Tencent Cloud

Panduan Kepatuhan Tencent Cloud terhadap Persyaratan Regulasi Keamanan Siber Indonesia

April 2026

CONTENTS

01 Ringkasan

Di tengah gelombang digitalisasi global, teknologi informasi telah terintegrasi secara mendalam dalam arus perdagangan internasional dan proses pertumbuhan ekonomi Indonesia, menjadi mesin penggerak utama untuk peningkatan industri dan pelepasan potensi ekonomi. Dalam konteks ini, Pemerintah Indonesia dan Kementerian Komunikasi dan Digital (The Ministry of Communication and Digital Affairs, selanjutnya disebut "Komdigi") menyadari sepenuhnya bahwa membangun infrastruktur hukum dan sistem pengawasan yang komprehensif merupakan jaminan kunci untuk mendukung perkembangan teknologi informasi. Langkah ini tidak hanya bertujuan mengatur skenario penerapan teknologi informasi dan mencegah risiko penyalahgunaan, tetapi juga berkomitmen untuk memperkuat penghalang keamanan ekosistem digital melalui regulasi standar, sehingga meletakkan fondasi yang kokoh bagi pembangunan berkelanjutan ekonomi digital. Berdasarkan visi pengembangan dan tuntutan regulasi di atas, Pemerintah Indonesia dan Kementerian Komunikasi dan Digital telah menetapkan serangkaian persyaratan regulasi yang spesifik dan jelas di bidang sistem dan transaksi elektronik. Serangkaian tindakan pengawasan ini tidak hanya mencerminkan tekad strategis Indonesia untuk mengembangkan ekonomi digital secara besar-besaran dan merebut peluang transformasi digital, tetapi juga menunjukkan komitmen teguh mereka dalam memperkuat mekanisme akuntabilitas industri, menjamin keamanan siber dan data, di tengah pesatnya ekspansi ruang digital, serta memberikan panduan yang jelas bagi perkembangan ekosistem digital Indonesia yang terstandarisasi dan aman.

Tencent Cloud secara aktif memantau perkembangan dan publikasi terbaru dari Pemerintah Indonesia serta Kementerian Komunikasi dan Digital, dan berkomitmen untuk membantu pelanggan di Indonesia memenuhi persyaratan regulasi dari otoritas pengawas. Dokumen ini akan menjelaskan bagaimana Tencent Cloud membantu pelanggan mematuhi persyaratan regulasi, dengan fokus pada pedoman dan pemberitahuan pengawasan berikut yang menjadi perhatian utama pelanggan:

- NOMOR 11 TAHUN 2008 Tentang Informasi dan Transaksi Elektronik

- NOMOR 19 TAHUN 2016 Tentang perubahan atas undang-undang perubahan atas undang-undang NOMOR 11 TAHUN 2008
- NOMOR 71 TAHUN 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik
- Nomor 5 Tahun 2020 Tentang Penyelenggara Sistem Elektronik Lingkup Privat
- Nomor 10 Tahun 2021 Tentang Perubahan atas Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2020

02

Keamanan dan Kepatuhan Privasi Tencent Cloud

Kepatuhan adalah fondasi pengembangan Tencent Cloud. Tencent Cloud mengidentifikasi dan menerapkan standar keamanan internasional dan industri yang mutakhir, mematuhi persyaratan kepatuhan di berbagai negara/wilayah dan sektor, terus menyempurnakan sistem manajemen internal, meningkatkan tingkat kontrol keamanan Tencent Cloud, serta berupaya sepenuhnya membangun layanan cloud yang dapat dipercaya oleh pelanggan. Secara bersamaan, Tencent Cloud juga aktif berpartisipasi dalam perumusan dan promosi standar keamanan industri, berpegang pada prinsip kepatuhan sebagai layanan, serta membangun dan mengoperasikan ekosistem cloud yang aman dan andal.

