LAMPIRAN

Lampiran 1 Kuesioner uji ahli

No: 1

PENGUJIAN KUESIONER

PENGUKURAN MANAJEMEN RESIKO KEAMANAN INFORMASI MENGGUNAKAN STANDARISASI ISO/IEC 27001 PADA LPD DESA ADAT BULELENG

DATA RESPONDEN

Nama : .....

Bidang ahli : .....

PETUNJUK PENGISIAN

1. Isilah identitas diri pada tempat data responden di atas yaitu nama responden dan bidang ahli .
2. Dimohonkan kesediaan Bapak/Ibu untuk menjawab setiap nomor item angket dengan sejujurnya sesuai dengan petunjuk yang ada.
3. Pilihlah jawaban dengan memberikan tanda (√) pada kolom pilihan Bapak/Ibu.
4. Setiap pertanyaan harus dijawab, dan tidak boleh ada yang kosong.
5. Tidak ada jawaban yang dianggap salah, benar, baik maupun buruk, karena itu Bapak/Ibu tidak perlu ragu dalam mengisi angket ini.
6. Setelah selesai diisi, mohon angket ini agar segera dikembalikan kepada peneliti.

Keterangan :

1. Mengenai klausul yang dipakai dalam ISO/IEC 27001 Terlampir.
2. Pada kolom keterangan diisikan saran dan perbaikan untuk butir soal pada setiap klausul.

Kontrol dalam ISO/IEC 27001

A.5 Information Security Policies (Kebijakan Keamanan Informasi)

Dirancang untuk memastikan bahwa kebijakan ditulis dan diawasi secara keseluruhan sesuai dengan arahan dari organisasi keamanan informasi.

A.6 Organisation of Information Security (Keamanan Informasi Perusahaan)

mencakup tugas dan tanggung jawab tertentu. *Annex* ini terbagi menjadi dua yaitu:

- A.6.1 yang memastikan bahwa organisasi telah menetapkan kerangka kerja yang dapat menerapkan dan memelihara keamanan informasi secara memadai.

- A.6.2 yang membahas *mobile devices* dan *remote working*. Siapa pun yang bekerja dari rumah atau perjalanan, baik penuh waktu atau paruh waktu, bisa mengikuti aturan yang berlaku.

A.7 Asset Management (Manajemen Aset)

Cara bagaimana organisasi atau perusahaan mengidentifikasi aset informasi dan menentukan tanggung jawab perlindungan sesuai dengan standar yang berlaku

A.8 Human Resource Security (Keamanan Sumber Daya Manusia)

Memastikan bahwa karyawan dan kontraktor memahami hak dan tanggung jawab mereka di perusahaan.

A.9 Physical and Environmental Security (Keamanan Fisik dan Lingkungan)

Membahas keamanan fisik dan lingkungan pada organisasi atau

perusahaan yang terbagi menjadi dua, yaitu:

- A.9.1 untuk mencegah akses fisik yang tidak sah, kerusakan atau gangguan ke tempat organisasi atau data yang ada di dalamnya.
- A.9.2 untuk mencegah kehilangan, kerusakan atau pencurian peralatan aset informasi perusahaan baik itu *software* atau *file* fisik.

A.11 Access Control (Kontrol Akses)

Kontrol akses ini bertujuan untuk memastikan bahwa karyawan hanya bisa melihat dan mengelola informasi yang relevan dengan jabatan mereka.

Kontrol akses memiliki empat bagian yaitu persyaratan bisnis dari kontrol akses, manajemen akses pengguna, tanggung jawab pengguna dan kontrol akses pada sistem dan aplikasi.

A.13 Information Security Incident Management (Manajemen Insiden Keamanan Informasi)

Dalam bagian ini membahas bagaimana mengelola dan melaporkan insiden keamanan. Proses ini melibatkan penjelasan karyawan mana saja yang harus bertanggung jawab terhadap tindakan tertentu sehingga penanganannya bisa konsisten dan efektif.

A.5	Kebijakan Keamanan			
A.5.1	Kebijakan Terhadap Keamanan Informasi			
A.5.1.1	Dokumen Mengenai Keamanan Informasi			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
1.	Kebijakan keamanan informasi telah dilakukan oleh LPD Desa Adat Buleleng			
2.	LPD telah melaksanakan kebijakan keamanan informasi dan telah dikomunikasikan dengan benar kepada pegawai			
A.5.1.2	Kajian Terhadap Keamanan Informasi			
3.	LPD melakukan kajian terhadap Keamanan informasi			
4.	Pengkajian terhadap keamanan informasi harus dilakukan ketika situasi berubah			

A.6	Organisasi Mengenai Keamanan Informasi			
A.6.1	Organisasi Internal			
A.6.1.1	Komitmen Tehadap Keamanan Informasi			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
1.	LPD melaksanakan serangkaian komitmen terhadap suatu keamanan informasi			
A.6.1.2	Koordinasi Mengenai Keamanan Informasi			
2.	LPD melaksanakan koordinasi mengenai keamanan informasi			
A.6.1.3	Perjanjian Perihal Kerahasiaan			
3.	Terdapat perjanjian perihal kerahasian keamanan informasi			
A.6.1.4	Kontak Terhadap Suatu Kelompok Khusus			
4.	LPD melakukan kontak dengan kelompok khusus yang memahami tentang keamanan informasi			

A.6.1.5	Kajian Yang Independen Terhadap Keamanan Informasi			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
5.	LPD telah melakukan kajian yang independen terhadap keamanan informasi			
A.6.2	Perihal Pihak Eksternal			
A.6.2.1	Identifikasi Resiko Dari Pihak Eksternal			
6.	Terdapat indentifikasi resiko dari pihak eksternal terkait aplikasi			
A.6.2.2	Penekanan Keamanan Ketika Menjalin Kontak Dengan Pelanggan			
7.	Terdapat penekanan keamanaan pada saat menjalin kontak dengan nasabah			
A.6.2.3	Penekanan Perjanjian Terhadap Pihak Ketiga			
8.	Terdapat penekanan keamanan pada saat melakukan perjanjian terhadap pihak ketiga terkait aplikasi			

A.7	Manajemen Aset			
A.7.1	Tanggung Jawab Terhadap Aset			
A.7.1.1	Inventaris Aset			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
1.	Terdapat inventarisasi semua aset yang terkait dengan informasi dan pemrosesan informasi di LPD			
A.7.1.2	Kepemilikan Aset			
2.	Semua asset informasi memiliki pemilik yang jelas dan menyadari tanggung jawab mereka			
A.7.1.3	Penerapan Aset Yang Telah Masuk			
3.	Terdapat kebijakan pengguna yang dapat diterima untuk setiap kelas/jenis aset informasi			

A.7.2	Klasifikasi Informasi			
A.7.2.1	Pedoman Klasifikasi			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
4.	Terdapat kebijakan yang mengatur klasifikasi informasi			
A.7.2.2	Pelabelan Dan Penanganan Informasi			
5.	Terdapat prosedur atau proses untuk klasifikasi informasi ditandai dengan tepat pada setiap aset			

A.8	Keamanan Sumber Daya Manusia			
A.8.1	Sebelum Dipekerjakan			
A.8.1.1	Tanggung Jawab Dan Fungsi			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
1.	Terdapat tanggung jawab dan fungsi dari masing – masing staf yang dipekerjakan di LPD			
A.8.1.2	Penyaringan (*Screening*)			
2.	LPD melakukan verifikasi latar belakang terhadap karyawan baru yang akan dipekerjakan			
3.	LPD melakukan pemeriksaan sesuai dengan hukum, peraturan, dan etika yang relevan			
A.8.1.3	Rumusan Syarat Dan Aturan Dalam Kepegawaian			
4.	Semua staf yang bekerja di LPD Desa Adat Buleleng bersedia untuk menandatangani perjanjian kerahasiaan informasi			

A.8.2	Selama Bekerja			
A.8.2.1	Tanggung Jawab Manajemen			
No	Pernyataan	Relevan	Tidak Relevan	Keterangan
5.	Manajemen memberikan penjelasan kepada semua staf dan pengguna pihak ketiga untuk menerapkan keamanan sesuai dengan kebijakan dan prosedur yang ditetapkan			
A.8.2.2	Proses Pendisiplinan			
6.	Terdapat proses pendisiplinan formal yang dapat diterapkan pada staf yang telah melakukan pelanggaran keamanan informasi			
A.8.3	Pengakhiran Dan Perubahan Pekerjaan			
A.8.3.1	Tanggung Jawab Pengakhiran Pekerjaan			
7.	Terdapat proses terdokumentasi formal untuk mengakhiri atau mengubah tugas pekerjaan			
8.	LPD Desa Adat Buleleng mampu menegakkan kepatuhan dengan tugas pasca kerja			

A.8.3.2	Pengembalian Aset			
No	Pernyataan	Relevan	Tidak Relevan	Keterangan
9.	Terdapat proses untuk memastikan semua staf dan pengguna eksternal mengembalikan aset organisasi pada pemutusan hubungan kerja, kontrak, atau perjanjian mereka			
A.8.3.3	Penghapusan Hak Akses			
10.	Terdapat proses untuk memastikan hak akses pengguna dihapus pada pemutusan hubungan kerja atau kontrak, atau disesuaikan dengan perubahan			

A.9	Keamanan Fisik Dan Lingkungan			
A.9.1	Area Yang Aman			
A.9.1.1	Parameter Keamanan Fisik			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
1.	Batasan keamanan yang ditentukan di LPD Desa Adat Buleleng, dan area informasi sensitive atau kritis dipisahkan serta dikontrol dengan tepat			
A.9.1.2	Menjaga Ruangan, Kantor, Atau Fasilias Lainnya			
2.	Ruangan, kantor, atau fasilitas lainnya telah dirancang dan dikonfigurasi dengan mempertimbangkan keamanan			
A.9.1.3	Penjagaan Terhadap Adanya Ancaman			
3.	Melakukan perlindungan maupun pencegahan dari ancaman baik itu ancaman eksternal, maupun internal			
A.9.1.4	Bekerja Di Area Yang Aman			
4.	LPD Desa Adat Buleleng sudah menerapkan prosedur untuk bekerja di daerah yang aman dan sudah diterapkan			

A.9.1.5	Area Akses Publik Dan Bongkar Muat			
No	Pernyataan	Relevan	Tidak Relevan	Keterangan
5.	Terdapat akses publik yang terisolasi dari fasilitas pemrosesan informasi			
A.9.2	Keamanan Peralatan			
A.9.2.1	Penempatan Dan Perlindungan Peralatan			
6.	Terdapat identifikasi bahaya lingkungan yang diidentifikasi dan dipertimbangkan ketika lokasi peralatan dipilih			
A.9.2.2	Sarana Pendukung			
7	Terdapat UPS atau generator cadangan dan telah diuji dalam skala waktu yang sesuai			
A.9.2.3	Keamanan Kabel			

8.	Penilaian risiko yang telah dilakukan di lokasi kabel listrik dan telekomunikasi			
A.9.2.4	Pemeliharaan Peralatan			
No	Pernyataan	Relevan	Tidak Relevan	Keterangan
9.	Terdapat jadwal pemeliharaan peralatan yang ketat			
A.9.2.5	Pembuangan Atas Penggunaan Kembali Peralatan Dengan Aman			
10.	Kebijakan yang mencakup bagaimana aset informasi dapat digunakan kembali Dimana data dihapus, apakah sudah diverifikasi dengan benar			

A.11	Pengendalian Akses			
A.11.1	Persyaratan Proses Bisnis Dalam Pengendalian Akses			
A.11.1.1	Kebijakan Pengendalian Akses			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
1.	Terdapat kebijakan pengendalian akses yang terdokumentasi dan apakah kebijakan tersebut didasari kebutuhan bisnis			
A.11.2	Manajemen Pengguna			
A.11.2.1	Pendaftaran Pengguna			
2.	Terdapat proses pendaftaran akses pengguna secara formal			
A.11.2.2	Manajemen *Password* Pengguna			
3.	Sistem manajemen *password* pengguna sudah sesuai dengan standar keamanan			
A.11.2.3	Tinjauan Terhadap Hak Akses Pengguna			

4.	Terdapat proses bagi pemilik aset untuk meninjau hak akses ke aset mereka secara teratur dan apakah proses peninjauan ini diverifikasi			
A.11.3	Tanggung Jawab Pengguna			
A.11.3.1	Penggunaan *Password* Pengguna			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
5.	Sistem *password* pengguna interaktif dan *password* yang rumit diperlukan			
A.11.3.2	Kebijakan *Clear Desk Dan Clear Screen*			
6.	Terdapat kebijakan *Clear Desk Dan Clear Screen*			
A.11.4	Pengendalian Akses Jaringan			
A.11.4.1	Kebijakan Mengenai Penggunaan Layanan Jaringan			
7	Terdapat proses manajemen jaringan			
A.11.4.2	Identifikasi Peralatan Dalam Jaringan			

8.	Melakukan identifikasi peralatan dalam jaringan yang digunakan			
A.11.4.3	Segregasi Dalam jaringan			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
9.	Topologi jaringan memberlakukan pemisahan jaringan untuk tugas yang berbeda			
A.11.5	Pengendalian Akses Sistem Operasi			
A.11.5.1	Langkah *Log- On* Yang Aman			
10.	Terdapat akses yang dikendalikan oleh prosedur *log-on* yang aman			
A.11.5.2	Proses Identifikasi dan Otentikasi Pengguna			
11.	Terdapat proses identifikasi dan otentikasi pengguna dalam penggunaan aplikasi			
A.11.5.3	Sistem Manajemen *Password*			

12.	Terdapat sistem manajemen *password* didalam aplikasi			
A.11.5.4	Penggunaan Sistem *Utilities*			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
13.	Sistem *Utilities* tambahan di dalam aplikasi			
A.11.5.5	Sesi *Time-Out*			
14.	Sesi *time-out* di dalam proses transaksi di aplikasi			
A.11.5.6	Pembatasan Waktu Koneksi			
15.	Terdapat pembatasan waktu koneksi saat aplikasi tidak digunakan			

A.11.6	Pengendalian Akses Aplikasi Dan Informasi			
A.11.6.1	Pembatasan Akses Informasi			
16.	Akses ke informasi dan fungsi sistem aplikasi dibatasi sesuai dengan kebijakan kontrol akses			
A.11.6.2	Isolasi sistem yang *sensitive*			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
17.	Terdapat pengisolasian sistem yang dianggap *sensitive*			
A.11.7	*Mobile Computing* Dan Kerja Jarak Jauh (*Teleworking*)			
A.11.7.1	*Mobile Computing Dan Komunikasi*			
18.	Aplikasi yang digunakan menerapkan *mobile computing* dalam penggunaanya			
A.11.7.2	*Kerja Jarak Jauh (TeleWorking)*			
19.	Terdapat kebijakan untuk *teleworking* di LPD Desa Adat Buleleng			
20.	Terdapat proses yang ditetapkan untuk pekerja jarak jauh untuk mendapatkan akses serta diberi saran dan peralatan untuk melindungi asset mereka			

A.13	Manajemen Keamanan Informasi			
A.13.1	Melaporkan Insiden Keamanan			
A.13.1.1	Melaporkan Insiden Terhadap Keamanan Informasi			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
1.	Terdapat proses pelaporan kejadian keamanan informasi secara tepat waktu dan apakah ada proses untuk meninjau dan bertindak atas peristiwa keamanan informasi yang dilaporkan			
A.13.1.2	Pelaporan Kelemahan Keamanan			
2.	Terdapat proses pelaporan kelemahan keamanan informasi yang teridentifikasi			

3.	Proses ini dikomunikasikan secara luas dan Apakah ada proses untuk meninjau dan menangani laporan secara tepat waktu			
A.13.2	Manajemen Mengenai Insiden Keamanan Informai Dan Perbaikan			
A.13.2.1	Tanggung Jawab Dan Prosedur			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
4.	Terdapat tanggung jawab manajemen diidentifikasikan dan didokumentasikan dengan jelas dalam proses manajemen insiden			
A.13.2.2	Pembelajaran Dari Insiden Keamanan Informasi			
5.	Terdapat proses atau kerangka kerja yang memungkinkan organisasi untuk belajar dari insiden keamanan informasi dan mengurangi dampak/kemungkinan kejadian di masa depan			

A.13.2.3	Pengumpulan Informasi			
6.	Terdapat kebijakan kesiapan forensik jika terjadi insiden keamanan informasi			
No.	Pernyataan			Keterangan
7	Terdapat data yang relevan dikumpulkan dengan cara yang memungkinkan untuk digunakan sebagai bukti			

Singaraja, ... Januari 2023

NIP.

Lampiran 2 Hasil kuesioner uji ahli

No: 2

PENGUJIAN KUESIONER

PENGUKURAN MANAJEMEN RESIKO KEAMANAN INFORMASI MENGGUNAKAN STANDARISASI ISO/IEC 27001 PADA LPD DESA ADAT BULELENG

DATA RESPONDEN

Nama : Gede Arna Jude Saskara, S.T.,M.T.

Bidang ahli : Sistem Informasi

PETUNJUK PENGISIAN

3. Isilah identitas diri pada tempat data responden di atas yaitu nama responden dan bidang ahli .
4. Dimohonkan kesediaan Bapak/Ibu guru untuk menjawab setiap nomor item angket dengan sejujurnya sesuai dengan petunjuk yang ada.
5. Pilihlah jawaban dengan memberikan tanda (√) pada kolom pilihan Bapak/Ibu.
6. Setiap pertanyaan harus dijawab, dan tidak boleh ada yang kosong.
7. Tidak ada jawaban yang dianggap salah, benar, baik maupun buruk, karena itu Bapak/Ibu tidak perlu ragu dalam mengisi angket ini.
8. Setelah selesai diisi, mohon angket ini agar segera dikembalikan kepada peneliti.

Keterangan :

1. Mengenai klausul yang dipakai dalam ISO/IEC 27001 Terlampir.
2. Pada kolom keterangan diisikan saran dan perbaikan untuk butir soal pada setiap klausul.

Kontrol dalam ISO/IEC 27001

A.5 Information Security Policies (Kebijakan Keamanan Informasi)

Dirancang untuk memastikan bahwa kebijakan ditulis dan diawasi secara keseluruhan sesuai dengan arahan dari organisasi keamanan informasi.

