara konsisten?

Bagian V: Pengelolaan Aset Informasi

Pengelolaan Aset Informasi	
No	**Pengelolaan Aset Informasi**
1	Apakah tersedia daftar inventaris aset informasi dan aset yang berhubungan dengan proses teknologi informasi secara lengkap, akurat dan terpelihara ? (termasuk kepemilikan aset)
2	Apakah tersedia definisi klasifikasi aset informasi yang sesuai dengan peraturan perundangan yang berlaku?
3	Apakah tersedia proses yang mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingan aset bagi Instansi dan keperluan pengamanannya?
4	Apakah tersedia definisi tingkatan akses yang berbeda dari setiap klasifikasi aset informasi
4	Apakah tersedia definisi tingkatan akses yang berbeda dari setiap klasifikasi aset informasi dan matrix yang merekam alokasi akses tersebut?
5	Apakah tersedia proses pengelolaan perubahan terhadap sistem, proses bisnis dan proses teknologi informasi (termasuk perubahan konfigurasi) yang diterapkan secara konsisten?
6	Apakah tersedia proses pengelolaan konfigurasi yang diterapkan secara konsisten?
7	Apakah tersedia proses untuk merilis suatu aset baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset informasi?
Apakah Instansi anda memiliki dan menerapkan perangkat di bawah ini, sebagai kelanjutan dari proses penerapan mitigasi risiko?	
8	Definisi tanggungjawab pengamanan informasi secara individual untuk semua personil di Instansi anda
9	Tata tertib penggunaan komputer, email, internet dan intranet
10	Tata tertib pengamanan dan penggunaan aset Instansi terkait HAKI
11	Peraturan terkait instalasi piranti lunak di aset TI milik instansi

12	Peraturan penggunaan data pribadi yang mensyaratkan pemberian ijin tertulis oleh pemilik data pribadi
13	Pengelolaan identitas elektronik dan proses otentikasi (username & password) termasuk kebijakan terhadap pelanggarannya
14	Persyaratan dan prosedur pengelolaan/pemberian akses, otentikasi dan otorisasi untuk menggunakan aset informasi
15	Ketetapan terkait waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data
16	Ketetapan terkait pertukaran data dengan pihak eksternal dan pengamanannya
17	Proses penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi
18	Prosedur back-up dan ujicoba pengembalian data (restore) secara berkala
19	Ketentuan pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi aset yang ada di dalamnya
20	Proses pengecekan latar belakang SDM
21	Proses pelaporan insiden keamanan informasi kepada pihak eksternal ataupun pihak yang berwajib.
22	Prosedur penghancuran data/aset yang sudah tidak diperlukan
23	Prosedur kajian penggunaan akses (user access review) dan hak aksesnya (user access rights) berikut langkah pembenahan apabila terjadi ketidak sesuaian (non-conformity) terhadap kebijakan yang berlaku
24	Prosedur untuk user yang mutasi/keluar atau tenaga kontrak/outsource yang habis masa kerjanya
25	Apakah tersedia daftar data/informasi yang harus di-backup dan laporan analisa kepatuhan terhadap prosedur backup-nya?
26	Apakah tersedia daftar rekaman pelaksanaan keamanan informasi dan