Hingga saat ini, Tencent Cloud telah memperoleh berbagai sertifikasi dan kualifikasi kepatuhan keamanan serta privasi melalui audit atau penilaian independen pihak ketiga, membuktikan bahwa pembangunan manajemen keamanan dan perlindungan privasi Tencent Cloud memenuhi standar sertifikasi terkait atau praktik baik industri. Untuk informasi lebih lanjut tentang kepatuhan Tencent Cloud, silakan lihat halaman **Tencent Cloud Compliance Center** . Jika memerlukan sertifikat atau laporan kepatuhan terkait, harap ajukan permohonan dan unduh melalui **Compliance Document Download**.

Berikut adalah beberapa contoh sertifikasi otoritatif internasional, serta pengakuan regional dan industri dari Tencent Cloud:

2.1 Sertifikasi Otoritatif Internasional

Sertifikasi Keamanan Cloud CSA STAR	STAR (Security, Trust & Assurance Registry) adalah sertifikasi keamanan cloud internasional yang diluncurkan oleh Cloud Security Alliance (CSA), organisasi nirlaba otoritatif global. Sertifikasi ini memperluas kerangka Sistem Manajemen Keamanan Informasi ISO/IEC 27001 dengan mengintegrasikan Cloud Control Matrix (CCM), sehingga memvisualisasikan isu-isu spesifik keamanan cloud dan memberikan gambaran umum yang intuitif kepada pengguna mengenai evaluasi arsitektur keamanan. Berdasarkan praktik keamanan yang telah terakumulasi oleh Tencent selama bertahun-tahun, Tencent Cloud telah meraih

	sertifikasi CSA STAR Gold tingkat global. Pencapaian ini menunjukkan bahwa sistem pengendalian keamanan Tencent Cloud memenuhi standar keamanan cloud internasional yang diakui secara luas.
Audit SOC	Laporan System and Organization Controls (selanjutnya disebut "Laporan SOC") adalah serangkaian laporan terkait kontrol internal penyedia layanan yang diterbitkan oleh kantor akuntan publik pihak ketiga profesional sesuai dengan standar yang ditetapkan oleh American Institute of Certified Public Accountants (AICPA). Sebagai laporan audit independen, Laporan SOC mencakup titik-titik kontrol yang berkaitan dengan keamanan, ketersediaan, dan kerahasiaan platform Tencent Cloud. Berdasarkan jenis layanan asuransi yang berbeda, Laporan SOC dapat disediakan bagi pengguna cloud serta auditor mereka, memberikan informasi berharga kepada pengguna Tencent Cloud untuk mengevaluasi dan mengatasi risiko yang terkait dengan penyedia layanan.

2.2 Sertifikasi Sistem ISO/IEC

Sertifikasi ISO/IEC 22301: 2019	ISO/IEC 22301: 2019 adalah standar internasional yang berfokus pada Manajemen Kelangsungan Bisnis (Business Continuity Management, BCM). Standar ini menyediakan metodologi BCM yang komprehensif dan universal, dengan tujuan membantu perusahaan mengidentifikasi dan merespons peristiwa-peristiwa disruptif potensial, memastikan kelangsungan operasi kritis, sehingga mengurangi risiko dan melindungi organisasi dari dampak signifikan. Tencent Cloud telah memperoleh sertifikasi ISO/IEC 22301: 2019, yang membuktikan bahwa Tencent Cloud telah membangun proses manajemen kelangsungan bisnis yang formal untuk menjamin keberlanjutan dan stabilitas operasi bisnisnya sendiri.
Sertifikasi ISO/IEC 27001: 2022	ISO/IEC 27001: 2022 adalah standar sertifikasi Sistem Manajemen Keamanan Informasi (ISMS) yang paling diakui, ketat, dan diterima secara luas di tingkat internasional dalam bidang keamanan informasi. Dengan memperoleh sertifikasi ini, sebuah perusahaan