A.6 Organisation of Information Security (Keamanan Informasi Perusahaan)

mencakup tugas dan tanggung jawab tertentu. *Annex* ini terbagi menjadi dua yaitu:

- A.6.1 yang memastikan bahwa organisasi telah menetapkan kerangka kerja yang dapat menerapkan dan memelihara keamanan informasi secara memadai.

- A.6.2 yang membahas *mobile devices* dan *remote working*. Siapa pun yang bekerja dari rumah atau perjalanan, baik penuh waktu atau paruh waktu, bisa mengikuti aturan yang berlaku.

A.7 Asset Management (Manajemen Aset)

Cara bagaimana organisasi atau perusahaan mengidentifikasi aset informasi dan menentukan tanggung jawab perlindungan sesuai dengan standar yang berlaku

A.8 Human Resource Security (Keamanan Sumber Daya Manusia)

Memastikan bahwa karyawan dan kontraktor memahami hak dan tanggung jawab mereka di perusahaan.

A.9 Physical and Environmental Security (Keamanan Fisik dan Lingkungan)

Membahas keamanan fisik dan lingkungan pada organisasi atau

perusahaan yang terbagi menjadi dua, yaitu:

- A.9.1 untuk mencegah akses fisik yang tidak sah, kerusakan atau gangguan ke tempat organisasi atau data yang ada di dalamnya.
- A.9.2 untuk mencegah kehilangan, kerusakan atau pencurian peralatan aset informasi perusahaan baik itu *software* atau *file* fisik.

A.11 Access Control (Kontrol Akses)

Kontrol akses ini bertujuan untuk memastikan bahwa karyawan hanya bisa melihat dan mengelola informasi yang relevan dengan jabatan mereka.

Kontrol akses memiliki empat bagian yaitu persyaratan bisnis dari kontrol akses, manajemen akses pengguna, tanggung jawab pengguna dan kontrol akses pada sistem dan aplikasi.

A.13 Information Security Incident Management (Manajemen Insiden Keamanan Informasi)

Dalam bagian ini membahas bagaimana mengelola dan melaporkan insiden keamanan. Proses ini melibatkan penjelasan karyawan mana saja yang harus bertanggung jawab terhadap tindakan tertentu sehingga penanganannya bisa konsisten dan efektif.

A.5	Kebijakan Keamanan			
A.5.1	Kebijakan Terhadap Keamanan Informasi			
A.5.1.1	Dokumen Mengenai Keamanan Informasi			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
1.	Kebijakan keamanan informasi telah dilakukan oleh LPD Desa Adat Buleleng		✓	Apakah paham dlu terhadap keamanan informasi? Apakah d lpd terdapat aplikasi? Apakah lpd sudah menerapkan keamanan? Apakah ada kebijakan keamanan di lpd yang telah di terapkan?
2.	LPD telah melaksanakan kebijakan keamanan informasi dan telah dikomunikasikan dengan benar kepada pegawai		✓	Apakah kebijakan sudah di sosialisasikan dan adakah buktinya? Apakah dari sosialisasi sudah d terapkan dan buktinya?
A.5.1.2	Kajian Terhadap Keamanan Informasi			
3.	LPD melakukan kajian terhadap Keamanan informasi		✓	Apakah kebijakan yang sudah dilakukan maupun dterapkan sudahkah dilakukan evaluasi terhadap kebijakan?
4.	Pengkajian terhadap keamanan informasi harus dilakukan ketika situasi berubah		✓	Dipertegas lagi yang dimaksud pengkajian terhadap keamanan informasi harus dilakukan ketika situasi berubah

A.6	Organisasi Mengenai Keamanan Informasi			
A.6.1	Organisasi Internal			
A.6.1.1	Komitmen Tehadap Keamanan Informasi			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
1.	LPD melaksanakan serangkaian komitmen terhadap suatu keamanan informasi	✓		Apakah lpd telah memiliki komitmen dalam menerapkan keamanan informasi?
A.6.1.2	Koordinasi Mengenai Keamanan Informasi			
2.	LPD melaksanakan koordinasi mengenai keamanan informasi	✓		
A.6.1.3	Perjanjian Perihal Kerahasiaan			
3.	Terdapat perjanjian perihal kerahasian keamanan informasi		✓	apakah lpd telah memiliki perjanjian kerjasama dengan BSSN/KOMINFO
A.6.1.4	Kontak Terhadap Suatu Kelompok Khusus			
4.	LPD melakukan kontak dengan kelompok khusus yang memahami tentang keamanan informasi		✓	Lpd sudah memiliki kontak dengan tim keamanan bssn/kominfo buleleng terkait dengan keamanan data

A.6.1.5	Kajian Yang Independen Terhadap Keamanan Informasi			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
5.	LPD telah melakukan kajian yang independen terhadap keamanan informasi	✓		Diperjelas tentang kajian yang independen pada klausul yang ada sehingga lebih mempertegas pernyataan yang ada
A.6.2	Perihal Pihak Eksternal			
A.6.2.1	Identifikasi Resiko Dari Pihak Eksternal			
6.	Terdapat indentifikasi resiko dari pihak eksternal terkait aplikasi	✓		Lpd harus tahu resiko dari sistem yang telah digunakan (analis resiko) dipertegas kembali
A.6.2.2	Penekanan Keamanan Ketika Menjalin Kontak Dengan Pelanggan			
7.	Terdapat penekanan keamanaan pada saat menjalin kontak dengan nasabah	✓		Dipertegas pernyataan apakah ada tanda tangan kontrak
A.6.2.3	Penekanan Perjanjian Terhadap Pihak Ketiga			
8.	Terdapat penekanan keamanan pada saat melakukan perjanjian terhadap pihak ketiga terkait aplikasi	✓		Adakah klausul untuk perjanjian kerjasama lpd dengan pengembang sistem

A.7	Manajemen Aset			
A.7.1	Tanggung Jawab Terhadap Aset			
A.7.1.1	Inventaris Aset			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
1.	Terdapat inventarisasi semua aset yang berkait dengan informasi dan pemrosesan informasi di LPD	✓		
A.7.1.2	Kepemilikan Aset			
2.	Semua asset informasi memiliki pemilik yang jelas dan menyadari tanggung jawab mereka	✓		
A.7.1.3	Penerapan Aset Yang Telah Masuk			
3.	Terdapat kebijakan pengguna yang dapat diterima untuk setiap kelas/jenis aset informasi	✓		Dipertegas untuk kebijakannya apa saja yang terdapat di lpd

A.7.2	Klasifikasi Informasi			
A.7.2.1	Pedoman Klasifikasi			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
4.	Terdapat kebijakan yang mengatur klasifikasi informasi	✓		Dipertegas dengan contoh Misalkan informasi nasabah,dokumen dll
A.7.2.2	Pelabelan Dan Penanganan Informasi			
5.	Terdapat prosedur atau proses untuk klasifikasi informasi ditandai dengan tepat pada setiap aset	✓		Apakah terdapat prosedur untuk klasifikasi informasi Apakah terdapat proses untuk mengurutkan asset secara tepat

A.8	Keamanan Sumber Daya Manusia			
A.8.1	Sebelum Dipekerjakan			
A.8.1.1	Tanggung Jawab Dan Fungsi			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
1.	Terdapat tanggung jawab dan fungsi dari masing – masing staf yang dipekerjakan di LPD	✓		
A.8.1.2	Penyaringan (*Screening*)			
2.	LPD melakukan verifikasi latar belakang terhadap karyawan baru yang akan dipekerjakan	✓		
3.	LPD melakukan pemeriksaan sesuai dengan hukum, peraturan, dan etika yang relevan terhadap staf yang akan dipekerjakan	✓		
A.8.1.3	Rumusan Syarat Dan Aturan Dalam Kepegawaian			
4.	Semua staf yang bekerja di LPD Desa Adat Buleleng bersedia untuk menandatangani perjanjian kerahasiaan informasi	✓		

A.8.2	Selama Bekerja			
A.8.2.1	Tanggung Jawab Manajemen			
No	Pernyataan	Relevan	Tidak Relevan	Keterangan
5.	Manajemen memberikan penjelasan kepada semua staf dan pengguna pihak ketiga untuk menerapkan keamanan sesuai dengan kebijakan dan prosedur yang ditetapkan	✓		
A.8.2.2	Proses Pendisiplinan			
6.	Terdapat proses pendisiplinan formal yang dapat diterapkan pada staf yang telah melakukan pelanggaran keamanan informasi	✓		
A.8.3	Pengakhiran Dan Perubahan Pekerjaan			
A.8.3.1	Tanggung Jawab Pengakhiran Pekerjaan			
7.	Terdapat proses terdokumentasi formal untuk mengakhiri atau mengubah tugas pekerjaan	✓		Dipertegas untuk dokumentasi formal yang di maksud
8.	LPD Desa Adat Buleleng mampu menegakkan kepatuhan dengan tugas pasca kerja	✓		Dipertegas apa yang di maksud dengan kepatuhan dengan tugas pasca kerja

A.8.3.2	Pengembalian Aset			
No	Pernyataan	Relevan	Tidak Relevan	Keterangan
9.	Terdapat proses untuk memastikan semua staf dan pengguna eksternal mengembalikan aset organisasi pada pemutusan hubungan kerja, kontrak, atau perjanjian mereka	✓		
A.8.3.3	Penghapusan Hak Akses			
10.	Terdapat proses untuk memastikan hak akses pengguna dihapus pada pemutusan hubungan kerja atau kontrak, atau disesuaikan dengan perubahan	✓		

A.9	Keamanan Fisik Dan Lingkungan			
A.9.1	Area Yang Aman			
A.9.1.1	Parameter Keamanan Fisik			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
1.	Batasan keamanan yang ditentukan di LPD Desa Adat Buleleng, dan area informasi sensitive atau kritis dipisahkan serta dikontrol dengan tepat	✓		Batasan keamanan yang dimaksud seperti apa?
A.9.1.2	Menjaga Ruangan, Kantor, Atau Fasilias Lainnya			
2.	Ruangan, kantor, atau fasilitas lainnya telah dirancang dan dikonfigurasi dengan mempertimbangkan keamanan	✓		Dipertegas untuk perencanaan keamanan sudah diperhitungkan Dilihat dari sisi gedung dan perangkatnya?
A.9.1.3	Penjagaan Terhadap Adanya Ancaman			
3.	Melakukan perlindungan maupun pencegahan dari ancaman baik itu ancaman eksternal, maupun internal	✓		Apakah lpd punya rencana perlindungan/pencegahan jika terjadi ancaman
A.9.1.4	Bekerja Di Area Yang Aman			
4.	LPD Desa Adat Buleleng sudah menerapkan prosedur untuk bekerja di daerah yang aman dan sudah diterapkan	✓		Dipertegas untuk area aman seperti apa?

A.9.1.5	Area Akses Publik Dan Bongkar Muat			
No	Pernyataan	Relevan	Tidak Relevan	Keterangan
5.	Terdapat akses publik yang terisolasi dari fasilitas pemrosesan informasi	✓		Apakah keamanan secara fisik/teknologi?
A.9.2	Keamanan Peralatan			
A.9.2.1	Penempatan Dan Perlindungan Peralatan			
6.	Terdapat identifikasi bahaya lingkungan yang diidentifikasi dan dipertimbangkan ketika lokasi peralatan dipilih	✓		Dipertegas lagi Maksudnya dari lokasi peralatan yang dipilih seperti apa?
A.9.2.2	Sarana Pendukung			
7	Terdapat UPS atau generator cadangan dan telah diuji dalam skala waktu yang sesuai	✓		Dipertegas apa maksud dari skala waktu yang sesuai?
A.9.2.3	Keamanan Kabel			
8.	Penilaian risiko yang telah dilakukan di lokasi kabel listrik dan telekomunikasi	✓		Penilaian resiko apa yang dilakukan? Dipertegas lagi

A.9.2.4	Pemeliharaan Peralatan			
No	Pernyataan	Relevan	Tidak Relevan	Keterangan
9.	Terdapat jadwal pemeliharaan peralatan yang ketat	✓		Diperjelas tentang jadwal pemeliharaan dan kosekuensi jika tidak melaksanakannya?
A.9.2.5	Pembuangan Atas Penggunaan Kembali Peralatan Dengan Aman			
10.	Kebijakan yang mencakup bagaimana aset informasi dapat digunakan kembali Dimana data dihapus, apakah sudah diverifikasi dengan benar	✓		Dipertegas untuk penghapusan dokumen seperti apa prosedurnya

A.11	Pengendalian Akses			
A.11.1	Persyaratan Proses Bisnis Dalam Pengendalian Akses			
A.11.1.1	Kebijakan Pengendalian Akses			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
1.	Terdapat kebijakan pengendalian akses yang terdokumentasi dan apakah kebijakan tersebut didasari kebutuhan bisnis	✓		Di pertegas Apa maksud dari kebijakan pengendalian akses yang terdukumentasi?
A.11.2	Manajemen Pengguna			
A.11.2.1	Pendaftaran Pengguna			
2.	Terdapat proses pendaftaran akses pengguna secara formal	✓		
A.11.2.2	Manajemen *Password* Pengguna			
3.	Sistem manajemen *password* pengguna sudah sesuai dengan standar keamanan	✓		
A.11.2.3	Tinjauan Terhadap Hak Akses Pengguna			
4.	Terdapat proses bagi pemilik aset untuk meninjau hak akses ke aset mereka secara teratur dan apakah proses peninjauan ini diverifikasi	✓		Dipertegas lagi apa yang dimaksud dengan akses" pengguna

A.11.3	Tanggung Jawab Pengguna			
A.11.3.1	Penggunaan *Password* Pengguna			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
5.	Sistem *password* pengguna interaktif dan *password* yang rumit diperlukan	✓		Diperbaiki untuk pernyataanya mengenai password yang interaktif
A.11.3.2	Kebijakan *Clear Desk Dan Clear Screen*			
6.	Terdapat kebijakan *Clear Desk Dan Clear Screen*	✓		Apa yang di maksud denga clear desk dan clear screen?
A.11.4	Pengendalian Akses Jaringan			
A.11.4.1	Kebijakan Mengenai Penggunaan Layanan Jaringan			
7	Terdapat proses manajemen jaringan	✓		
A.11.4.2	Identifikasi Peralatan Dalam Jaringan			
8.	Melakukan identifikasi peralatan dalam jaringan yang digunakan	✓		Apa yang dimaksud dengan identifikasi peralatan?

A.11.4.3	Segregasi Dalam jaringan			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
9.	Topologi jaringan memberlakukan pemisahan jaringan untuk tugas yang berbeda	✓		
A.11.5	Pengendalian Akses Sistem Operasi			
A.11.5.1	Langkah *Log- On* Yang Aman			
10.	Terdapat akses yang dikendalikan oleh prosedur *log-on* yang aman	✓		Diperjelas untuk log on yang dilakukan dan log onnya ke mana?
A.11.5.2	Proses Identifikasi dan Otentikasi Pengguna			
11.	Terdapat proses identifikasi dan otentikasi pengguna dalam penggunaan aplikasi	✓		
A.11.5.3	Sistem Manajemen *Password*			
12.	Terdapat sistem manajemen *password* didalam aplikasi	✓		Dipertegas apa yang dimaksud dengan manajemen pass di dalam aplikasi

A.11.5.4	Penggunaan Sistem *Utilities*			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
13.	Sistem *Utilities* tambahan di dalam aplikasi	✓		Maksud dari utilitas tambahan?
A.11.5.5	Sesi *Time-Out*			
14.	Sesi *time-out* di dalam proses transaksi di aplikasi	✓		Dipertegas lagi apa bedanya dengan yang no 15
A.11.5.6	Pembatasan Waktu Koneksi			
15.	Terdapat pembatasan waktu koneksi saat aplikasi tidak digunakan	✓		Dipertegas lagi untuk pernyataannya
A.11.6	Pengendalian Akses Aplikasi Dan Informasi			
A.11.6.1	Pembatasan Akses Informasi			
16.	Akses ke informasi dan fungsi sistem aplikasi dibatasi sesuai dengan kebijakan kontrol akses	✓		

A.11.6.2	Isolasi sistem yang *sensitive*			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
17.	Terdapat pengisolasian sistem yang dianggap *sensitive*	✓		
A.11.7	*Mobile Computing* Dan Kerja Jarak Jauh (*Teleworking*)			
A.11.7.1	*Mobile Computing Dan Komunikasi*			
18.	Aplikasi yang digunakan menerapkan *mobile computing* dalam penggunaanya	✓		
A.11.7.2	*Kerja Jarak Jauh (TeleWorking)*			
19.	Terdapat kebijakan untuk *teleworking* di LPD Desa Adat Buleleng	✓		
20.	Terdapat proses yang ditetapkan untuk pekerja jarak jauh untuk mendapatkan akses serta diberi saran dan peralatan untuk melindungi asset mereka	✓		

A.13	Manajemen Keamanan Informasi			
A.13.1	Melaporkan Insiden Keamanan			
A.13.1.1	Melaporkan Insiden Terhadap Keamanan Informasi			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
1.	Terdapat proses pelaporan kejadian keamanan informasi secara tepat waktu dan apakah ada proses untuk meninjau dan bertindak atas peristiwa keamanan informasi yang dilaporkan	✓		
A.13.1.2	Pelaporan Kelemahan Keamanan			
2.	Terdapat proses pelaporan kelemahan keamanan informasi yang teridentifikasi	✓		
3.	Proses ini dikomunikasikan secara luas dan Apakah ada proses untuk meninjau dan menangani laporan secara tepat waktu	✓		Dipertegas lagi

A.13.2	Manajemen Mengenai Insiden Keamanan Informai Dan Perbaikan			
A.13.2.1	Tanggung Jawab Dan Prosedur			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
4.	Terdapat tanggung jawab manajemen diidentifikasikan dan didokumentasikan dengan jelas dalam proses manajemen insiden	✓		Diperjelas lagi apa yang dimaksud dari kaliamat tersebut
A.13.2.2	Pembelajaran Dari Insiden Keamanan Informasi			
5.	Terdapat proses atau kerangka kerja yang memungkinkan organisasi untuk belajar dari insiden keamanan informasi dan mengurangi dampak/kemungkinan kejadian di masa depan	✓		
A.13.2.3	Pengumpulan Informasi			
6.	Terdapat kebijakan kesiapan forensik jika terjadi insiden keamanan informasi	✓		

No.	Pernyataan			Keterangan
7	Terdapat data yang relevan dikumpulkan dengan cara yang memungkinkan untuk digunakan sebagai bukti	✓		

Singaraja, 28 Januari 2023

Gede Arna Jude Saskara, S.T.,M.T.
NIP. 199105152020121003

No: 1

PENGUJIAN

KUESIONER

PENGUKURAN MANAJEMEN RESIKO KEAMANAN INFORMASI MENGGUNAKAN STANDARISASI ISO/IEC 27001 PADA

LPD DESA ADATBULELENG

DATA RESPONDEN

Nama : Gede Arna Jude Saskara, S.T.,M.T.