	bentuk pengamanan yang sesuai dengan klasifikasinya?
27	Apakah tersedia prosedur penggunaan perangkat pengolah informasi milik pihak ketiga (termasuk perangkat milik pribadi dan mitra kerja/vendor) dengan memastikan aspekHAKI dan pengamanan akses yang digunakan?
Pengamanan Fisik	
28	Apakah sudah diterapkan pengamanan fasilitas fisik (lokasi kerja) yang sesuai dengan kepentingan/klasifikasi aset informasi, secara berlapis dan dapat mencegah upaya akses olehpihak yang tidak berwenang?
29	Apakah tersedia proses untuk mengelola alokasi kunci masuk (fisik dan elektronik) ke fasilitas fisik?
30	Apakah infrastruktur komputasi terlindungi dari dampak lingkungan atau api dan berada dalam kondisi dengan suhu dan kelembaban yang sesuai dengan prasyarat pabrikannya?
31	Apakah infrastruktur komputasi yang terpasang terlindungi dari gangguan pasokan listrik atau dampak dari petir?
32	Apakah tersedia peraturan pengamanan perangkat komputasi milik Instansi anda apabila digunakan di luar lokasi kerja resmi (kantor)?
33	Apakah tersedia proses untuk memindahkan aset TIK (piranti lunak, perangkat keras, data/informasi dll) dari lokasi yang sudah ditetapkan (dalam daftar inventaris)
34	Apakah konstruksi ruang penyimpanan perangkat pengolah informasi penting menggunakan rancangan dan material yang dapat menanggulangi risiko kebakaran dan dilengkapi dengan fasilitas pendukung (deteksi kebakaran/asap, pemadam api, pengatur suhu dan kelembaban) yang sesuai?
35	Apakah tersedia proses untuk memeriksa (inspeksi) dan merawat: perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan aset informasi penting?
36	Apakah tersedia mekanisme pengamanan dalam pengiriman aset

	informasi (perangkat dan dokumen) yang melibatkan pihak ketiga?
37	Apakah tersedia peraturan untuk mengamankan lokasi kerja penting (ruang server, ruang arsip) dari risiko perangkat atau bahan yang dapat membahayakan aset informasi (termasuk fasilitas pengolah informasi) yang ada di dalamnya? (misal larangan penggunaan telpon genggam di dalam ruang server, menggunakan kamera dll)
38	Apakah tersedia proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga yang bekerja untuk kepentingan Instansi anda?

Bagian VI: Teknologi dan Keamanan Informasi

Teknologi dan Keamanan Informasi	
No	**Pengamanan Teknologi**
1	Apakah layanan TIK (sistem komputer) yang menggunakan internet sudah dilindungi dengan lebih dari 1 lapis pengamanan?
2	Apakah jaringan komunikasi disegmentasi sesuai dengan kepentingannya (pembagian Instansi, kebutuhan aplikasi, jalur akses khusus, dll)?
3	Apakah tersedia konfigurasi standar untuk keamanan sistem bagi keseluruhan aset jaringan, sistem dan aplikasi, yang dimutakhirkan sesuai perkembangan (standar industri yang berlaku) dan kebutuhan?
4	Apakah Instansi anda secara rutin menganalisa kepatuhan penerapan konfigurasi standar yang ada?
5	Apakah jaringan, sistem dan aplikasi yang digunakan secara rutin dipindai untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan/keutuhan konfigurasi?
6	Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dirancang untuk memastikan ketersediaan (rancangan redundan) sesuai kebutuhan/persyaratan yang ada?
7	Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dimonitor untuk memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada?
8	Apakah setiap perubahan dalam sistem informasi secara otomatis terekam di dalam log?
9	Apakah upaya akses oleh yang tidak berhak secara otomatis terekam di dalam log?
10	Apakah semua log dianalisa secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik)?

11	Apakah Instansi anda menerapkan enkripsi untuk melindungi aset informasi penting sesuai kebijakan pengelolaan yang ada?
12	Apakah Instansi anda mempunyai standar dalam menggunakan enkripsi?
13	Apakah Instansi anda menerapkan pengamanan untuk mengelola kunci enkripsi (termasuk sertifikat elektronik) yang digunakan, termasuk siklus penggunaannya?
14	Apakah semua sistem dan aplikasi secara otomatis mendukung dan menerapkan penggantian password secara otomatis, termasuk menon-aktifkan password, mengatur kompleksitas/panjangnya dan penggunaan kembali password lama?
15	Apakah akses yang digunakan untuk mengelola sistem (administrasi sistem) menggunakanbentuk pengamanan khusus yang berlapis?
16	Apakah sistem dan aplikasi yang digunakan sudah menerapkan pembatasan waktu akses termasuk otomatisasi proses timeouts, lockout setelah kegagalan login,dan penarikan akses?
17	Apakah Instansi anda menerapkan pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi?
18	Apakah Instansi anda menerapkan bentuk pengamanan khusus untuk melindungi akses dari luar Instansi?
19	Apakah sistem operasi untuk setiap perangkat desktop dan server dimutakhirkan dengan versi terkini?
20	Apakah setiap desktop dan server dilindungi dari penyerangan virus (malware)?
21	Apakah ada rekaman dan hasil analisa (jejak audit - audit trail) yang mengkonfirmasi bahwa antivirus/antimalware telah dimutakhirkan secara rutin dan sistematis?