	menunjukkan bahwa mereka telah membangun sistem manajemen keamanan informasi yang ilmiah dan efektif, guna menyelaraskan strategi pengembangan perusahaan dengan langkah-langkah manajemen keamanan informasi, serta memastikan risiko keamanan informasi yang relevan dikendalikan dan ditangani dengan tepat. Sertifikasi ISO/IEC 27001: 2022 lebih mencerminkan komitmen Tencent Cloud terhadap keamanan, menunjukkan bahwa Tencent Cloud telah membangun sistem manajemen yang ilmiah dan efektif, serta mampu menyediakan produk dan layanan cloud yang aman dan dapat diandalkan bagi pengguna.
Sertifikasi ISO/IEC 20000-1: 2018	ISO/IEC 20000-1: 2018 merupakan standar internasional yang dirumuskan khusus untuk manajemen layanan teknologi informasi (ITSM). Sistem ini menstandarisasi manajemen layanan TI suatu perusahaan, mencakup pola pembentukan, penerapan, operasi, pemantauan, peninjauan, pemeliharaan, dan peningkatan, guna membantu perusahaan secara berkelanjutan mengidentifikasi dan mengelola permasalahan TI terkait, memperkuat komunikasi dengan pengguna, serta membangun sistem layanan terstandar yang mampu menyempurnakan diri. Tencent Cloud telah memperoleh sertifikasi ISO/IEC 20000-1: 2018 dengan cakupan sertifikasi yang meliputi layanan komputasi awan, layanan terkelola (managed services), serta layanan pemulihan bencana. Dengan pendekatan yang berorientasi pada layanan prima, Tencent Cloud secara konsisten menyempurnakan mekanisme layanan dan komunikasi teknologi informasi dengan pelanggan.
Sertifikasi ISO/IEC 9001: 2015	ISO/IEC 9001: 2015 adalah sistem manajemen mutu yang matang dan diakui secara luas di tingkat internasional. Sistem ini menyediakan kerangka kerja dan pedoman normatif untuk manajemen mutu di seluruh proses penyediaan produk atau layanan perusahaan, bertujuan membantu perusahaan mempertahankan produk atau layanannya serta memastikan kualitas yang stabil dan konsisten dalam penyerahan. Tencent Cloud telah memperoleh sertifikasi ISO/IEC 9001 dengan cakupan yang meliputi layanan komputasi awan, layanan terkelola,

	serta layanan pemulihan bencana. Dengan menerapkan sistem manajemen mutu, Tencent Cloud mencapai target mutu yang diharapkan secara efektif dan efisien, sehingga menjamin kualitas produk dan layanan cloud serta operasionalnya.
Sertifikasi ISO/IEC 27017: 2015	ISO/IEC 27017: 2015 merupakan pelengkap dari ISO/IEC 27002: 2013 dan merupakan standar praktis untuk keamanan informasi layanan cloud. Standar ini menyediakan kontrol keamanan spesifik beserta panduan penerapannya bagi penyedia layanan cloud dan pelanggan, sehingga memperkuat pengendalian atas ancaman dan risiko kerentanan dalam komputasi awan. Tencent Cloud telah memperoleh sertifikasi ISO/IEC 27017: 2015. Hal ini tidak hanya menunjukkan bahwa Tencent Cloud senantiasa mengadopsi praktik terbaik yang diakui secara internasional, tetapi juga membuktikan bahwa Tencent Cloud telah membangun sistem manajemen keamanan cloud yang lebih komprehensif, sehingga meningkatkan kemampuan layanan keamanan cloud secara keseluruhan.
Sertifikasi ISO/IEC 27018: 2014	ISO/IEC 27018: 2014 merupakan standar keamanan global yang paling komprehensif dan diakui untuk penanganan Informasi Pribadi Teridentifikasi (PII) dalam lingkungan cloud publik. Standar ini bertujuan menyediakan seperangkat pedoman praktis bagi penyedia layanan cloud guna melindungi privasi pengguna, serta memastikan keamanan data pribadi dalam lingkungan komputasi awan. Perolehan sertifikasi ISO/IEC 27018: 2014 oleh Tencent Cloud menandakan bahwa sistem manajemen informasi pribadi Tencent Cloud mematuhi ketentuan hukum dan regulasi perlindungan informasi pribadi yang ketat secara internasional, sehingga memberikan kepercayaan dan jaminan lebih kepada pelanggan Tencent Cloud terkait keamanan cloud mereka.
Sertifikasi ISO/IEC 29151: 2017	ISO/IEC 29151 merupakan standar internasional yang digunakan untuk menerapkan langkah-langkah pengendalian terkait pemrosesan Informasi Pribadi Teridentifikasi (PII), guna memenuhi persyaratan yang ditentukan berdasarkan penilaian risiko dan dampak privasi yang terkait dengan perlindungan PII.