Bidang ahli : Sistem Informasi

PETUNJUK PENGISIAN

1. Isilah identitas diri pada tempat data responden di atas yaitu nama responden danbidang ahli .
2. Dimohonkan kesediaan Bapak/Ibu guru untuk menjawab setiap nomor itemangket dengan sejujurnya sesuai dengan petunjuk yang ada.
3. Pilihlah jawaban dengan memberikan tanda (√) pada kolom pilihan Bapak/Ibu.
4. Setiap pertanyaan harus dijawab, dan tidak boleh ada yang kosong.
5. Tidak ada jawaban yang dianggap salah, benar, baik maupun buruk, karena ituBapak/Ibu tidak perlu ragu dalam mengisi angket ini.
6. Setelah selesai diisi, mohon angket ini agar segera dikembalikan kepada peneliti.

Keterangan :

1. Mengenai klausul yang dipakai dalam ISO/IEC 27001 Terlampir.

2. Pada kolom keterangan diisikan saran dan perbaikan untuk butir soal padasetiap klausul.

Kontrol dalam ISO/IEC 27001

A.5 Information Security Policies (Kebijakan Keamanan Informasi)

Dirancang untuk memastikan bahwa kebijakan ditulis dan diawasi secarakeseluruhan sesuai dengan arahan dari organisasi keamanan informasi.

A.6 Organisation of Information Security (Keamanan Informasi Perusahaan)

mencakup tugas dan tanggung jawab tertentu. *Annex* ini terbagi menjadi dua yaitu:

- A.6.1 yang memastikan bahwa organisasi telah menetapkan kerangka kerja yangdapat menerapkan dan memelihara keamanan informasi secara memadai.

- A.6.2 yang membahas *mobile devices* dan *remote working*. Siapa pun yang bekerja dari rumah atau perjalanan, baik penuh waktu atau paruh waktu, bisa mengikuti aturan yang berlaku.

A.7 Asset Management (Manajemen Aset)

Cara bagaimana organisasi atau perusahaan mengidentifikasi aset informasi dan menentukan tanggung jawab perlindungan sesuai dengan standar yang berlaku

A.8 Human Resource Security (Keamanan Sumber Daya Manusia)

Memastikan bahwa karyawan dan kontraktor memahami hak dan tanggungjawab mereka di perusahaan.

A.9 Physical and Environmental Security (Keamanan Fisik dan Lingkungan)

Membahas keamanan fisik dan lingkungan pada organisasi atau perusahaanyang terbagi menjadi dua, yaitu:

- A.9.1 untuk mencegah akses fisik yang tidak sah, kerusakan atau gangguan ke tempat organisasi atau data yang ada di dalamnya.
- A.9.2 untuk mencegah kehilangan, kerusakan atau pencurian peralatan aset informasi perusahaan baik itu *software* atau *file* fisik.

A.11 Access Control (Kontrol Akses)

Kontrol akses ini bertujuan untuk memastikan bahwa karyawan hanya bisamelihat dan mengelola informasi yang relevan dengan jabatan mereka.

Kontrol akses memiliki empat bagian yaitu persyaratan bisnis dari kontrol akses, manajemen akses pengguna, tanggung jawab pengguna dan kontrol akses pada sistem dan aplikasi.

A.13 Information Security Incident Management (Manajemen Insiden Keamanan Informasi)

Dalam bagian ini membahas bagaimana mengelola dan melaporkan insiden keamanan. Proses ini melibatkan penjelasan karyawan mana saja yang harus bertanggung jawab terhadap tindakan tertentu sehingga penanganannya bisa konsisten dan efektif

A.5	Kebijakan Keamanan			
A.5.1	Kebijakan Terhadap Keamanan Informasi			
A.5.1.1	Dokumen Mengenai Keamanan Informasi			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
1.	LPD memiliki dokumen mengenai keamanan informasi	✓		
2.	LPD telah melaksanakan sosialisi tentang kebijakan keamanan informasi dan telah di terapkan	✓		
A.5.1.2	Kajian Terhadap Keamanan Informasi			
3.	LPD telah melakukan kajian terhadap Keamanan informasi serta telah mengevaluasi kebijakan keamanan informasi	✓		
4.	LPD telah melakukan pengkajian terhadap keamanan informasi mengikuti perkembangan zaman	✓		

A.6	Organisasi Mengenai Keamanan Informasi			
A.6.1	Organisasi Internal			
A.6.1.1	Komitmen Tehadap Keamanan Informasi			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
1.	LPD telah memiliki komitmen dalam menerapkan keamanan informasi	✓		
A.6.1.2	Koordinasi Mengenai Keamanan Informasi			
2.	LPD melaksanakan koordinasi mengenai keamanan informasi	✓		
A.6.1.3	Perjanjian Perihal Kerahasiaan			
3.	LPD telah melakukan perjanjian kerjasama perihal kerahasian informasi dengan BSSN,KOMINFO maupun instansi yang terkait keamanan informasi lainnya	✓		
A.6.1.4	Kontak Terhadap Suatu Kelompok Khusus			
4.	LPD telah melakukan kontak dengan tim yang memahami tentang keamanan informasi seperti BSSN,KOMINFO maupun tim yang terkait dengan keamanan data	✓		

A.6.1.5	Kajian Yang Independen Terhadap Keamanan Informasi			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
5.	LPD telah melakukan kajian yang independen terhadap keamanan informasi	✓		
A.6.2	Perihal Pihak Eksternal			
A.6.2.1	Identifikasi Resiko Dari Pihak Eksternal			
6.	LPD telah melakukan indentifikasi resiko dari aplikasi yang digunakan dari pihak pengembang	✓		
A.6.2.2	Penekanan Keamanan Ketika Menjalin Kontak Dengan Pelanggan			
7.	LPD telah melakukan penekanan keamanaan pada saat menjalin kontak dengan nasabah	✓		
A.6.2.3	Penekanan Perjanjian Terhadap Pihak Ketiga			
8.	LPD telah melakukan perjanjian kerjasama dengan pihak pengembang aplikasi terkait tentang penekanan keamanan informasi	✓		

A.7	Manajemen Aset			
A.7.1	Tanggung Jawab Terhadap Aset			
A.7.1.1	Inventaris Aset			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
1.	LPD miliki inventarisasi semua aset yang berkait dengan informasi dan pemrosesan informasi di LPD	✓		
A.7.1.2	Kepemilikan Aset			
2.	Semua asset LPD tentang informasi memiliki pemilik yang jelas dan menyadari tanggung jawab mereka	✓		
A.7.1.3	Penerapan Aset Yang Telah Masuk			
3.	LPD memiliki kebijakan pengguna yang dapat diterima untuk setiap kelas/jenis aset informasi	✓		

A.7.2	Klasifikasi Informasi			
A.7.2.1	Pedoman Klasifikasi			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
4.	LPD kebijakan yang mengatur klasifikasi informasi	✓		
A.7.2.2	Pelabelan Dan Penanganan Informasi			
5.	LPD memiliki prosedur atau proses untuk klasifikasi informasi ditandai dengan tepat pada setiap aset	✓		
6.	LPD memiliki proses untuk mengurutkan asset secara tepat	✓		

A.8	Keamanan Sumber Daya Manusia			
A.8.1	Sebelum Dipekerjakan			
A.8.1.1	Tanggung Jawab Dan Fungsi			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
1.	Terdapat tanggung jawab dan fungsi dari masing – masing staf yang dipekerjakan di LPD	✓		
A.8.1.2	Penyaringan (*Screening*)			
2.	LPD melakukan verifikasi latar belakang terhadap karyawan baru yang akan dipekerjakan	✓		
3.	LPD melakukan pemeriksaan sesuai dengan hukum, peraturan, dan etika yang relevan terhadap staf yang akan dipekerjakan	✓		

A.8.1.3	Rumusan Syarat Dan Aturan Dalam Kepegawaian			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
4.	Semua staf yang bekerja di LPD Desa Adat Buleleng bersedia untuk menandatangani perjanjian kerahasiaan informasi	✓		
A.8.2	Selama Bekerja			
A.8.2.1	Tanggung Jawab Manajemen			
5.	LPD memberikan penjelasan kepada semua staf dan pengguna pihak ketiga untuk menerapkan keamanan sesuai dengan kebijakan dan prosedur yang ditetapkan	✓		
A.8.2.2	Proses Pendisiplinan			
6.	LPD memiliki proses pendisiplinan formal yang dapat diterapkan pada staf yang telah melakukan pelanggaran keamanan informasi	✓		

A.8.3	Pengakhiran Dan Perubahan Pekerjaan			
A.8.3.1	Tanggung Jawab Pengakhiran Pekerjaan			
No	Pernyataan	Relevan	Tidak Relevan	Keterangan
7.	LPD memiliki proses terdokumentasi formal untuk mengakhiri atau mengubah tugas pekerjaan	✓		
8.	LPD telah menegakkan kepatuhan dengan tugas pasca kerja	✓		
A.8.3.2	Pengembalian Aset			
9.	LPD memiliki proses untuk memastikan semua staf dan pengguna eksternal mengembalikan aset organisasi pada pemutusan hubungan kerja, kontrak, atau perjanjian mereka	✓		

A.8.3.3	Penghapusan Hak Akses			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
10.	LPD proses untuk memastikan hak akses pengguna dihapus pada pemutusan hubungan kerja atau kontrak, atau disesuaikan dengan perubahan	✓		

A.9	Keamanan Fisik Dan Lingkungan			
A.9.1	Area Yang Aman			
A.9.1.1	Parameter Keamanan Fisik			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
1.	LPD memiliki batasan keamanan informasi yang ditentukan, dan area informasi sensitive atau kritis dipisahkan serta dikontrol dengan tepat	✓		
A.9.1.2	Menjaga Ruangan, Kantor, Atau Fasilias Lainnya			
2.	LPD memiliki ruangan, kantor, atau fasilitas lainnya telah dirancang dan dikonfigurasi dengan mempertimbangkan keamanan informasi	✓		
A.9.1.3	Penjagaan Terhadap Adanya Ancaman			
3.	LPD memiliki rencana perlindungan maupun pencegahan dari ancaman baik itu ancaman eksternal, maupun internal	✓		

A.9.1.4	Bekerja Di Area Yang Aman			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
4.	LPD Desa Adat Buleleng sudah menerapkan prosedur untuk bekerja di daerah yang aman dan sudah diterapkan	✓		
A.9.1.5	Area Akses Publik Dan Bongkar Muat			
5.	LPD memiliki akses publik yang terisolasi dari fasilitas pemrosesan informasi	✓		
A.9.2	Keamanan Peralatan			
A.9.2.1	Penempatan Dan Perlindungan Peralatan			
6.	LPD telah melakukan identifikasi bahaya lingkungan yang diidentifikasi dan dipertimbangkan ketika pemilihan lokasi peralatan	✓		

A.9.2.2	Sarana Pendukung			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
7	LPD memiliki UPS atau generator cadangan dan telah diuji dalam skala waktu yang sesuai	✓		
A.9.2.3	Keamanan Kabel			
8.	LPD memiliki penilaian risiko yang telah dilakukan di lokasi kabel listrik dan telekomunikasi	✓		
A.9.2.4	Pemeliharaan Peralatan			
9.	LPD memilki jadwal pemeliharaan peralatan yang dilakukan secara rutin dan konsisten	✓		

A.9.2.5	Pembuangan Atas Penggunaan Kembali Peralatan Dengan Aman			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
10.	LPD memiliki kebijakan yang mencakup bagaimana aset informasi dapat digunakan kembali dimana data dihapus, dan sudah diverifikasi dengan benar	✓		

A.11	Pengendalian Akses			
A.11.1	Persyaratan Proses Bisnis Dalam Pengendalian Akses			
A.11.1.1	Kebijakan Pengendalian Akses			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
1.	LPD memiliki kebijakan pengendalian akses yang terdokumentasi yang didasari kebutuhan bisnis	✓		
A.11.2	Manajemen Pengguna			
A.11.2.1	Pendaftaran Pengguna			
2.	LPD memiliki proses pendaftaran akses pengguna secara formal	✓		
A.11.2.2	Manajemen *Password* Pengguna			
3.	LPD memiliki sistem manajemen *password* pengguna sudah sesuai dengan standar keamanan	✓		

A.11.2.3	Tinjauan Terhadap Hak Akses Pengguna			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
4.	LPD melaksanakan peninjauan secara teratur dan terverifikasi terhadap kepemilikan asset dan hak aksesnya	✓		
A.11.3	Tanggung Jawab Pengguna			
A.11.3.1	Penggunaan *Password* Pengguna			
5.	LPD memiliki sistem password yang tidak mudah diretas	✓		
A.11.3.2	Kebijakan *Clear Desk Dan Clear Screen*			
6.	LPD memiliki kebijakan *Clear Desk Dan Clear Screen*	✓		

A.11.4	Pengendalian Akses Jaringan			
A.11.4.1	Kebijakan Mengenai Penggunaan Layanan Jaringan			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
7	LPD memiliki kebijakan pengguna layanan jaringan	✓		
A.11.4.2	Identifikasi Peralatan Dalam Jaringan			
8.	LPD Melakukan identifikasi peralatan dalam jaringan yang digunakan	✓		
A.11.4.3	Segregasi Dalam jaringan			
9.	LPD memiliki topologi jaringan yang memberlakukan pemisahan jaringan untuk tugas yang berbeda	✓		

A.11.5	Pengendalian Akses Sistem Operasi			
A.11.5.1	Langkah *Log- On* Yang Aman			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
10.	LPD memiliki akses yang dikendalikan oleh prosedur *log-on* yang aman pada aplikasi	✓		
A.11.5.2	Proses Identifikasi dan Otentikasi Pengguna			
11.	LPD memiliki proses identifikasi dan otentikasi pengguna dalam penggunaan aplikasi	✓		
A.11.5.3	Sistem Manajemen *Password*			
12.	LPD memiliki sistem manajemen password	✓		

A.11.5.4	Penggunaan Sistem *Utilities*			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
13.	LPD menggunakan Sistem *Utilities* tambahan	✓		
A.11.5.5	Sesi *Time-Out*			
14.	LPD memiliki sesi *time-out* di dalam proses transaksi di aplikasi	✓		
A.11.5.6	Pembatasan Waktu Koneksi			
15.	LPD memiliki pembatasan waktu koneksi saat aplikasi tidak digunakan	✓		

A.11.6	Pengendalian Akses Aplikasi Dan Informasi			
A.11.6.1	Pembatasan Akses Informasi			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
16.	LPD mempunyai akses ke informasi dan fungsi sistem aplikasi dibatasi sesuai dengan kebijakan kontrol akses	✓		
A.11.6.2	Isolasi sistem yang *sensitive*			
17.	LPD memiliki pengisolasian sistem yang dianggap *sensitive*	✓		

A.11.7	*Mobile Computing* Dan Kerja Jarak Jauh (*Teleworking*)			
A.11.7.1	*Mobile Computing Dan Komunikasi*			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
18.	Aplikasi yang digunakan di LPD menerapkan *mobile computing* dalam penggunaanya	✓		
A.11.7.2	*Kerja Jarak Jauh (TeleWorking)*			
19.	Terdapat kebijakan untuk *teleworking* di LPD Desa Adat Buleleng	✓		
20.	LPD memiliki proses yang ditetapkan untuk pekerja jarak jauh untuk mendapatkan akses serta diberi saran dan peralatan untuk melindungi asset mereka	✓		

A.13	Manajemen Keamanan Informasi			
A.13.1	Melaporkan Insiden Keamanan			
A.13.1.1	Melaporkan Insiden Terhadap Keamanan Informasi			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
1.	LPD mempunyai proses pelaporan kejadian keamanan informasi secara tepat waktu serta terdapat proses untuk meninjau dan bertindak atas peristiwa keamanan informasi yang dilaporkan	✓		
A.13.1.2	Pelaporan Kelemahan Keamanan			
2.	LPD mempunyai proses pelaporan kelemahan keamanan informasi yang teridentifikasi	✓		

No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
3.	LPD memiliki proses pelaporan keamanan yang dikomunikasikan secara luas dan meninjau serta menangani laporan secara tepat waktu	✓		
A.13.2	Manajemen Mengenai Insiden Keamanan Informai Dan Perbaikan			
A.13.2.1	Tanggung Jawab Dan Prosedur			
4.	LPD memiliki tanggung jawab manajemen diidentifikasikan dan didokumentasikan dengan jelas dalam proses manajemen insiden	✓		
A.13.2.2	Pembelajaran Dari Insiden Keamanan Informasi			
5.	LPD memiliki proses atau kerangka kerja yang memungkinkan organisasi untuk belajar dari insiden keamanan informasi dan mengurangi dampak/kemungkinan kejadian di masa depan	✓		

A.13.2.3	Pengumpulan Informasi			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
6.	LPD memiliki kebijakan kesiapan forensik jika terjadi insiden keamanan informasi	✓		
No.	Pernyataan			Keterangan
7	LPD memiliki data yang relevan dikumpulkan dengan cara yang memungkinkan untuk digunakan sebagai bukti	✓		

Singaraja, 1 Februari 2023

Gede Arna Jude Saskara, S.T.,M.T.
NIP. 199105152020121003

No: 2

PENGUJIAN KUESIONER

PENGUKURAN MANAJEMEN RESIKO KEAMANAN INFORMASI MENGGUNAKAN STANDARISASI ISO/IEC 27001 PADA LPD DESA ADAT BULELENG

DATA RESPONDEN

Nama : I MADE ARDWI PRADNYANA, S.T.,M.T
Bidang ahli : Sistem Informasi

PETUNJUK PENGISIAN

7. Isilah identitas diri pada tempat data responden di atas yaitu nama responden dan bidang ahli .
8. Dimohonkan kesediaan Bapak/Ibu guru untuk menjawab setiap nomor item angket dengan sejujurnya sesuai dengan petunjuk yang ada.
9. Pilihlah jawaban dengan memberikan tanda (√) pada kolom pilihan Bapak/Ibu.
10. Setiap pertanyaan harus dijawab, dan tidak boleh ada yang kosong.
11. Tidak ada jawaban yang dianggap salah, benar, baik maupun buruk, karena itu Bapak/Ibu tidak perlu ragu dalam mengisi angket ini.
12. Setelah selesai diisi, mohon angket ini agar segera dikembalikan kepada peneliti.