22	Apakah adanya laporan penyerangan virus/malware yang gagal/sukses ditindaklanjuti dan diselesaikan?
23	Apakah keseluruhan jaringan, sistem dan aplikasi sudah menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang ada?
24	Apakah setiap aplikasi yang ada memiliki spesifikasi dan fungsi keamanan yang diverifikasi/validasi pada saat proses pengembangan dan uji-coba?
25	Apakah instansi ada menerapkan lingkungan pengembangan dan uji-coba yang sudah diamankan sesuai dengan standar platform teknologi yang ada dan digunakan untuk seluruh siklus hidup sistem yng dibangun?
26	Apakah Instansi anda melibatkan pihak independen untuk mengkaji kehandalankeamanan informasi secara rutin?

Bagian VII: Suplemen

Pengamanan Keterlibatan Pihak Ketiga Penyedia Layanan	
No	**Manajemen Risiko dan Pengelolaan Keamanan pihak ketiga**
1.	Apakah instansi/perusahaan mengidentifikasi risiko keamanan informasi yang ada terkait dengan kerjasama dengan pihak ketiga atau karyawan kontrak?
2.	Apakah instansi/perusahaan mengkomunikasikan dan mengklarifikasi risiko keamanan informasi yang ada pada pihak ketiga kepada mereka?
3.	Apakah instansi/perusahaan mengklarifikasi persyaratan mitigasi risiko instansi/perusahaan dan ekspektasi mitigasi risiko yang harus dipatuhi oleh pihak ketiga?
4.	Apakah rencana mitigasi terhadap risiko yang diidentifikasi tersebut disetujui oleh manajemen pihak ketiga atau karyawan kontrak?
5.	Apakah instansi/perusahaan telah menerapkan kebijakan keamanan informasi bagi pihak ketiga secara memadai, mencakup persyaratan pengendalian akses, penghancuran informasi, manajemen risiko penyediaan layanan pihak ketiga, dan NDA bagi karyawan pihak ketiga?
6.	Apakah kebijakan tersebut (5) telah dikomunikasikan kepada pihak ketiga dan mereka menyatakan persetujuannya dalam dokumen kontrak, SLA atau dokumen sejenis lainnya?
7.	Apakah hak audit TI secara berkala ke pihak ketiga/pihak ketiga telah ditetapkan sebagai bagian dan persyaratan kontrak, dikomunikasikan dan disetujui pihak ketiga? Termasuk di dalamnya akses terhadap laporan audit internal / eksternal tentang kondisi kontrol keamanan informasi pihak ketiga/pihak ketiga?

Pengelolaan Sub-Kontraktor/Alih Daya pada Pihak Ketiga	
8.	Apakah pihak ketiga sudah mengidentifikasi risiko terkait alih daya, subkontraktor atau penyedia teknologi/infrastruktur yang digunakan dalam layanannya?
9.	Apakah pihak ketiga sudah menerapkan pengendalian risikonya dalam perjanjian dengan mereka atau dokumen sejenis?
10.	Apakah pihak ketiga melakukan pemantauan dan evaluasi terhadap kepatuhan alih daya, subkontraktor atau penyedia teknologi/infrastruktur terhadap persyaratan keamanan yang ditetapkan?
Pengelolaan Layanan dan Keamanan Pihak Ketiga	
11.	Apakah instansi/perusahaan telah menetapkan proses, prosedur atau rencana terdokumentasi untuk mengelola dan memantau layanan dan aspek keamanan informasi (termasuk pengamanan aset informasi dan infrastruktur milik instanasi/perusahaan yang diakses) dalam hubungan kerjasama dengan pihak ketiga?
12.	Apakah peran dan tanggung jawab pemantauan, evaluasi dan/atau audit aspek keamanan informasi pihak ketiga telah ditetapkan dan/atau ditugaskan dalam unit organisasi tertentu?
13.	Apakah tersedia laporan berkala tentang pencapaian sasaran tingkat layanan (SLA) dan aspek keamanan yang disyaratkan dalam perjanjian komersil (kontrak)?
14.	Apakah ada rapat secara berkala untuk memantau dan mengevaluasi pencapaian sasaran tingkat layanan (SLA) dan aspek keamanan?
15.	Apakah hasil pemantauan dan evaluasi terhadap laporan atau pembahasan dalam rapat berkala tersebut didokumentasikan, dikomunikasikan dan ditindaklanjuti oleh pihak ketiga serta