Keterangan :

3. Mengenai klausul yang dipakai dalam ISO/IEC 27001 Terlampir.
4. Pada kolom keterangan diisikan saran dan perbaikan untuk butir soal pada setiap klausul.

Kontrol dalam ISO/IEC 27001

A.5 Information Security Policies (Kebijakan Keamanan Informasi)

Dirancang untuk memastikan bahwa kebijakan ditulis dan diawasi secara keseluruhan sesuai dengan arahan dari organisasi keamanan informasi.

A.6 Organisation of Information Security (Keamanan Informasi Perusahaan)

mencakup tugas dan tanggung jawab tertentu. *Annex* ini terbagi menjadi dua yaitu:

- A.6.1 yang memastikan bahwa organisasi telah menetapkan kerangka kerja yang dapat menerapkan dan memelihara keamanan informasi secara memadai.

- A.6.2 yang membahas *mobile devices* dan *remote working*. Siapa pun yang bekerja dari rumah atau perjalanan, baik penuh waktu atau paruh waktu, bisa mengikuti aturan yang berlaku.

A.7 Asset Management (Manajemen Aset)

Cara bagaimana organisasi atau perusahaan mengidentifikasi aset informasi dan menentukan tanggung jawab perlindungan sesuai dengan standar yang berlaku

A.8 Human Resource Security (Keamanan Sumber Daya Manusia)

Memastikan bahwa karyawan dan kontraktor memahami hak dan tanggung jawab mereka di perusahaan.

A.9 Physical and Environmental Security (Keamanan Fisik dan Lingkungan)

Membahas keamanan fisik dan lingkungan pada organisasi atau

perusahaan yang terbagi menjadi dua, yaitu:

- A.9.1 untuk mencegah akses fisik yang tidak sah, kerusakan atau gangguan ke tempat organisasi atau data yang ada di dalamnya.
- A.9.2 untuk mencegah kehilangan, kerusakan atau pencurian peralatan aset informasi perusahaan baik itu *software* atau *file* fisik.

A.11 Access Control (Kontrol Akses)

Kontrol akses ini bertujuan untuk memastikan bahwa karyawan hanya bisa melihat dan mengelola informasi yang relevan dengan jabatan mereka.

Kontrol akses memiliki empat bagian yaitu persyaratan bisnis dari kontrol akses, manajemen akses pengguna, tanggung jawab pengguna dan kontrol akses pada sistem dan aplikasi.

A.13 Information Security Incident Management (Manajemen Insiden Keamanan Informasi)

Dalam bagian ini membahas bagaimana mengelola dan melaporkan insiden keamanan. Proses ini melibatkan penjelasan karyawan mana saja yang harus bertanggung jawab terhadap tindakan tertentu sehingga penanganannya bisa konsisten dan efektif.

A.5	Kebijakan Keamanan			
A.5.1	Kebijakan Terhadap Keamanan Informasi			
A.5.1.1	Dokumen Mengenai Keamanan Informasi			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
1.	Kebijakan keamanan informasi telah dilakukan oleh LPD Desa Adat Buleleng		✓	
2.	LPD telah melaksanakan kebijakan keamanan informasi dan telah dikomunikasikan dengan benar kepada pegawai		✓	
A.5.1.2	Kajian Terhadap Keamanan Informasi			
3.	LPD melakukan kajian terhadap Keamanan informasi		✓	
4.	Pengkajian terhadap keamanan informasi harus dilakukan ketika situasi berubah		✓	

A.6	Organisasi Mengenai Keamanan Informasi			
A.6.1	Organisasi Internal			
A.6.1.1	Komitmen Tehadap Keamanan Informasi			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
1.	LPD melaksanakan serangkaian komitmen terhadap suatu keamanan informasi	✓		dipertegas Apakah lpd telah memiliki komitmen dalam menerapkan keamanan informasi?
A.6.1.2	Koordinasi Mengenai Keamanan Informasi			
2.	LPD melaksanakan koordinasi mengenai keamanan informasi	✓		
A.6.1.3	Perjanjian Perihal Kerahasiaan			
3.	Terdapat perjanjian perihal kerahasian keamanan informasi		✓	apakah lpd telah memiliki perjanjian kerjasama dengan BSSN/KOMINFO
A.6.1.4	Kontak Terhadap Suatu Kelompok Khusus			
4.	LPD melakukan kontak dengan kelompok khusus yang memahami tentang keamanan informasi		✓	Lpd sudah memiliki kontak dengan tim keamanan bssn/kominfo buleleng terkait dengan keamanan data

A.6.1.5	Kajian Yang Independen Terhadap Keamanan Informasi			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
5.	LPD telah melakukan kajian yang independen terhadap keamanan informasi	✓		Diperjelas tentang kajian yang independen pada klausul yang ada sehingga lebih mempertegas pernyataan yang ada
A.6.2	Perihal Pihak Eksternal			
A.6.2.1	Identifikasi Resiko Dari Pihak Eksternal			
6.	Terdapat indentifikasi resiko dari pihak eksternal terkait aplikasi	✓		Lpd harus tahu resiko dari sistem yang telah digunakan (analis resiko) dipertegas kembali
A.6.2.2	Penekanan Keamanan Ketika Menjalin Kontak Dengan Pelanggan			
7.	Terdapat penekanan keamanaan pada saat menjalin kontak dengan nasabah	✓		Dipertegas pernyataan apakah ada tanda tangan kontrak
A.6.2.3	Penekanan Perjanjian Terhadap Pihak Ketiga			
8.	Terdapat penekanan keamanan pada saat melakukan perjanjian terhadap pihak ketiga terkait aplikasi	✓		Adakah klausul untuk perjanjian kerjasama lpd dengan pengembang sistem

A.7	Manajemen Aset			
A.7.1	Tanggung Jawab Terhadap Aset			
A.7.1.1	Inventaris Aset			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
1.	Terdapat inventarisasi semua aset yang berkait dengan informasi dan pemrosesan informasi di LPD	✓		
A.7.1.2	Kepemilikan Aset			
2.	Semua asset informasi memiliki pemilik yang jelas dan menyadari tanggung jawab mereka	✓		
A.7.1.3	Penerapan Aset Yang Telah Masuk			
3.	Terdapat kebijakan pengguna yang dapat diterima untuk setiap kelas/jenis aset informasi	✓		Dipertegas untuk kebijakannya apa saja yang terdapat di lpd

A.7.2	Klasifikasi Informasi			
A.7.2.1	Pedoman Klasifikasi			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
4.	Terdapat kebijakan yang mengatur klasifikasi informasi	✓		Dipertegas dengan contoh Misalkan informasi nasabah,dokumen dll
A.7.2.2	Pelabelan Dan Penanganan Informasi			
5.	Terdapat prosedur atau proses untuk klasifikasi informasi ditandai dengan tepat pada setiap aset	✓		Apakah terdapat prosedur untuk klasifikasi informasi Apakah terdapat proses untuk mengurutkan asset secara tepat

\

A.8	Keamanan Sumber Daya Manusia			
A.8.1	Sebelum Dipekerjakan			
A.8.1.1	Tanggung Jawab Dan Fungsi			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
1.	Terdapat tanggung jawab dan fungsi dari masing – masing staf yang dipekerjakan di LPD	✓		
A.8.1.2	Penyaringan (*Screening*)			
2.	LPD melakukan verifikasi latar belakang terhadap karyawan baru yang akan dipekerjakan	✓		
3.	LPD melakukan pemeriksaan sesuai dengan hukum, peraturan, dan etika yang relevan terhadap staf yang akan dipekerjakan	✓		
A.8.1.3	Rumusan Syarat Dan Aturan Dalam Kepegawaian			
4.	Semua staf yang bekerja di LPD Desa Adat Buleleng bersedia untuk menandatangani perjanjian kerahasiaan informasi	✓		

A.8.2	Selama Bekerja			
A.8.2.1	Tanggung Jawab Manajemen			
No	Pernyataan	Relevan	Tidak Relevan	Keterangan
5.	Manajemen memberikan penjelasan kepada semua staf dan pengguna pihak ketiga untuk menerapkan keamanan sesuai dengan kebijakan dan prosedur yang ditetapkan	✓		
A.8.2.2	Proses Pendisiplinan			
6.	Terdapat proses pendisiplinan formal yang dapat diterapkan pada staf yang telah melakukan pelanggaran keamanan informasi	✓		
A.8.3	Pengakhiran Dan Perubahan Pekerjaan			
A.8.3.1	Tanggung Jawab Pengakhiran Pekerjaan			
7.	Terdapat proses terdokumentasi formal untuk mengakhiri atau mengubah tugas pekerjaan	✓		Dipertegas untuk dokumentasi formal yang di maksud
8.	LPD Desa Adat Buleleng mampu menegakkan kepatuhan dengan tugas pasca kerja	✓		Dipertegas apa yang di maksud dengan kepatuhan dengan tugas pasca kerja

A.8.3.2	Pengembalian Aset			
No	Pernyataan	Relevan	Tidak Relevan	Keterangan
9.	Terdapat proses untuk memastikan semua staf dan pengguna eksternal mengembalikan aset organisasi pada pemutusan hubungan kerja, kontrak, atau perjanjian mereka	✓		
A.8.3.3	Penghapusan Hak Akses			
10.	Terdapat proses untuk memastikan hak akses pengguna dihapus pada pemutusan hubungan kerja atau kontrak, atau disesuaikan dengan perubahan	✓		

A.9	Keamanan Fisik Dan Lingkungan			
A.9.1	Area Yang Aman			
A.9.1.1	Parameter Keamanan Fisik			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
1.	Batasan keamanan yang ditentukan di LPD Desa Adat Buleleng, dan area informasi sensitive atau kritis dipisahkan serta dikontrol dengan tepat	✓		Batasan keamanan yang dimaksud seperti apa?
A.9.1.2	Menjaga Ruangan, Kantor, Atau Fasilias Lainnya			
2.	Ruangan, kantor, atau fasilitas lainnya telah dirancang dan dikonfigurasi dengan mempertimbangkan keamanan	✓		Dipertegas untuk perencanaan keamanan sudah diperhitungkan Dilihat dari sisi gedung dan perangkatnya?
A.9.1.3	Penjagaan Terhadap Adanya Ancaman			
3.	Melakukan perlindungan maupun pencegahan dari ancaman baik itu ancaman eksternal, maupun internal	✓		Apakah lpd punya rencana perlindungan/pencegahan jika terjadi ancaman
A.9.1.4	Bekerja Di Area Yang Aman			

4.	LPD Desa Adat Buleleng sudah menerapkan prosedur untuk bekerja di daerah yang aman.	✓		Dipertegas untuk area aman seperti apa?
A.9.1.5	Area Akses Publik Dan Bongkar Muat			
No	Pernyataan	Relevan	Tidak Relevan	Keterangan
5.	Terdapat akses publik yang terisolasi dari fasilitas pemrosesan informasi	✓		Apakah keamanan secara fisik/teknologi?
A.9.2	Keamanan Peralatan			
A.9.2.1	Penempatan Dan Perlindungan Peralatan			
6.	Terdapat identifikasi bahaya lingkungan yang diidentifikasi dan dipertimbangkan ketika pemilihan lokasi peralatan	✓		Dipertegas lagi Maksudnya dari lokasi peralatan yang dipilih seperti apa?
A.9.2.2	Sarana Pendukung			
7	Terdapat UPS atau generator cadangan dan telah diuji dalam skala waktu yang sesuai	✓		Dipertegas apa maksud dari skala waktu yang sesuai?
A.9.2.3	Keamanan Kabel			

8.	Penilaian risiko yang telah dilakukan di lokasi kabel listrik dan telekomunikasi	✓		Penilaian resiko apa yang dilakukan? Dipertegas lagi
A.9.2.4	Pemeliharaan Peralatan			
No	Pernyataan	Relevan	Tidak Relevan	Keterangan
9.	Terdapat jadwal pemeliharaan peralatan yang ketat	✓		Diperjelas tentang jadwal pemeliharaan dan kosekuensi jika tidak melaksanakannya?
A.9.2.5	Pembuangan Atas Penggunaan Kembali Peralatan Dengan Aman			
10.	Kebijakan yang mencakup bagaimana aset informasi dapat digunakan kembali dimana data dihapus, dan sudah diverifikasi dengan benar	✓		Dipertegas untuk penghapusan dokumen seperti apa prosedurnya

A.11	Pengendalian Akses			
A.11.1	Persyaratan Proses Bisnis Dalam Pengendalian Akses			
A.11.1.1	Kebijakan Pengendalian Akses			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
1.	Terdapat kebijakan pengendalian akses yang terdokumentasi dan apakah kebijakan tersebut didasari kebutuhan bisnis	✓		Lpd memiliki kebijakan pengendalian akses yang terdokumentasi yang didasari kebutuhan bisnis
A.11.2	Manajemen Pengguna			
A.11.2.1	Pendaftaran Pengguna			
2.	Terdapat proses pendaftaran akses pengguna secara formal	✓		
A.11.2.2	Manajemen *Password* Pengguna			
3.	Sistem manajemen *password* pengguna sudah sesuai dengan standar keamanan	✓		

A.11.2.3	Tinjauan Terhadap Hak Akses Pengguna			
4.	Terdapat proses bagi pemilik aset untuk meninjau hak akses ke aset mereka secara teratur dan apakah proses peninjauan ini diverifikasi	✓		Lpd melakasanakan peninjauan secara teratur dan terverifikasi terhadap kepemilikan asset dan hak aksesnya
A.11.3	Tanggung Jawab Pengguna			
A.11.3.1	Penggunaan *Password* Pengguna			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
5.	Sistem *password* pengguna interaktif dan *password* yang rumit	✓		Lpd memiliki sistem password pengguna yang tidak mudah diretas
A.11.3.2	Kebijakan *Clear Desk Dan Clear Screen*			
6.	Terdapat kebijakan *Clear Desk Dan Clear Screen*	✓		Lpd memiliki kebijakan *Clear Desk Dan Clear Screen*
A.11.4	Pengendalian Akses Jaringan			
A.11.4.1	Kebijakan Mengenai Penggunaan Layanan Jaringan			
7	Terdapat proses manajemen jaringan	✓		LPD memiliki kebijakan penggunaan layanan jaringan

A.11.4.2	Identifikasi Peralatan Dalam Jaringan			
8.	Melakukan identifikasi peralatan dalam jaringan yang digunakan	✓		Lpd melakukan indentifikasi peralatan jaringan yang digunakan
A.11.4.3	Segregasi Dalam jaringan			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
9.	Topologi jaringan memberlakukan pemisahan jaringan untuk tugas yang berbeda	✓		Lpd memiliki topologi jaringan yang memberlakukan pemisahan jaringan untuk tugas yang berbeda
A.11.5	Pengendalian Akses Sistem Operasi			
A.11.5.1	Langkah *Log- On* Yang Aman			
10.	Terdapat akses yang dikendalikan oleh prosedur *log-on* yang aman	✓		
A.11.5.2	Proses Identifikasi dan Otentikasi Pengguna			
11.	Terdapat proses identifikasi dan otentikasi pengguna dalam penggunaan aplikasi	✓		

A.11.5.3	Sistem Manajemen *Password*			
12.	Terdapat sistem manajemen *password* didalam aplikasi	✓		Lpd memiliki sistem manajemen password
A.11.5.4	Penggunaan Sistem *Utilities*			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
13.	Sistem *Utilities* tambahan di dalam aplikasi	✓		LPD menggunakan sistem utilities tambahan
A.11.5.5	Sesi *Time-Out*			
14.	Sesi *time-out* di dalam proses transaksi di aplikasi	✓		
A.11.5.6	Pembatasan Waktu Koneksi			
15.	Terdapat pembatasan waktu koneksi saat aplikasi tidak digunakan	✓		

A.11.6	Pengendalian Akses Aplikasi Dan Informasi			
A.11.6.1	Pembatasan Akses Informasi			
16.	Akses ke informasi dan fungsi sistem aplikasi dibatasi sesuai dengan kebijakan kontrol akses	✓		
A.11.6.2	Isolasi sistem yang *sensitive*			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
17.	Terdapat pengisolasian sistem yang dianggap *sensitive*	✓		
A.11.7	*Mobile Computing* Dan Kerja Jarak Jauh (*Teleworking*)			
A.11.7.1	*Mobile Computing Dan Komunikasi*			
18.	Aplikasi yang digunakan menerapkan *mobile computing* dalam penggunaanya	✓		
A.11.7.2	*Kerja Jarak Jauh (TeleWorking)*			
19.	Terdapat kebijakan untuk *teleworking* di LPD Desa Adat Buleleng	✓		
20.	Terdapat proses yang ditetapkan untuk pekerja jarak jauh untuk mendapatkan akses serta diberi saran dan peralatan untuk melindungi asset mereka	✓		

A.13	Manajemen Keamanan Informasi			
A.13.1	Melaporkan Insiden Keamanan			
A.13.1.1	Melaporkan Insiden Terhadap Keamanan Informasi			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
1.	Terdapat proses pelaporan kejadian keamanan informasi secara tepat waktu dan apakah ada proses untuk meninjau dan bertindak atas peristiwa keamanan informasi yang dilaporkan	✓		Di bagi 2 pernyataan
A.13.1.2	Pelaporan Kelemahan Keamanan			
2.	Terdapat proses pelaporan kelemahan keamanan informasi yang teridentifikasi	✓		

3.	Proses ini dikomunikasikan secara luas dan Apakah ada proses untuk meninjau dan menangani laporan secara tepat waktu	✓		Dipertegas lagi
A.13.2	Manajemen Mengenai Insiden Keamanan Informai Dan Perbaikan			
A.13.2.1	Tanggung Jawab Dan Prosedur			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
4.	Terdapat tanggung jawab manajemen diidentifikasikan dan didokumentasikan dengan jelas dalam proses manajemen insiden	✓		Lpd memiliki manajemen mengenai insiden keamanan informasi dan perbaikan yang mencakup tanggung jawab dan prosedur
A.13.2.2	Pembelajaran Dari Insiden Keamanan Informasi			
5.	Terdapat proses atau kerangka kerja yang memungkinkan organisasi untuk belajar dari insiden keamanan informasi dan mengurangi dampak/kemungkinan kejadian di masa depan	✓		

A.13.2.3	Pengumpulan Informasi			
6.	Terdapat kebijakan kesiapan forensik jika terjadi insiden keamanan informasi	✓		
No.	Pernyataan			Keterangan
7	Terdapat data yang relevan dikumpulkan dengan cara yang memungkinkan untuk digunakan sebagai bukti	✓		

Singaraja, 31 Januari 2023

I MADE ARDWI PRADNYANA, S.T.,M.T
NIP. 198611182015041001

No: 2

PENGUJIAN

KUESIONER

PENGUKURAN MANAJEMEN RESIKO KEAMANAN INFORMASI MENGGUNAKAN STANDARISASI ISO/IEC 27001 PADA

LPD DESA ADATBULELENG

DATA RESPONDEN

Nama : I MADE ARDWI PRADNYANA, S.T.,M.T
Bidang ahli : Sistem Informasi

PETUNJUK PENGISIAN

1. Isilah identitas diri pada tempat data responden di atas yaitu nama responden danbidang ahli .
2. Dimohonkan kesediaan Bapak/Ibu guru untuk menjawab setiap nomor itemangket dengan sejujurnya sesuai dengan petunjuk yang ada.
3. Pilihlah jawaban dengan memberikan tanda (√) pada kolom pilihan Bapak/Ibu.
4. Setiap pertanyaan harus dijawab, dan tidak boleh ada yang kosong.
5. Tidak ada jawaban yang dianggap salah, benar, baik maupun buruk, karena ituBapak/Ibu tidak perlu ragu dalam mengisi angket ini.
6. Setelah selesai diisi, mohon angket ini agar segera dikembalikan kepada peneliti.

Keterangan :

1. Mengenai klausul yang dipakai dalam ISO/IEC 27001 Terlampir.
2. Pada kolom keterangan diisikan saran dan perbaikan untuk butir soal padasetiap klausul.

Kontrol dalam ISO/IEC 27001

A.5 Information Security Policies (Kebijakan Keamanan Informasi)

Dirancang untuk memastikan bahwa kebijakan ditulis dan diawasi secarakeseluruhan sesuai dengan arahan dari organisasi keamanan informasi.

A.6 Organisation of Information Security (Keamanan Informasi Perusahaan)

mencakup tugas dan tanggung jawab tertentu. *Annex* ini terbagi menjadi dua yaitu:

- A.6.1 yang memastikan bahwa organisasi telah menetapkan kerangka kerja yangdapat menerapkan dan memelihara keamanan informasi secara memadai.
- A.6.2 yang membahas *mobile devices* dan *remote working*. Siapa pun yang bekerja dari rumah atau perjalanan, baik penuh waktu atau paruh waktu, bisa mengikuti aturan yang berlaku.

A.7 Asset Management (Manajemen Aset)

Cara bagaimana organisasi atau perusahaan mengidentifikasi aset informasi dan menentukan tanggung jawab perlindungan sesuai dengan standar yang berlaku

A.8 Human Resource Security (Keamanan Sumber Daya Manusia)

Memastikan bahwa karyawan dan kontraktor memahami hak dan tanggungjawab mereka di perusahaan.

A.9 Physical and Environmental Security (Keamanan Fisik dan Lingkungan)

Membahas keamanan fisik dan lingkungan pada organisasi atau perusahaanyang terbagi menjadi dua, yaitu:

- A.9.1 untuk mencegah akses fisik yang tidak sah, kerusakan atau gangguan ke tempat organisasi atau data yang ada di dalamnya.
- A.9.2 untuk mencegah kehilangan, kerusakan atau pencurian peralatan aset informasi perusahaan baik itu *software* atau *file* fisik.

A.11 Access Control (Kontrol Akses)

Kontrol akses ini bertujuan untuk memastikan bahwa karyawan hanya bisamelihat dan mengelola informasi yang relevan dengan jabatan mereka.

Kontrol akses memiliki empat bagian yaitu persyaratan bisnis dari kontrol akses, manajemen akses pengguna, tanggung jawab pengguna dan kontrol akses pada sistem dan aplikasi.

A.13 Information Security Incident Management (Manajemen Insiden Keamanan Informasi)

Dalam bagian ini membahas bagaimana mengelola dan melaporkan insiden keamanan. Proses ini melibatkan penjelasan karyawan mana saja yang harus bertanggung jawab terhadap tindakan tertentu sehingga penanganannya bisa konsisten dan efektif

A.5	Kebijakan Keamanan			
A.5.1	Kebijakan Terhadap Keamanan Informasi			
A.5.1.1	Dokumen Mengenai Keamanan Informasi			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
1.	LPD memiliki dokumen mengenai keamanan informasi	✓		
2.	LPD telah melaksanakan sosialisi tentang kebijakan keamanan informasi dan telah di terapkan	✓		
A.5.1.2	Kajian Terhadap Keamanan Informasi			
3.	LPD telah melakukan kajian terhadap Keamanan informasi serta telah mengevaluasi kebijakan keamanan informasi	✓		
4.	LPD telah melakukan pengkajian terhadap keamanan informasi mengikuti perkembangan zaman	✓		

A.6	Organisasi Mengenai Keamanan Informasi			
A.6.1	Organisasi Internal			
A.6.1.1	Komitmen Tehadap Keamanan Informasi			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
1.	LPD telah memiliki komitmen dalam menerapkan keamanan informasi	✓		
A.6.1.2	Koordinasi Mengenai Keamanan Informasi			
2.	LPD melaksanakan koordinasi mengenai keamanan informasi	✓		
A.6.1.3	Perjanjian Perihal Kerahasiaan			
3.	LPD telah melakukan perjanjian kerjasama perihal kerahasian informasi dengan BSSN,KOMINFO maupun instansi yang terkait keamanan informasi lainnya	✓		
A.6.1.4	Kontak Terhadap Suatu Kelompok Khusus			
4.	LPD telah melakukan kontak dengan tim yang memahami tentang keamanan informasi seperti BSSN,KOMINFO maupun tim yang terkait dengan keamanan data	✓		

A.6.1.5	Kajian Yang Independen Terhadap Keamanan Informasi			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
5.	LPD telah melakukan kajian yang independen terhadap keamanan informasi	✓		
A.6.2	Perihal Pihak Eksternal			
A.6.2.1	Identifikasi Resiko Dari Pihak Eksternal			
6.	LPD telah melakukan indentifikasi resiko dari aplikasi yang digunakan dari pihak pengembang	✓		
A.6.2.2	Penekanan Keamanan Ketika Menjalin Kontak Dengan Pelanggan			
7.	LPD telah melakukan penekanan keamanaan pada saat menjalin kontak dengan nasabah	✓		
A.6.2.3	Penekanan Perjanjian Terhadap Pihak Ketiga			
8.	LPD telah melakukan perjanjian kerjasama dengan pihak pengembang aplikasi terkait tentang penekanan keamanan informasi	✓		

A.7	Manajemen Aset			
A.7.1	Tanggung Jawab Terhadap Aset			
A.7.1.1	Inventaris Aset			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
1.	LPD miliki inventarisasi semua aset yang berkait dengan informasi dan pemrosesan informasi di LPD	✓		
A.7.1.2	Kepemilikan Aset			
2.	Semua asset LPD tentang informasi memiliki pemilik yang jelas dan menyadari tanggung jawab mereka	✓		
A.7.1.3	Penerapan Aset Yang Telah Masuk			
3.	LPD memiliki kebijakan pengguna yang dapat diterima untuk setiap kelas/jenis aset informasi	✓		

A.7.2	Klasifikasi Informasi			
A.7.2.1	Pedoman Klasifikasi			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
4.	LPD kebijakan yang mengatur klasifikasi informasi	✓		
A.7.2.2	Pelabelan Dan Penanganan Informasi			
5.	LPD memiliki prosedur atau proses untuk klasifikasi informasi ditandai dengan tepat pada setiap aset	✓		
6.	LPD memiliki proses untuk mengurutkan asset secara tepat	✓		

A.8	Keamanan Sumber Daya Manusia			
A.8.1	Sebelum Dipekerjakan			
A.8.1.1	Tanggung Jawab Dan Fungsi			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
1.	Terdapat tanggung jawab dan fungsi dari masing – masing staf yang dipekerjakan di LPD	✓		
A.8.1.2	Penyaringan (*Screening*)			
2.	LPD melakukan verifikasi latar belakang terhadap karyawan baru yang akan dipekerjakan	✓		
3.	LPD melakukan pemeriksaan sesuai dengan hukum, peraturan, dan etika yang relevan terhadap staf yang akan dipekerjakan	✓		

A.8.1.3	Rumusan Syarat Dan Aturan Dalam Kepegawaian			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
4.	Semua staf yang bekerja di LPD Desa Adat Buleleng bersedia untuk menandatangani perjanjian kerahasiaan informasi	✓		
A.8.2	Selama Bekerja			
A.8.2.1	Tanggung Jawab Manajemen			
5.	LPD memberikan penjelasan kepada semua staf dan pengguna pihak ketiga untuk menerapkan keamanan sesuai dengan kebijakan dan prosedur yang ditetapkan	✓		
A.8.2.2	Proses Pendisiplinan			
6.	LPD memiliki proses pendisiplinan formal yang dapat diterapkan pada staf yang telah melakukan pelanggaran keamanan informasi	✓		

A.8.3	Pengakhiran Dan Perubahan Pekerjaan			
A.8.3.1	Tanggung Jawab Pengakhiran Pekerjaan			
No	Pernyataan	Relevan	Tidak Relevan	Keterangan
7.	LPD memiliki proses terdokumentasi formal untuk mengakhiri atau mengubah tugas pekerjaan	✓		
8.	LPD telah menegakkan kepatuhan dengan tugas pasca kerja	✓		
A.8.3.2	Pengembalian Aset			
9.	LPD memiliki proses untuk memastikan semua staf dan pengguna eksternal mengembalikan aset organisasi pada pemutusan hubungan kerja, kontrak, atau perjanjian mereka	✓		

A.8.3.3	Penghapusan Hak Akses			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
10.	LPD proses untuk memastikan hak akses pengguna dihapus pada pemutusan hubungan kerja atau kontrak, atau disesuaikan dengan perubahan	✓		

A.9	Keamanan Fisik Dan Lingkungan			
A.9.1	Area Yang Aman			
A.9.1.1	Parameter Keamanan Fisik			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
1.	LPD memiliki batasan keamanan informasi yang ditentukan, dan area informasi sensitive atau kritis dipisahkan serta dikontrol dengan tepat	✓		
A.9.1.2	Menjaga Ruangan, Kantor, Atau Fasilias Lainnya			
2.	LPD memiliki ruangan, kantor, atau fasilitas lainnya telah dirancang dan dikonfigurasi dengan mempertimbangkan keamanan informasi	✓		
A.9.1.3	Penjagaan Terhadap Adanya Ancaman			
3.	LPD memiliki rencana perlindungan maupun pencegahan dari ancaman baik itu ancaman eksternal, maupun internal	✓		

A.9.1.4	Bekerja Di Area Yang Aman			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
4.	LPD Desa Adat Buleleng sudah menerapkan prosedur untuk bekerja di daerah yang aman dan sudah diterapkan	✓		
A.9.1.5	Area Akses Publik Dan Bongkar Muat			
5.	LPD memiliki akses publik yang terisolasi dari fasilitas pemrosesan informasi	✓		
A.9.2	Keamanan Peralatan			
A.9.2.1	Penempatan Dan Perlindungan Peralatan			
6.	LPD telah melakukan identifikasi bahaya lingkungan yang diidentifikasi dan dipertimbangkan ketika pemilihan lokasi peralatan	✓		

A.9.2.2	Sarana Pendukung			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
7	LPD memiliki UPS atau generator cadangan dan telah diuji dalam skala waktu yang sesuai	✓		
A.9.2.3	Keamanan Kabel			
8.	LPD memiliki penilaian risiko yang telah dilakukan di lokasi kabel listrik dan telekomunikasi	✓		
A.9.2.4	Pemeliharaan Peralatan			
9.	LPD memilki jadwal pemeliharaan peralatan yang dilakukan secara rutin dan konsisten	✓		

A.9.2.5	Pembuangan Atas Penggunaan Kembali Peralatan Dengan Aman			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
10.	LPD memiliki kebijakan yang mencakup bagaimana aset informasi dapat digunakan kembali dimana data dihapus, dan sudah diverifikasi dengan benar	✓		

A.11	Pengendalian Akses			
A.11.1	Persyaratan Proses Bisnis Dalam Pengendalian Akses			
A.11.1.1	Kebijakan Pengendalian Akses			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
1.	LPD memiliki kebijakan pengendalian akses yang terdokumentasi yang didasari kebutuhan bisnis	✓		
A.11.2	Manajemen Pengguna			
A.11.2.1	Pendaftaran Pengguna			
2.	LPD memiliki proses pendaftaran akses pengguna secara formal	✓		
A.11.2.2	Manajemen *Password* Pengguna			
3.	LPD memiliki sistem manajemen *password* pengguna sudah sesuai dengan standar keamanan	✓		

A.11.2.3	Tinjauan Terhadap Hak Akses Pengguna			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
4.	LPD melaksanakan peninjauan secara teratur dan terverifikasi terhadap kepemilikan asset dan hak aksesnya	✓		
A.11.3	Tanggung Jawab Pengguna			
A.11.3.1	Penggunaan *Password* Pengguna			
5.	LPD memiliki sistem password yang tidak mudah diretas	✓		
A.11.3.2	Kebijakan *Clear Desk Dan Clear Screen*			
6.	LPD memiliki kebijakan *Clear Desk Dan Clear Screen*	✓		

A.11.4	Pengendalian Akses Jaringan			
A.11.4.1	Kebijakan Mengenai Penggunaan Layanan Jaringan			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
7	LPD memiliki kebijakan pengguna layanan jaringan	✓		
A.11.4.2	Identifikasi Peralatan Dalam Jaringan			
8.	LPD Melakukan identifikasi peralatan dalam jaringan yang digunakan	✓		
A.11.4.3	Segregasi Dalam jaringan			
9.	LPD memiliki topologi jaringan yang memberlakukan pemisahan jaringan untuk tugas yang berbeda	✓		

A.11.5	Pengendalian Akses Sistem Operasi			
A.11.5.1	Langkah *Log- On* Yang Aman			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
10.	LPD memiliki akses yang dikendalikan oleh prosedur *log-on* yang aman pada aplikasi	✓		
A.11.5.2	Proses Identifikasi dan Otentikasi Pengguna			
11.	LPD memiliki proses identifikasi dan otentikasi pengguna dalam penggunaan aplikasi	✓		
A.11.5.3	Sistem Manajemen *Password*			
12.	LPD memiliki sistem manajemen password	✓		

A.11.5.4	Penggunaan Sistem *Utilities*			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
13.	LPD menggunakan Sistem *Utilities* tambahan	✓		
A.11.5.5	Sesi *Time-Out*			
14.	LPD memiliki sesi *time-out* di dalam proses transaksi di aplikasi	✓		
A.11.5.6	Pembatasan Waktu Koneksi			
15.	LPD memiliki pembatasan waktu koneksi saat aplikasi tidak digunakan	✓		

A.11.6	Pengendalian Akses Aplikasi Dan Informasi			
A.11.6.1	Pembatasan Akses Informasi			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
16.	LPD mempunyai akses ke informasi dan fungsi sistem aplikasi dibatasi sesuai dengan kebijakan kontrol akses	✓		
A.11.6.2	Isolasi sistem yang *sensitive*			
17.	LPD memiliki pengisolasian sistem yang dianggap *sensitive*	✓		

A.11.7	*Mobile Computing* Dan Kerja Jarak Jauh (*Teleworking*)			
A.11.7.1	*Mobile Computing Dan Komunikasi*			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
18.	Aplikasi yang digunakan di LPD menerapkan *mobile computing* dalam penggunaanya	✓		
A.11.7.2	*Kerja Jarak Jauh (TeleWorking)*			
19.	Terdapat kebijakan untuk *teleworking* di LPD Desa Adat Buleleng	✓		
20.	LPD memiliki proses yang ditetapkan untuk pekerja jarak jauh untuk mendapatkan akses serta diberi saran dan peralatan untuk melindungi asset mereka	✓		

A.13	Manajemen Keamanan Informasi			
A.13.1	Melaporkan Insiden Keamanan			
A.13.1.1	Melaporkan Insiden Terhadap Keamanan Informasi			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
1.	LPD mempunyai proses pelaporan kejadian keamanan informasi secara tepat waktu serta terdapat proses untuk meninjau dan bertindak atas peristiwa keamanan informasi yang dilaporkan	✓		
A.13.1.2	Pelaporan Kelemahan Keamanan			
2.	LPD mempunyai proses pelaporan kelemahan keamanan informasi yang teridentifikasi	✓		

No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
3.	LPD memiliki proses pelaporan keamanan yang dikomunikasikan secara luas dan meninjau serta menangani laporan secara tepat waktu	✓		
A.13.2	Manajemen Mengenai Insiden Keamanan Informai Dan Perbaikan			
A.13.2.1	Tanggung Jawab Dan Prosedur			
4.	LPD memiliki tanggung jawab manajemen diidentifikasikan dan didokumentasikan dengan jelas dalam proses manajemen insiden	✓		
A.13.2.2	Pembelajaran Dari Insiden Keamanan Informasi			
5.	LPD memiliki proses atau kerangka kerja yang memungkinkan organisasi untuk belajar dari insiden keamanan informasi dan mengurangi dampak/kemungkinan kejadian di masa depan	✓		

A.13.2.3	Pengumpulan Informasi			
No.	Pernyataan	Relevan	Tidak Relevan	Keterangan
6.	LPD memiliki kebijakan kesiapan forensik jika terjadi insiden keamanan informasi	✓		
No.	Pernyataan			Keterangan
7	LPD memiliki data yang relevan dikumpulkan dengan cara yang memungkinkan untuk digunakan sebagai bukti	✓		

Singaraja, 01 Februari 2023

I MADE ARDWI PRADNYANA, S.T.,M.T
NIP. 198611182015041001

Lampiran 3.Hasil Kuesioner

No: .....