	dilaporkan kemajuannya kepada instansi/perusahaan?
16.	Apakah instansi/perusahaan telah menetapkan rencana dan melakukan audit terhadap pemenuhan persyaratan keamanan informasi oleh pihak ketiga?
17.	Apakah hasil audit tersebut ditindaklanjuti oleh pihak ketiga dengan melaporkan rencana perbaikan yang terukur dan bukti-bukti penerapan rencana tersebut?
18.	Apakah kondisi terkait denda / penalti karena ketidakpatuhan pihak ketiga terhadap persyaratan dan / atau tingkat layanan telah didokumentasikan, dikomunikasikan, dipahami dan diterapkan?
Pengelolaan Perubahan Layanan dan Kebijakan Pihak Ketiga	
19.	Apakah instansi/perusahaan mengelola perubahan yang terjadi dalam hubungan dengan pihak ketiga yang menyangkut antara lain?- Perubahan layanan pihak ketiga;- Perubahan kebijakan, prosedur, dan/atau - Kontrol risiko pihak ketiga?
20.	Apakah risiko yang menyertai perubahan tersebut dikaji, didokumentasikan dan ditetapkan rencana mitigasi barunya?
Penanganan Aset	
21.	Apakah pihak ketiga memiliki prosedur formal untuk menangani data selama dalam siklus hidupnya mulai dari pembuatan, pendaftaran, perubahan, dan penghapusan / penghancuran aset?
22.	Apakah per untuk penghancuran (disposal) data secara aman telah disepakati bersama pihak ketiga (pihak ketiga)?
Pengelolaan Insiden oleh Pihak Ketiga	
23.	Apakah pihak ketiga memiliki prosedur untuk pelaporan, pemantauan, penanganan, dan analisis insiden keamanan informasi?
24.	Apakah pihak ketiga memiliki bukti-bukti penerapan yang

	memadai dalam menangani insiden keamanan informasi?
Rencana Kelangsungan Layanan Pihak Ketiga	
25.	Apakah pihak ketiga memiliki kebijakan, prosedur atau rencana terdokumentasi untuk mengatasi kelangsungan layanan pihak ketiga dalam keadaan darurat/bencana?
26.	Apakah kebijakan, prosedur atau rencana kelangsungan layanan tersebut telah diujicoba, didokumentasikan hasilnya dan dievaluasi efektivitasnya?
27.	Apakah pihak ketiga memiliki organisasi atau tim khusus yang ditugaskan untuk mengelola proses kelangsungan layanannya?
Pengamanan Layanan Infrastruktur Awan (Cloud Service)	
28.	Apakah instansi/perusahaan sudah melakukan kajian risiko terkait penggunaan layanan berbasis cloud dan menyesuaikan kebijakan keamanan informasi terkait layanan ini?
29.	Apakah instansi/perusahaan sudah menetapkan data apa saja yang akan disimpan/diolah/dipertukarkan melalui layanan berbasis cloud?
30.	Apakah instansi/perusahaan sudah menerapkan langkah pengamanan data pribadi yang disimpan/diolah/dipertukarkan melalui layanan cloud?
31.	Apakah instansi/perusahaan sudah mengkaji, menetapkan kriteria dan memastikan aspek hukum (jurisdiksi, hak dan kewenangan) terkait penggunaan layanan berbasis cloud?
32.	Apakah instansi/perusahaan sudah mengevaluasi penyelenggara layanan cloud terkait reputasi penyelenggaranya?
33.	Apakah instansi/perusahaan sudah menetapkan standar keamanan teknis penggunaan layanan cloud, termasuk aspek penggunaannya oleh pengguna di internal instansi/perusahaan?
34.	Apakah instansi/perusahaan sudah mengevaluasi kelaikan keamanan layanan cloud termasuk aspek ketersediaannya dan