KUESIONER

PENGUKURAN MANAJEMEN RESIKO KEAMANAN INFORMASI MENGGUNAKAN STANDARISASI ISO/IEC 27001 PADA LPD DESA ADATBULELENG

DATA RESPONDEN

Nama : I GUSTI NGR. CANDRAYADHI

Jabatan : KEPALA LPD

PETUNJUK PENGISIAN

1. Isilah identitas diri pada tempat data responden di atas yaitu nama responden dan bidang ahli .
2. Dimohonkan kesediaan Bapak/Ibu untuk menjawab setiap nomor item angket dengan sejujurnya sesuai dengan petunjuk yang ada.
3. Pilihlah jawaban dengan memberikan tanda (V) pada kolom pilihan Bapak/Ibu.
4. **Setiap pertanyaan harus dijawab, dan tidak boleh ada yang kosong.**
5. Tidak ada jawaban yang dianggap salah, benar, baik maupun buruk, karena itu Bapak/Ibu tidak perlu ragu dalam mengisi angket ini.
6. Setelah selesai diisi, mohon angket ini agar segera dikembalikan kepada peneliti.

Keterangan :

1. Skala 0 - *Not Existence*

Perusahaan tidak menyadari pentingnya membuat perencanaan strategis di bidang teknologi informasi. Dalam skala ini penting untuk dilakukan evaluasi pengendalian dan dijadikan sebagai temuan yang penting.

2. Skala 1 - *Initial*

   Perusahaan telah menyadari akan pentingnya pembuatan perencanaan strategis di bidang teknologi informasi. Namun, tidak ada proses yang distandarisasi; perencanaan, perancangan dan manajemen masih belum terorganisir dengan baik. Dalam skala ini keperluan untuk dijadikan temuan tidak diutamakan, karena tingkat kemungkinan terjadinya resiko tidak sebesar skala nol.

3. Skala 2 - *Repeatable*

   Perusahaan telah menetapkan prosedur untuk dipatuhi oleh karyawan, namun belum dikomunikasikan dan belum adanya pemberian latihan formal kepada setiap karyawan mengenai prosedur; dan tanggung jawab diberikan sepenuhnya kepada individu sehingga pemberian kepercayaan sepenuhnya kemungkinan dapat terjadi penyalahgunaan.

4. Skala 3 - *Defined*

   Seluruh proses telah didokumentasikan dan telah dikomunikasikan, serta dilaksanakan berdasarkan metode pengembangan sistem komputerisasi yang baik, namun belum ada proses evaluasi terhadap sistem tersebut, sehingga masih ada kemungkinan terjadinya penyimpangan.

5. Skala 4 - *Managed*

   Proses komputerisasi telah dapat dimonitor dan dievaluasi dengan baik, manajemen proyek pengembangan sistem komputerisasi sudah dijalankan dengan lebih terorganisir.

6. Skala 5 – *Optimised*

Best Practices (pedoman terbaik) telah diikuti dan diotomatisasi pada sistem berdasarkan proses yang terencana, terorganisir dan menggunakan metodologi yang tepat.

Kontrol dalam *ISO/IEC 27001*:

A.5 Information Security Policies (Kebijakan Keamanan Informasi)

Dirancang untuk memastikan bahwa kebijakan ditulis dan diawasi secarakeseluruhan sesuai dengan arahan dari organisasi keamanan informasi.

A.6 Organisation of Information Security (Keamanan Informasi Perusahaan)

mencakup tugas dan tanggung jawab tertentu. *Annex* ini terbagi menjadi dua yaitu:

- A.6.1 yang memastikan bahwa organisasi telah menetapkan kerangka kerja yang dapat menerapkan dan memelihara keamanan informasi secara memadai.

- A.6.2 yang membahas *mobile devices* dan *remote working*. Siapa pun yang bekerja dari rumah atau perjalanan, baik penuh waktu atau paruh waktu, bisa mengikuti aturan yang berlaku.

A.7 Asset Management (Manajemen Aset)

Cara bagaimana organisasi atau perusahaan mengidentifikasi aset informasi danmenentukan tanggung jawab perlindungan sesuai dengan standar yang berlaku

A.8 Human Resource Security (Keamanan Sumber Daya Manusia)

Memastikan bahwa karyawan dan kontraktor memahami hak dan tanggungjawab mereka di perusahaan.

A.9 Physical and Environmental Security (Keamanan Fisik dan Lingkungan)

Membahas keamanan fisik dan lingkungan pada organisasi atau perusahaanyang terbagi menjadi dua, yaitu:

- A.9.1 untuk mencegah akses fisik yang tidak sah, kerusakan atau gangguan ke tempat organisasi atau data yang ada di dalamnya.
- A.9.2 untuk mencegah kehilangan, kerusakan atau pencurian peralatan aset informasi perusahaan baik itu *software* atau *file* fisik.

A.11 Access Control (Kontrol Akses)

Kontrol akses ini bertujuan untuk memastikan bahwa karyawan hanya bisamelihat dan mengelola informasi yang relevan dengan jabatan mereka.

Kontrol akses memiliki empat bagian yaitu persyaratan bisnis dari kontrol akses, manajemen akses pengguna, tanggung jawab pengguna dan kontrol akses pada sistem dan aplikasi.

A.13 Information Security Incident Management (Manajemen Insiden Keamanan Informasi)

Dalam bagian ini membahas bagaimana mengelola dan melaporkan insiden keamanan. Proses ini melibatkan penjelasan karyawan mana saja yang harus bertanggung jawab terhadap tindakan tertentu sehingga penanganannya bisa konsisten dan efektif

A.5	Kebijakan Keamanan								
A.5.1	Kebijakan Terhadap Keamanan Informasi								
A.5.1.1	Dokumen Mengenai Keamanan Informasi								
No.	Pernyataan	0	1	2	3	4	5	Nilai	Keterangan
1.	LPD memiliki dokumen mengenai keamanan informasi				✓				Memiliki dan melakukan kerjasama dengan PT. USSI No : 00102/C/USSI/IX/2020
2.	LPD telah melaksanakan sosialisasi tentang kebijakan keamanan informasi dan telah diterapkan				✓				melakukan sosialisasi kepada seluruh staf yang bekerja
A.5.1.2	Kajian Terhadap Keamanan Informasi								
3.	LPD telah melakukan kajian terhadap Keamanan informasi serta telah mengevaluasi kebijakan keamaman informasi				✓				melakukan kajian dan evaluasi bersama dengan pihak pengembang
4.	LPD telah melakukan pengkajian terhadap keamanan informasi mengikuti perkembangan zaman					✓			Berkoordinasi dengan PT. USSI selaku pengembang
		Tingkat Kemampuan							

A.6	Organisasi Mengenai Keamanan Informasi								
A.6.1	Organisasi Internal								
A.6.1.1	Komitmen Tehadap Keamanan Informasi								
No.	Pernyataan	0	1	2	3	4	5	Nilai	Keterangan
1.	LPD telah memiliki komitmen dalam menerapkan keamanan informasi					✓			melakukan pengecekan / audit tentang keamanan dengan PT UISI
A.6.1.2	Koordinasi Mengenai Keamanan Informasi								
2.	LPD melaksanakan Koordinasi mengenai keamanan Informasi					✓			melakukan koordinasi rutin dengan pihak pengembang
A.6.1.3	Perjanjian Perihal Kerahasiaan								
3.	LPD telah melakukan perjanjian kerjasama perihal kerahasian keamanan informasi dengan BSSN, KOMINFO maupun instansi yang terkait keamanan informasi lainnya				✓				melakukan kerjasama dengan pihak pengembang terkait keamanan No : 00102/[redacted]C/UISI/IX/2020

A.6.1.4	Kontak Terhadap Suatu Kelompok Khusus								
No.	**Pernyataan**	**0**	**1**	**2**	**3**	**4**	**5**	**Nilai**	**Keterangan**
4.	LPD telah melakukan kontak dengan tim yang memahami tentang keamanan informasi seperti BSSN,KOMINFO maupun tim yang terkait keamanan informasi lainnya					✓			melakukan dengan Pihak Penyedia yaitu PT. CISSI
A.6.1.5	**Kajian Yang Independen Terhadap Keamanan Informasi**								
5.	LPD telah melakukan kajian yang independen terhadap keamanan informasi					✓			melakukan dengan pihak pengembang
A.6.2	**Perihal Pihak Eksternal**								
A.6.2.1	**Identifikasi Resiko Dari Pihak Eksternal**								
6.	LPD telah melakukan indentifikasi resiko dari aplikasi yang digunakan dari pihak pengembang					✓			Terdapat di surat service level ~~sama~~ Agreement
A.6.2.2	**Penekanan Keamanan Ketika Menjalin Kontak Dengan Pelanggan**								
7.	LPD telah melakukan penekanan keamanaan pada saat menjalin kontak dengan nasabah					✓			melakukan pemberitahuan tentang hal-hal yang harus dijaga tentang kerahasiaan data rekening

A.6.2.3	Penekanan Perjanjian Terhadap Pihak Ketiga								
No.	**Pernyataan**	**0**	**1**	**2**	**3**	**4**	**5**	**Nilai**	**Keterangan**
8.	Terdapat penekanan keamanan pada saat LPD telah melakukan perjanjian kerjasama dengan pihak pengembang aplikasi terkait tentang penekanan keamanan informasi					✓			melakukan di surat perjanjian dengan PT. UISI
		Tingkat Kemampuan							

A.7	Manajemen Aset								
A.7.1	Tanggung Jawab Terhadap Aset								
A.7.1.1	Inventaris Aset								
No.	Pernyataan	0	1	2	3	4	5	Nilai	Keterangan
1.	LPD miliki inventarisasi semua aset yang berkait dengan informasi dan pemrosesan informasi di LPD					✓			terdapat pada dokumen Inventaris Asset
A.7.1.2	Kepemilikan Aset								
2.	Semua asset LPD tentang informasi memiliki pemilik yang jelas dan menyadari tanggung jawab mereka				✓				memiliki dan terdapat di dokumen kepemilikan Aset
A.7.1.3	Penerapan Aset Yang Telah Masuk								
3.	LPD memiliki kebijakan pengguna yang dapat diterima untuk setiap kelas/jenis aset informasi					✓			memiliki di dokumen kepemilikan asset
A.7.2	Klasifikasi Informasi								
A.7.2.1	Pedoman Klasifikasi								
4.	LPD kebijakan yang mengatur klasifikasi informasi				✓				memiliki di kepemilikan asset

A.7.2.2	Pelabelan Dan Penanganan Informasi								
No.	Pernyataan	0	1	2	3	4	5	Nilai	Keterangan
5.	LPD memiliki prosedur atau proses untuk klasifikasi informasi ditandai dengan tepat pada setiap aset					✓			memiliki prosedur dalam pengklasifikasian
6.	LPD memiliki proses untuk mengurutkan asset secara tepat				✓				memiliki proses dalam pengurutan aset
		Tingkat Kemampuan							

A.8	Keamanan Sumber Daya Manusia								
A.8.1	Sebelum Dipekerjakan								
A.8.1.1	Tanggung Jawab Dan Fungsi								
No.	Pernyataan	0	1	2	3	4	5	Nilai	Keterangan
1.	Terdapat tanggung jawab dan fungsi dari masing – masing staf yang dipekerjakan					✓			Terdapat pada kontrak kerja
A.8.1.2	Penyaringan (*Screening*)								
2.	LPD melakukan verifikasi latar belakang terhadap karyawan baru yang akan dipekerjakan					✓			memeriksa latar belakang karyawan sebelum dipekerjakan
3.	LPD melakukan pemeriksaan sesuai dengan hukum, peraturan, dan etika yang relevan terhadap staf yang akan dipekerjakan					✓			melakukan sesuai peraturan yang ada di LPD
A.8.1.3	Rumusan Syarat Dan Aturan Dalam Kepegawaian								
4.	Semua staf yang bekerja di LPD Desa Adat Buleleng bersedia untuk menandatangani perjanjian kerahasiaan informasi					✓			terdapat pada perjanjian kerja
A.8.2	Selama Bekerja								

A.8.2.1	Tanggung Jawab Manajemen								
No	Pernyataan	0	1	2	3	4	5	Nilai	Keterangan
5.	LPD memberikan penjelasan kepada semua staf dan pengguna pihak ketiga untuk menerapkan keamanan sesuai dengan kebijakan dan prosedur yang ditetapkan					✓			terdapat pada SOP dalam bekerja
A.8.2.2	Proses Pendisiplinan								
6.	LPD memiliki proses pendisiplinan formal yang dapat diterapkan pada staf yang telah melakukan pelanggaran keamanan informasi					✓			memberikan Arahan serta teguran terhadap para Staf
A.8.3	Pengakhiran Dan Perubahan Pekerjaan								
A.8.3.1	Tanggung Jawab Pengakhiran Pekerjaan								
7.	LPD memiliki proses terdokumentasi formal untuk mengakhiri atau mengubah tugas pekerjaan				✓				melakukan setiap adanya perubahan tugas kerja
8.	LPD telah menegakkan kepatuhan dengan tugas pasca kerja				✓				melakukan pelatihan kepada Staf yang bekerja

A.8.3.2	Pengembalian Aset								
No	Pernyataan	0	1	2	3	4	5	Nilai	Keterangan
9.	LPD memiliki proses untuk memastikan semua staf dan pengguna eksternal mengembalikan aset organisasi pada pemutusan hubungan kerja, kontrak, atau perjanjian mereka					✓			melakukannya pada saat pemberhentian staf
A.8.3.3	Penghapusan Hak Akses								
10.	LPD proses untuk memastikan hak akses pengguna dihapus pada pemutusan hubungan kerja atau kontrak, atau disesuaikan dengan perubahan					✓			melakukan sesuai prosedur yang telah dibuat
	Tingkat Kemampuan								

A.9	Keamanan Fisik Dan Lingkungan								
A.9.1	Area Yang Aman								
A.9.1.1	Parameter Keamanan Fisik								
No.	Pernyataan	0	1	2	3	4	5	Nilai	Keterangan
1.	LPD memiliki batasan keamanan informasi yang ditentukan, dan area informasi sensitive atau kritis dipisahkan serta dikontrol dengan tepat					✓			masih belum sesuai dengan arahan pihak pengembang
A.9.1.2	Menjaga Ruangan, Kantor, Atau Fasilias Lainnya								
2.	LPD memiliki ruangan, kantor, atau fasilitas lainnya telah dirancang dan dikonfigurasi dengan mempertimbangkan keamanan informasi				✓				memiliki ruangan yang sudah di desain dengan kebutuhan
A.9.1.3	Penjagaan Terhadap Adanya Ancaman								
3.	LPD memiliki rencana perlindungan maupun pencegahan dari ancaman baik itu ancaman eksternal, maupun internal					✓			sudah dikomunikasikan dengan pihak pengembang
A.9.1.4	Bekerja Di Area Yang Aman								
4.	LPD Desa Adat Buleleng sudah menerapkan prosedur untuk bekerja di daerah yang aman dan sudah diterapkan					✓			sudah menerapkannya pada SOP Pekerjaan

A.9.1.5	Area Akses Publik Dan Bongkar Muat								
No	**Pernyataan**	**0**	**1**	**2**	**3**	**4**	**5**	**Nilai**	**Keterangan**
5.	LPD memiliki akses publik yang terisolasi dari fasilitas pemrosesan informasi					✓			memiliki pembatas dengan area public
A.9.2	**Keamanan Peralatan**								
A.9.2.1	**Penempatan Dan Perlindungan Peralatan**								
6.	LPD telah melakukan identifikasi bahaya lingkungan yang diidentifikasi dan dipertimbangkan ketika pemilihan lokasi peralatan					✓			melalcukannya dengan pihak pengembang
A.9.2.2	**Sarana Pendukung**								
7	LPD memiliki UPS atau generator cadangan dan telah diuji dalam skala waktu yang sesuai					✓			memiliki dengan durasi 1 jam
A.9.2.3	**Keamanan Kabel**								
8.	LPD memiliki penilaian risiko yang telah dilakukan di lokasi kabel listrik dan telekomunikasi					✓			memiliki dan sudah di rancang

A.9.2.4	Pemeliharaan Peralatan								
No	Pernyataan	0	1	2	3	4	5	Nilai	Keterangan
9.	LPD memilki jadwal pemeliharaan peralatan yang dilakukan secara rutin dan konsisten					✓			memiliki jadwal pemeliharaan setiap 6 bulan sekali
A.9.2.5	Pembuangan Atas Penggunaan Kembali Peralatan Dengan Aman								
10.	LPD memiliki kebijakan yang mencakup bagaimana aset informasi dapat digunakan kembali dimana data dihapus, dan sudah diverifikasi dengan benar					✓			Sudah menerapkan
		Tingkat Kemampuan							

A.11	Pengendalian Akses								
A.11.1	Persyaratan Proses Bisnis Dalam Pengendalian Akses								
A.11.1.1	Kebijakan Pengendalian Akses								
No.	Pernyataan	0	1	2	3	4	5	Nilai	Keterangan
1.	LPD memiliki kebijakan pengendalian akses yang terdokumentasi yang didasari kebutuhan bisnis				✓				memiliki dan dikoordinasikan dengan pihak pengembang
A.11.2	Manajemen Pengguna								
A.11.2.1	Pendaftaran Pengguna								
2.	LPD memiliki proses pendaftaran akses pengguna secara formal				✓				melalui lam perjanjian pada saat pendaftaran sesuai SOP
A.11.2.2	Manajemen *Password* Pengguna								
3.	LPD memiliki sistem manajemen *password* pengguna sudah sesuai dengan standar keamanan					✓			sudah di koordinasikan dengan pihak pengembang aplikasi
A.11.2.3	Tinjauan Terhadap Hak Akses Pengguna								
4.	LPD melaksanakan peninjauan secara teratur dan terverifikasi terhadap kepemilikan asset dan hak aksesnya				✓				melalui lam peninjauan dengan SOP yang berlaku

A.11.3	Tanggung Jawab Pengguna								
A.11.3.1	Penggunaan *Password* Pengguna								
No.	Pernyataan	0	1	2	3	4	5	Nilai	Keterangan
5.	LPD memiliki sistem password yang tidak mudah diretas					✓			memiliki dan sudah di koordinasikan dengan pihak pengembang
A.11.3.2	Kebijakan *Clear Desk Dan Clear Screen*								
6.	LPD memiliki kebijakan *Clear Desk Dan Clear Screen*				✓				melaksanakannya sesuai SOP
A.11.4	Pengendalian Akses Jaringan								
A.11.4.1	Kebijakan Mengenai Penggunaan Layanan Jaringan								
7	LPD memiliki kebijakan pengguna layanan jaringan				✓				melakukan dengan pihak pengembang
A.11.4.2	Identifikasi Peralatan Dalam Jaringan								
8.	LPD Melakukan identifikasi peralatan dalam jaringan yang digunakan				✓				melakukan dengan pihak pengembang

A.11.4.3	Segregasi Dalam jaringan								
No.	**Pernyataan**	**0**	**1**	**2**	**3**	**4**	**5**	**Nilai**	**Keterangan**
9.	LPD memiliki topologi jaringan yang memberlakukan pemisahan jaringan untuk tugas yang berbeda				✓				melalcukan dan sesuai dari pihak pengembang
A.11.5	**Pengendalian Akses Sistem Operasi**								
A.11.5.1	**Langkah *Log- On* Yang Aman**								
10.	LPD memiliki akses yang dikendalikan oleh prosedur *log-on* yang aman pada aplikasi				✓				melalcukan dengan pihak pengembang Aplikasi
A.11.5.2	**Proses Identifikasi dan Otentikasi Pengguna**								
11.	LPD memiliki proses identifikasi dan otentikasi pengguna dalam penggunaan aplikasi					✓			melakukan dengan pihak Pengembang
A.11.5.3	**Sistem Manajemen *Password***								
12.	LPD memiliki sistem manajemen password					✓			memiliki sesuai saran pihak pengembang

A.11.5.4	Penggunaan Sistem *Utilities*								
No.	**Pernyataan**	**0**	**1**	**2**	**3**	**4**	**5**	**Nilai**	**Keterangan**
13.	LPD menggunakan Sistem *Utilities* tambahan				✓				menggunakan Anti.virus yang selalu diupdate
A.11.5.5	**Sesi *Time-Out***								
14.	LPD memiliki sesi *time-out* di dalam proses transaksi di aplikasi					✓			memiliki setiap 1 jam
A.11.5.6	**Pembatasan Waktu Koneksi**								
15.	LPD memiliki pembatasan waktu koneksi saat aplikasi tidak digunakan					✓			memiliki setiap 5 menit
A.11.6	**Pengendalian Akses Aplikasi Dan Informasi**								
A.11.6.1	**Pembatasan Akses Informasi**								
16.	LPD mempunyai akses ke informasi dan fungsi sistem aplikasi dibatasi sesuai dengan kebijakan kontrol akses					✓			memiliki dan sudah diatur oleh pihak pengembang

A.11.6.2	Isolasi sistem yang *sensitive*								
No.	**Pernyataan**	**0**	**1**	**2**	**3**	**4**	**5**	**Nilai**	**Keterangan**
17.	LPD memiliki pengisolasian sistem yang dianggap *sensitive*					✓			memiliki dan sudah diatur
A.11.7	***Mobile Computing* Dan Kerja Jarak Jauh (*Teleworking*)**								
A.11.7.1	***Mobile Computing Dan Komunikasi***								
18.	Aplikasi yang digunakan di LPD menerapkan *mobile computing* dalam penggunaanya					✓			memiliki perangkat mobile
A.11.7.2	***Kerja Jarak Jauh (TeleWorking)***								
19.	Terdapat kebijakan untuk *teleworking* di LPD Desa Adat Buleleng					✓			memiliki sesuai dengan standar
20.	LPD memiliki proses yang ditetapkan untuk pekerja jarak jauh untuk mendapatkan akses serta diberi saran dan peralatan untuk melindungi asset mereka					✓			memiliki sesuai standar SOP
	Tingkat Kemampuan								

A.13	Manajemen Keamanan Informasi								
A.13.1	Melaporkan Insiden Keamanan								
A.13.1.1	Melaporkan Insiden Terhadap Keamanan Informasi								
No.	Pernyataan	0	1	2	3	4	5	Nilai	Keterangan
1.	LPD mempunyai proses pelaporan kejadian keamanan informasi secara tepat waktu serta terdapat proses untuk meninjau dan bertindak atas peristiwa keamanan informasi yang dilaporkan					✓			memiliki proses pelaporan sesuai standar SOP
A.13.1.2	Pelaporan Kelemahan Keamanan								
2.	LPD mempunyai proses pelaporan kelemahan keamanan informasi yang teridentifikasi				✓				memiliki dan sudah dikoordinasikan dengan pihak pengembang

No.	Pernyataan	0	1	2	3	4	5	Nilai	Keterangan
3.	LPD memiliki proses pelaporan keamanan yang dikomunikasikan secara luas dan meninjau serta menangani laporan secara tepat waktu					✓			memiliki serta ditinjau dengan pihak pengembang
A.13.2	**Manajemen Mengenai Insiden Keamanan Informai Dan Perbaikan**								
A.13.2.1	**Tanggung Jawab Dan Prosedur**								
4.	LPD memiliki tanggung jawab manajemen diidentifikasikan dan didokumentasikan dengan jelas dalam proses manajemen insiden				✓				memiliki dan sudah di dokumentasikan
A.13.2.2	**Pembelajaran Dari Insiden Keamanan Informasi**								
5.	LPD memiliki proses atau kerangka kerja yang memungkinkan organisasi untuk belajar dari insiden keamanan informasi dan mengurangi dampak/kemungkinan				✓				memiliki sesuai arahan pihak pengembang

A.13.2.3	Pengumpulan Informasi								
No.	Pernyataan	0	1	2	3	4	5	Nilai	Keterangan
6.	LPD memiliki kebijakan kesiapan forensik jika terjadi insiden keamanan informasi				✓				memiliki sesuai standar SOP
7	LPD memiliki data yang relevan dikumpulkan dengan cara yang memungkinkan untuk digunakan sebagai bukti					✓			memiliki dan didokumentasi kan setiap ada permasalahan
		Tingkat Kemampuan							

Singaraja, 6 FEBRUARI 2023

I G.N. CANDRAYADHI

No: .....

KUESIONER

PENGUKURAN MANAJEMEN RESIKO KEAMANAN INFORMASI MENGGUNAKAN STANDARISASI ISO/IEC 27001 PADA LPD DESA ADATBULELENG

DATA RESPONDEN

Nama : Jonny

Jabatan : Bendahara

PETUNJUK PENGISIAN

1. Isilah identitas diri pada tempat data responden di atas yaitu nama responden dan bidang ahli .
2. Dimohonkan kesediaan Bapak/Ibu untuk menjawab setiap nomor item angket dengan sejujurnya sesuai dengan petunjuk yang ada.
3. Pilihlah jawaban dengan memberikan tanda (V) pada kolom pilihan Bapak/Ibu.
4. **Setiap pertanyaan harus dijawab, dan tidak boleh ada yang kosong.**
5. Tidak ada jawaban yang dianggap salah, benar, baik maupun buruk, karena itu Bapak/Ibu tidak perlu ragu dalam mengisi angket ini.
6. Setelah selesai diisi, mohon angket ini agar segera dikembalikan kepada peneliti.

Keterangan :

1. Skala 0 - *Not Existence*

Perusahaan tidak menyadari pentingnya membuat perencanaan strategis di bidang teknologi informasi. Dalam skala ini penting untuk dilakukan evaluasi pengendalian dan dijadikan sebagai temuan yang penting.

2. Skala 1 - *Initial*

Perusahaan telah menyadari akan pentingnya pembuatan perencanaan strategis di bidang teknologi informasi. Namun, tidak ada proses yang distandarisasi; perencanaan, perancangan dan manajemen masih belum terorganisir dengan baik. Dalam skala ini keperluan untuk dijadikan temuan tidak diutamakan, karena tingkat kemungkinan terjadinya resiko tidak sebesar skala nol.

3. Skala 2 - *Repeatable*

Perusahaan telah menetapkan prosedur untuk dipatuhi oleh karyawan, namun belum dikomunikasikan dan belum adanya pemberian latihan formal kepada setiap karyawan mengenai prosedur; dan tanggung jawab diberikan sepenuhnya kepada individu sehingga pemberian kepercayaan sepenuhnya kemungkinan dapat terjadi penyalahgunaan.

4. Skala 3 - *Defined*

Seluruh proses telah didokumentasikan dan telah dikomunikasikan, serta dilaksanakan berdasarkan metode pengembangan sistem komputerisasi yang baik, namun belum ada proses evaluasi terhadap sistem tersebut, sehingga masih ada kemungkinan terjadinya penyimpangan.

5. Skala 4 - *Managed*

Proses komputerisasi telah dapat dimonitor dan dievaluasi dengan baik, manajemen proyek pengembangan sistem komputerisasi sudah dijalankan dengan lebih terorganisir.

6. Skala 5 – *Optimised*

Best Practices (pedoman terbaik) telah diikuti dan diotomatisasi pada sistem berdasarkan proses yang terencana, terorganisir dan menggunakan metodologi yang tepat.

Kontrol dalam *ISO/IEC 27001*:

A.5 Information Security Policies (Kebijakan Keamanan Informasi)

Dirancang untuk memastikan bahwa kebijakan ditulis dan diawasi secarakeseluruhan sesuai dengan arahan dari organisasi keamanan informasi.

A.6 Organisation of Information Security (Keamanan Informasi Perusahaan)

mencakup tugas dan tanggung jawab tertentu. *Annex* ini terbagi menjadi dua yaitu:

- A.6.1 yang memastikan bahwa organisasi telah menetapkan kerangka kerja yang dapat menerapkan dan memelihara keamanan informasi secara memadai.

- A.6.2 yang membahas *mobile devices* dan *remote working*. Siapa pun yang bekerja dari rumah atau perjalanan, baik penuh waktu atau paruh waktu, bisa mengikuti aturan yang berlaku.

A.7 Asset Management (Manajemen Aset)

Cara bagaimana organisasi atau perusahaan mengidentifikasi aset informasi danmenentukan tanggung jawab perlindungan sesuai dengan standar yang berlaku

A.8 Human Resource Security (Keamanan Sumber Daya Manusia)

Memastikan bahwa karyawan dan kontraktor memahami hak dan tanggungjawab mereka di perusahaan.

A.9 Physical and Environmental Security (Keamanan Fisik dan Lingkungan)

Membahas keamanan fisik dan lingkungan pada organisasi atau perusahaanyang terbagi menjadi dua, yaitu:

- A.9.1 untuk mencegah akses fisik yang tidak sah, kerusakan atau gangguan ke tempat organisasi atau data yang ada di dalamnya.
- A.9.2 untuk mencegah kehilangan, kerusakan atau pencurian peralatan aset informasi perusahaan baik itu *software* atau *file* fisik.

A.11 Access Control (Kontrol Akses)

Kontrol akses ini bertujuan untuk memastikan bahwa karyawan hanya bisamelihat dan mengelola informasi yang relevan dengan jabatan mereka.

Kontrol akses memiliki empat bagian yaitu persyaratan bisnis dari kontrol akses, manajemen akses pengguna, tanggung jawab pengguna dan kontrol akses pada sistem dan aplikasi.

A.13 Information Security Incident Management (Manajemen Insiden Keamanan Informasi)

Dalam bagian ini membahas bagaimana mengelola dan melaporkan insiden keamanan. Proses ini melibatkan penjelasan karyawan mana saja yang harus bertanggung jawab terhadap tindakan tertentu sehingga penanganannya bisa konsisten dan efektif

A.5	Kebijakan Keamanan								
A.5.1	Kebijakan Terhadap Keamanan Informasi								
A.5.1.1	Dokumen Mengenai Keamanan Informasi								
No.	Pernyataan	0	1	2	3	4	5	Nilai	Keterangan
1.	LPD memiliki dokumen mengenai keamanan informasi				✓				
2.	LPD telah melaksanakan sosialisasi tentang kebijakan keamanan informasi dan telah diterapkan				✓				
A.5.1.2	Kajian Terhadap Keamanan Informasi								
3.	LPD telah melakukan kajian terhadap Keamanan informasi serta telah mengevaluasi kebijakan keamaman informasi			✓					
4.	LPD telah melakukan pengkajian terhadap keamanan informasi mengikuti perkembangan zaman				✓				
	Tingkat Kemampuan								

A.6	Organisasi Mengenai Keamanan Informasi								
A.6.1	Organisasi Internal								
A.6.1.1	Komitmen Tehadap Keamanan Informasi								
No.	Pernyataan	0	1	2	3	4	5	Nilai	Keterangan
1.	LPD telah memiliki komitmen dalam menerapkan keamanan informasi			✓					
A.6.1.2	Koordinasi Mengenai Keamanan Informasi								
2.	LPD melaksanakan Koordinasi mengenai keamanan Informasi			✓					
A.6.1.3	Perjanjian Perihal Kerahasiaan								
3.	LPD telah melakukan perjanjian kerjasama perihal kerahasian keamanan informasi dengan BSSN, KOMINFO maupun instansi yang terkait keamanan informasi lainnya			✓					

A.6.1.4	Kontak Terhadap Suatu Kelompok Khusus								
No.	**Pernyataan**	**0**	**1**	**2**	**3**	**4**	**5**	**Nilai**	**Keterangan**
4.	LPD telah melakukan kontak dengan tim yang memahami tentang keamanan informasi seperti BSSN,KOMINFO maupun tim yang terkait keamanan informasi lainnya			✓					
A.6.1.5	**Kajian Yang Independen Terhadap Keamanan Informasi**								
5.	LPD telah melakukan kajian yang independen terhadap keamanan informasi			✓					
A.6.2	**Perihal Pihak Eksternal**								
A.6.2.1	**Identifikasi Resiko Dari Pihak Eksternal**								
6.	LPD telah melakukan indentifikasi resiko dari aplikasi yang digunakan dari pihak pengembang			✓					
A.6.2.2	**Penekanan Keamanan Ketika Menjalin Kontak Dengan Pelanggan**								
7.	LPD telah melakukan penekanan keamanaan pada saat menjalin kontak dengan nasabah			✓					

A.6.2.3	Penekanan Perjanjian Terhadap Pihak Ketiga								
No.	**Pernyataan**	**0**	**1**	**2**	**3**	**4**	**5**	**Nilai**	**Keterangan**
8.	Terdapat penekanan keamanan pada saat LPD telah melakukan perjanjian kerjasama dengan pihak pengembang aplikasi terkait tentang penekanan keamanan informasi			✓					
		Tingkat Kemampuan							

A.7	Manajemen Aset								
A.7.1	Tanggung Jawab Terhadap Aset								
A.7.1.1	Inventaris Aset								
No.	Pernyataan	0	1	2	3	4	5	Nilai	Keterangan
1.	LPD miliki inventarisasi semua aset yang berkait dengan informasi dan pemrosesan informasi di LPD			✓					
A.7.1.2	Kepemilikan Aset								
2.	Semua asset LPD tentang informasi memiliki pemilik yang jelas dan menyadari tanggung jawab mereka			✓					
A.7.1.3	Penerapan Aset Yang Telah Masuk								
3.	LPD memiliki kebijakan pengguna yang dapat diterima untuk setiap kelas/jenis aset informasi		✓						
A.7.2	Klasifikasi Informasi								
A.7.2.1	Pedoman Klasifikasi								
4.	LPD kebijakan yang mengatur klasifikasi informasi			✓					

A.7.2.2	Pelabelan Dan Penanganan Informasi								
No.	Pernyataan	0	1	2	3	4	5	Nilai	Keterangan
5.	LPD memiliki prosedur atau proses untuk klasifikasi informasi ditandai dengan tepat pada setiap aset		v						
6.	LPD memiliki proses untuk mengurutkan asset secara tepat		✓						
		Tingkat Kemampuan							

A.8	Keamanan Sumber Daya Manusia								
A.8.1	Sebelum Dipekerjakan								
A.8.1.1	Tanggung Jawab Dan Fungsi								
No.	Pernyataan	0	1	2	3	4	5	Nilai	Keterangan
1.	Terdapat tanggung jawab dan fungsi dari masing – masing staf yang dipekerjakan				✓				
A.8.1.2	Penyaringan (*Screening*)								
2.	LPD melakukan verifikasi latar belakang terhadap karyawan baru yang akan dipekerjakan				✓				
3.	LPD melakukan pemeriksaan sesuai dengan hukum, peraturan, dan etika yang relevan terhadap staf yang akan dipekerjakan			✓					
A.8.1.3	Rumusan Syarat Dan Aturan Dalam Kepegawaian								
4.	Semua staf yang bekerja di LPD Desa Adat Buleleng bersedia untuk menandatangani perjanjian kerahasiaan informasi				✓				
A.8.2	Selama Bekerja								

A.8.2.1	Tanggung Jawab Manajemen								
No	**Pernyataan**	**0**	**1**	**2**	**3**	**4**	**5**	**Nilai**	**Keterangan**
5.	LPD memberikan penjelasan kepada semua staf dan pengguna pihak ketiga untuk menerapkan keamanan sesuai dengan kebijakan dan prosedur yang ditetapkan			✓					
A.8.2.2	**Proses Pendisiplinan**								
6.	LPD memiliki proses pendisiplinan formal yang dapat diterapkan pada staf yang telah melakukan pelanggaran keamanan informasi			✓					
A.8.3	**Pengakhiran Dan Perubahan Pekerjaan**								
A.8.3.1	**Tanggung Jawab Pengakhiran Pekerjaan**								
7.	LPD memiliki proses terdokumentasi formal untuk mengakhiri atau mengubah tugas pekerjaan			✓					
8.	LPD telah menegakkan kepatuhan dengan tugas pasca kerja			✓					

A.8.3.2	Pengembalian Aset								
No	Pernyataan	0	1	2	3	4	5	Nilai	Keterangan
9.	LPD memiliki proses untuk memastikan semua staf dan pengguna eksternal mengembalikan aset organisasi pada pemutusan hubungan kerja, kontrak, atau perjanjian mereka			✓					
A.8.3.3	Penghapusan Hak Akses								
10.	LPD proses untuk memastikan hak akses pengguna dihapus pada pemutusan hubungan kerja atau kontrak, atau disesuaikan dengan perubahan			✓					
	Tingkat Kemampuan								