	pemenuhan sertifikasi layanan berbasis ISO 27001?
35.	Apakah instansi/perusahaan sudah memiliki kebijakan, strategi dan proses untuk mengganti layanan cloud atau menyediakan fasilitas pengganti apabila terjadi gangguan sementara pada layanan tersebut?
36.	Apakah instansi/perusahaan sudah memiliki proses pelaporan insiden terkait layanan cloud?
37.	Apakah instansi/perusahaan sudah memiliki proses untuk menghentikan layanan cloud, termasuk proses pengamanan data yang ada (memindahkan dan menghapus data)?
Perlindungan Data Pribadi	
38.	Apakah instansi/perusahaan sudah mendokumentasikan jenis dan bentuk (dokumen kertas/elektronik) data pribadi yang disimpan, diolah dan dipertukarkan dengan pihak eksternal?
39.	Apakah instansi/perusahaan sudah memetakan alur pemrosesan data di internal dan pertukaran data dengan pihak eksternal, termasuk kapan dan dimana data pribadi tersebut diperoleh?
40.	Apakah proses terkait penyimpanan, pengolahan dan pertukaran data pribadi di instansi/perusahaan sudah didokumentasikan?
41.	Apakah instansi/perusahaan sudah memiliki kebijakan terkait Perlindungan Data Pribadi sesuai dengan Peraturan dan Perundangan yang berlaku?
42.	Apakah instansi/perusahaan sudah menunjuk pejabat-pejabat (Data Protection Officer, Data Controller, Data Processor) yang bertanggung-jawab dan berwenang dalam penerapan kebijakan dan proses Perlindungan Data Pribadi?
43.	Apakah instansi/perusahaan sudah menganalisa dampak terkait terungkapnya data pribadi yang disimpan, diolah dan dipertukarkan secara ilegal atau karena insiden lain?
44.	Apakah kajian risiko keamanan pada instansi/perusahaan sudah

	memasukkan aspek Perlindungan Data Pribadi?
45.	Apakah mekanisme perlindungan data pribadi sudah diterapkan sesuai keperluan mitigasi risiko dan peraturan perundangan yang berlaku?
46.	Apakah instansi/perusahaan sudah menjalankan program peningkatan pemahaman/kepedulian kepada seluruh pegawai terkait Perlindungan Data Pribadi, termasuk hal-hal terkait Peraturan Perundangan
47.	Apakah instansi/perusahaan sudah mendapatkan persetujuan dari pemilik data pribadi saat mengambil data tersebut, termasuk penjelasan hak pemilik data, apa saja yang akan diberlakukan pada data pribadi tersebut dan menyimpan catatan persetujuan tersebut ?
48.	Apakah instansi/perusahaan sudah memiliki proses untuk melaporkan insiden terkait terungkapnya data pribadi?
49.	Apakah instansi/perusahaan sudah menerapkan proses yang menjamin hak pemilik data pribadi untuk mengakses data tersebut?
50.	Apakah instansi/perusahaan sudah menerapkan proses yang terkait dapat memastikan data pribadi tersebut akurat dan termutakhirkan?
51.	Apakah instansi/perusahaan sudah menerapkan proses terkait periode penyimpanan data pribadi dan penghapusan/pemusnahannya sesuai dengan peraturan atau perjanjian dengan pemilik data?
52.	Apakah instansi/perusahaan sudah menerapkan proses terkait penghapusan/pemusnahan data apabila sudah tidak ada keperluan yang sah untuk menyimpan/mengolahnya lebih lanjut atau atas permintaan pemilik data dan menyimpan catatan proses tersebut?
53.	Apakah instansi/perusahaan sudah menerapkan proses terkait

	pengungkapan data pribadi atas permintaan resmi aparat penegak hukum?