A.9	Keamanan Fisik Dan Lingkungan								
A.9.1	Area Yang Aman								
A.9.1.1	Parameter Keamanan Fisik								
No.	Pernyataan	0	1	2	3	4	5	Nilai	Keterangan
1.	LPD memiliki batasan keamanan informasi yang ditentukan, dan area informasi sensitive atau kritis dipisahkan serta dikontrol dengan tepat			✓					
A.9.1.2	Menjaga Ruangan, Kantor, Atau Fasilias Lainnya								
2.	LPD memiliki ruangan, kantor, atau fasilitas lainnya telah dirancang dan dikonfigurasi dengan mempertimbangkan keamanan informasi		✓						
A.9.1.3	Penjagaan Terhadap Adanya Ancaman								
3.	LPD memiliki rencana perlindungan maupun pencegahan dari ancaman baik itu ancaman eksternal, maupun internal			✓					
A.9.1.4	Bekerja Di Area Yang Aman								
4.	LPD Desa Adat Buleleng sudah menerapkan prosedur untuk bekerja di daerah yang aman dan sudah diterapkan		✓						

A.9.1.5	Area Akses Publik Dan Bongkar Muat								
No	**Pernyataan**	**0**	**1**	**2**	**3**	**4**	**5**	**Nilai**	**Keterangan**
5.	LPD memiliki akses publik yang terisolasi dari fasilitas pemrosesan informasi		✓						
A.9.2	**Keamanan Peralatan**								
A.9.2.1	**Penempatan Dan Perlindungan Peralatan**								
6.	LPD telah melakukan identifikasi bahaya lingkungan yang diidentifikasi dan dipertimbangkan ketika pemilihan lokasi peralatan			✓					
A.9.2.2	**Sarana Pendukung**								
7	LPD memiliki UPS atau generator cadangan dan telah diuji dalam skala waktu yang sesuai			✓					
A.9.2.3	**Keamanan Kabel**								
8.	LPD memiliki penilaian risiko yang telah dilakukan di lokasi kabel listrik dan telekomunikasi			✓					

A.9.2.4	Pemeliharaan Peralatan								
No	**Pernyataan**	**0**	**1**	**2**	**3**	**4**	**5**	**Nilai**	**Keterangan**
9.	LPD memilki jadwal pemeliharaan peralatan yang dilakukan secara rutin dan konsisten			✓					
A.9.2.5	**Pembuangan Atas Penggunaan Kembali Peralatan Dengan Aman**								
10.	LPD memiliki kebijakan yang mencakup bagaimana aset informasi dapat digunakan kembali dimana data dihapus, dan sudah diverifikasi dengan benar			✓					
	Tingkat Kemampuan								

A.11	Pengendalian Akses								
A.11.1	Persyaratan Proses Bisnis Dalam Pengendalian Akses								
A.11.1.1	Kebijakan Pengendalian Akses								
No.	Pernyataan	0	1	2	3	4	5	Nilai	Keterangan
1.	LPD memiliki kebijakan pengendalian akses yang terdokumentasi yang didasari kebutuhan bisnis			✓					
A.11.2	Manajemen Pengguna								
A.11.2.1	Pendaftaran Pengguna								
2.	LPD memiliki proses pendaftaran akses pengguna secara formal			✓					
A.11.2.2	Manajemen *Password* Pengguna								
3.	LPD memiliki sistem manajemen *password* pengguna sudah sesuai dengan standar keamanan			✓					
A.11.2.3	Tinjauan Terhadap Hak Akses Pengguna								
4.	LPD melaksanakan peninjauan secara teratur dan terverifikasi terhadap kepemilikan asset dan hak aksesnya			✓					

A.11.3	Tanggung Jawab Pengguna								
A.11.3.1	Penggunaan *Password* Pengguna								
No.	Pernyataan	0	1	2	3	4	5	Nilai	Keterangan
5.	LPD memiliki sistem password yang tidak mudah diretas			✓					
A.11.3.2	Kebijakan *Clear Desk Dan Clear Screen*								
6.	LPD memiliki kebijakan *Clear Desk Dan Clear Screen*			✓					
A.11.4	Pengendalian Akses Jaringan								
A.11.4.1	Kebijakan Mengenai Penggunaan Layanan Jaringan								
7	LPD memiliki kebijakan pengguna layanan jaringan			✓					
A.11.4.2	Identifikasi Peralatan Dalam Jaringan								
8.	LPD Melakukan identifikasi peralatan dalam jaringan yang digunakan			✓					

A.11.4.3	Segregasi Dalam jaringan								
No.	**Pernyataan**	**0**	**1**	**2**	**3**	**4**	**5**	**Nilai**	**Keterangan**
9.	LPD memiliki topologi jaringan yang memberlakukan pemisahan jaringan untuk tugas yang berbeda			✓					
A.11.5	**Pengendalian Akses Sistem Operasi**								
A.11.5.1	**Langkah *Log- On* Yang Aman**								
10.	LPD memiliki akses yang dikendalikan oleh prosedur *log-on* yang aman pada aplikasi			✓					
A.11.5.2	**Proses Identifikasi dan Otentikasi Pengguna**								
11.	LPD memiliki proses identifikasi dan otentikasi pengguna dalam penggunaan aplikasi			✓					
A.11.5.3	**Sistem Manajemen *Password***								
12.	LPD memiliki sistem manajemen password				✓				

A.11.5.4	Penggunaan Sistem *Utilities*								
No.	**Pernyataan**	**0**	**1**	**2**	**3**	**4**	**5**	**Nilai**	**Keterangan**
13.	LPD menggunakan Sistem *Utilities* tambahan			✓					
A.11.5.5	**Sesi *Time-Out***								
14.	LPD memiliki sesi *time-out* di dalam proses transaksi di aplikasi			✓					
A.11.5.6	**Pembatasan Waktu Koneksi**								
15.	LPD memiliki pembatasan waktu koneksi saat aplikasi tidak digunakan			✓					
A.11.6	**Pengendalian Akses Aplikasi Dan Informasi**								
A.11.6.1	**Pembatasan Akses Informasi**								
16.	LPD mempunyai akses ke informasi dan fungsi sistem aplikasi dibatasi sesuai dengan kebijakan kontrol akses			✓					

A.11.6.2	Isolasi sistem yang *sensitive*								
No.	**Pernyataan**	**0**	**1**	**2**	**3**	**4**	**5**	**Nilai**	**Keterangan**
17.	LPD memiliki pengisolasian sistem yang dianggap *sensitive*			✓					
A.11.7	***Mobile Computing* Dan Kerja Jarak Jauh (*Teleworking*)**								
A.11.7.1	***Mobile Computing Dan Komunikasi***								
18.	Aplikasi yang digunakan di LPD menerapkan *mobile computing* dalam penggunaanya			✓					
A.11.7.2	***Kerja Jarak Jauh (TeleWorking)***								
19.	Terdapat kebijakan untuk *teleworking* di LPD Desa Adat Buleleng			✓					
20.	LPD memiliki proses yang ditetapkan untuk pekerja jarak jauh untuk mendapatkan akses serta diberi saran dan peralatan untuk melindungi asset mereka		✓						
		Tingkat Kemampuan							

A.13	Manajemen Keamanan Informasi								
A.13.1	Melaporkan Insiden Keamanan								
A.13.1.1	Melaporkan Insiden Terhadap Keamanan Informasi								
No.	Pernyataan	0	1	2	3	4	5	Nilai	Keterangan
1.	LPD mempunyai proses pelaporan kejadian keamanan informasi secara tepat waktu serta terdapat proses untuk meninjau dan bertindak atas peristiwa keamanan informasi yang dilaporkan			✓					
A.13.1.2	Pelaporan Kelemahan Keamanan								
2.	LPD mempunyai proses pelaporan kelemahan keamanan informasi yang teridentifikasi			√					

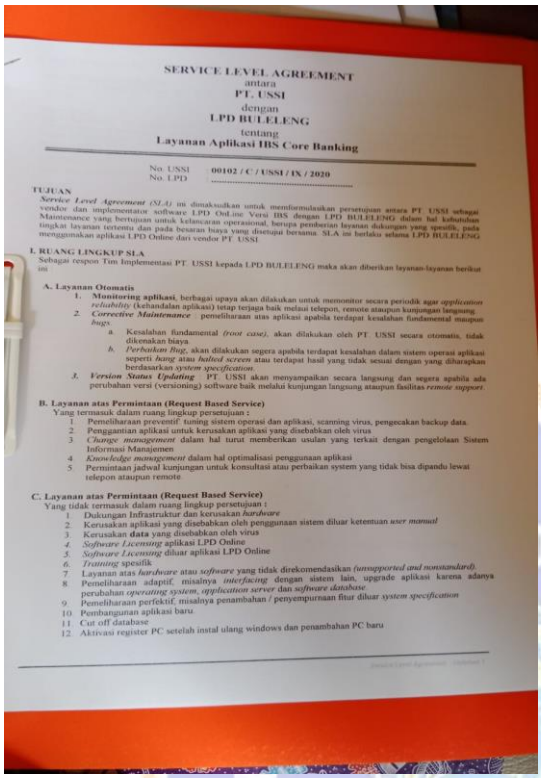
No.	Pernyataan	0	1	2	3	4	5	Nilai	Keterangan
3.	LPD memiliki proses pelaporan keamanan yang dikomunikasikan secara luas dan meninjau serta menangani laporan secara tepat waktu			✓					
A.13.2	**Manajemen Mengenai Insiden Keamanan Informai Dan Perbaikan**								
A.13.2.1	**Tanggung Jawab Dan Prosedur**								
4.	LPD memiliki tanggung jawab manajemen diidentifikasikan dan didokumentasikan dengan jelas dalam proses manajemen insiden			✓					
A.13.2.2	**Pembelajaran Dari Insiden Keamanan Informasi**								
5.	LPD memiliki proses atau kerangka kerja yang memungkinkan organisasi untuk belajar dari insiden keamanan informasi dan mengurangi dampak/kemungkinan			✓					

A.13.2.3	Pengumpulan Informasi								
No.	Pernyataan	0	1	2	3	4	5	Nilai	Keterangan
6.	LPD memiliki kebijakan kesiapan forensik jika terjadi insiden keamanan informasi			✓					
7	LPD memiliki data yang relevan dikumpulkan dengan cara yang memungkinkan untuk digunakan sebagai bukti			✓					
		Tingkat Kemampuan							

Singaraja, 06 FEBRUARI 2023

Jawy

Lampiran 3 Hasil temuan



SERVICE LEVEL AGREEMENT
antara
PT. USSI
dengan
LPD BULELENG
tentang
Layanan Aplikasi IBS Core Banking

No. USSI : 00102 / C / USSI / IX / 2020
No. LPD : .....

TUJUAN

Service Level Agreement (SLA) ini dimaksudkan untuk merumuskan persetujuan antara PT. USSI sebagai vendor dan implementator software LPD OnLine Versi IBS dengan LPD BULELENG dalam hal kebutuhan Maintenance yang bertujuan untuk kelancaran operasional, berupa pemberian layanan dukungan yang spesifik, pada tingkat layanan tertentu dan pada besaran biaya yang disetujui bersama. SLA ini berlaku selama LPD BULELENG menggunakan aplikasi LPD Online dari vendor PT. USSI.

I. RUANG LINGKUP SLA

Sebagai respon Tim Implementasi PT. USSI kepada LPD BULELENG maka akan diberikan layanan-layanan berikut ini

A. Layanan Otomatis

1. **Monitoring aplikasi**, berbagai upaya akan dilakukan untuk memonitor secara periodik agar *application reliability* (kehandalan aplikasi) tetap terjaga baik melaui telepon, remote ataupun kunjungan langsung.
2. ***Corrective Maintenance*** : pemeliharaan atas aplikasi apabila terdapat kesalahan fundamental maupun *bugs*.
   a. Kesalahan fundamental *(root case)*, akan dilakukan oleh PT. USSI secara otomatis, tidak dikenakan biaya.
   b. *Perbaikan Bug*, akan dilakukan segera apabila terdapat kesalahan dalam sistem operasi aplikasi seperti *hang* atau *halted screen* atau terdapat hasil yang tidak sesuai dengan yang diharapkan berdasarkan *system specification*.
3. ***Version Status Updating*** : PT. USSI akan menyampaikan secara langsung dan segera apabila ada perubahan versi (versioning) software baik melalui kunjungan langsung ataupun fasilitas *remote support*.

B. Layanan atas Permintaan (Request Based Service)

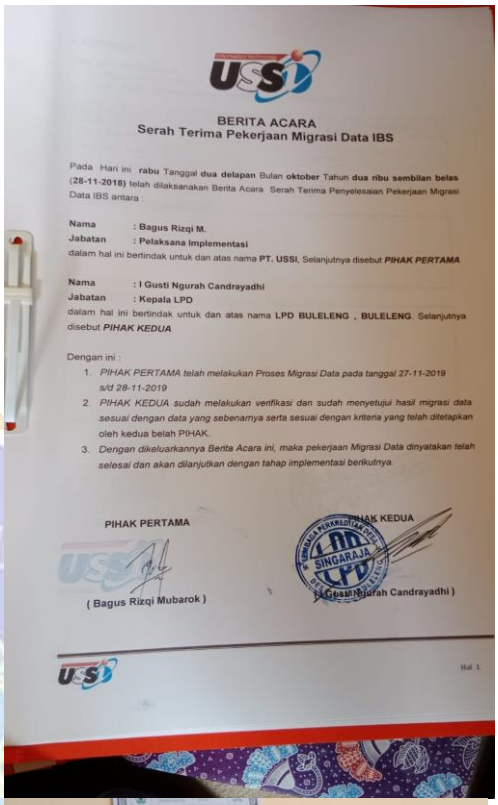
Yang termasuk dalam ruang lingkup persetujuan :

1. Pemeliharaan preventif: tuning sistem operasi dan aplikasi, scanning virus, pengecakan backup data.
2. Penggantian aplikasi untuk kerusakan aplikasi yang disebabkan oleh virus
3. *Change management* dalam hal turut memberikan usulan yang terkait dengan pengelolaan Sistem Informasi Manajemen
4. *Knowledge management* dalam hal optimalisasi penggunaan aplikasi
5. Permintaan jadwal kunjungan untuk konsultasi atau perbaikan system yang tidak bisa dipandu lewat telepon ataupun remote.

C. Layanan atas Permintaan (Request Based Service)

Yang tidak termasuk dalam ruang lingkup persetujuan :

1. Dukungan Infrastruktur dan kerusakan *hardware*
2. Kerusakan aplikasi yang disebabkan oleh penggunaan sistem diluar ketentuan *user manual*
3. Kerusakan **data** yang disebabkan oleh virus
4. *Software Licensing* aplikasi LPD Online
5. *Software Licensing* diluar aplikasi LPD Online
6. *Training* spesifik
7. Layanan atas *hardware* atau *software* yang tidak direkomendasikan *(unsupported and nonstandard)*.
8. Pemeliharaan adaptif, misalnya *interfacing* dengan sistem lain, upgrade aplikasi karena adanya perubahan *operating system, application server* dan *software database*.
9. Pemeliharaan perfektif, misalnya penambahan / penyempurnaan fitur diluar *system specification*
10. Pembangunan aplikasi baru.
11. Cut off database
12. Aktivasi register PC setelah instal ulang windows dan penambahan PC baru



USSI

BERITA ACARA
Serah Terima Pekerjaan Migrasi Data IBS

Pada Hari ini **rabu** Tanggal **dua delapan** Bulan **oktober** Tahun **dua ribu sembilan belas (28-11-2018)** telah dilaksanakan Berita Acara Serah Terima Penyelesaian Pekerjaan Migrasi Data IBS antara :

Nama : **Bagus Rizqi M.**
Jabatan : **Pelaksana Implementasi**
dalam hal ini bertindak untuk dan atas nama **PT. USSI**, Selanjutnya disebut ***PIHAK PERTAMA***

Nama : **I Gusti Ngurah Candrayadhi**
Jabatan : **Kepala LPD**
dalam hal ini bertindak untuk dan atas nama **LPD BULELENG , BULELENG**. Selanjutnya disebut ***PIHAK KEDUA***

Dengan ini :

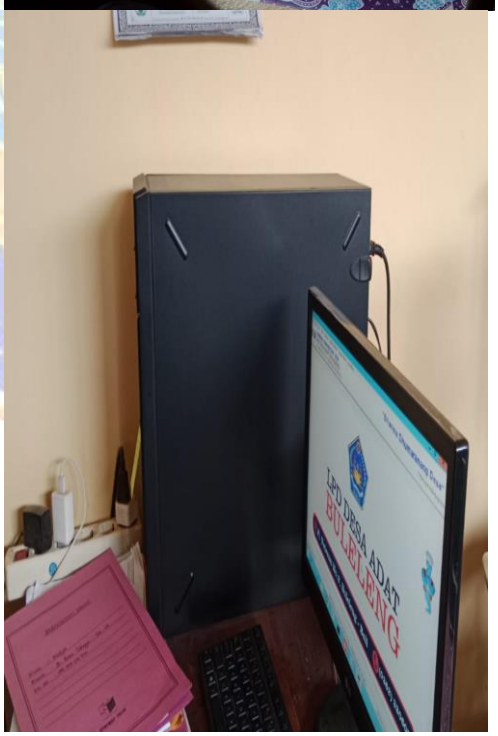
1. *PIHAK PERTAMA telah melakukan Proses Migrasi Data pada tanggal 27-11-2019 s/d 28-11-2019*
2. *PIHAK KEDUA sudah melakukan verifikasi dan sudah menyetujui hasil migrasi data sesuai dengan data yang sebenarnya serta sesuai dengan kriteria yang telah ditetapkan oleh kedua belah PIHAK.*
3. *Dengan dikeluarkannya Berita Acara ini, maka pekerjaan Migrasi Data dinyatakan telah selesai dan akan dilanjutkan dengan tahap implementasi berikutnya.*

PIHAK PERTAMA

(Bagus Rizqi Mubarok)

PIHAK KEDUA

(I Gusti Ngurah Candrayadhi)



Lampiran 4 Pengambilan data