	Tencent Cloud telah memperoleh sertifikasi ISO/IEC 29151: 2017. Hal ini menunjukkan bahwa Tencent Cloud telah mengembangkan sistem pengendalian keamanan yang sesuai berdasarkan tujuan PII dan kebutuhan bisnisnya, serta menyediakan kontrol perlindungan privasi tingkat tinggi untuk PII pengguna di lingkungan cloud.
Sertifikasi ISO/IEC 27701: 2019	ISO/IEC 27701: 2019 merupakan persyaratan dan panduan perluasan dari ISO/IEC 27001 dan ISO/IEC 27002 dalam manajemen informasi privasi. Standar ini menyediakan pedoman untuk membangun, menerapkan, memelihara, dan terus meningkatkan Sistem Manajemen Informasi Privasi, yang menjadi tonggak penting dalam pengelolaan risiko privasi secara berkelanjutan. Perolehan sertifikasi ISO/IEC 27701: 2019 oleh Tencent Cloud membuktikan bahwa Tencent Cloud senantiasa menempatkan perlindungan privasi pengguna sebagai inti layanannya. Hal ini secara penuh menggambarkan standarisasi dan keandalan perlindungan privasi dalam produk-produk Tencent Cloud.

2.3 Sertifikasi Regional & Industri

C5 Jerman	Katalog Kriteria Kepatuhan Komputasi Awan (Cloud Computing Compliance Criteria Catalogue, disingkat C5) dikembangkan oleh Bundesamt für Sicherheit in der Informationstechnik (BSI) Jerman, dengan tujuan memverifikasi kepatuhan keamanan informasi penyedia layanan cloud melalui pemeriksaan dan pelaporan yang terstandarisasi. C5 adalah standar keamanan tingkat tinggi yang sangat diakui dalam industri layanan cloud. Tencent Cloud telah lulus audit standar dasar dan tambahan C5:2020 Jerman. Hal ini menunjukkan bahwa Tencent Cloud telah memenuhi standar tinggi yang ditetapkan oleh pemerintah Jerman dalam hal perlindungan data dan keamanan informasi.
TISAX Jerman	TISAX adalah standar penilaian keamanan informasi dan keamanan pertukaran data untuk industri otomotif yang diluncurkan oleh Asosiasi Industri Otomotif Jerman (VDA) bekerja sama dengan Asosiasi Pertukaran Data Keamanan Industri Otomotif Eropa (ENX). TISAX memungkinkan saling pengakuan

	hasil penilaian keamanan informasi di dalam industri otomotif dan menyediakan mekanisme penilaian serta pertukaran yang seragam. Saat ini, sejumlah Pusat Data Internet (IDC) milik Tencent Cloud (termasuk yang berlokasi di Beijing, Shenzhen, dan lainnya) telah lulus audit penilaian TISAX Tingkat 3. Hal ini menunjukkan bahwa layanan yang disebarkan di wilayah-wilayah tersebut memenuhi persyaratan TISAX dan telah membangun serta memelihara sistem manajemen keamanan informasi yang komprehensif.
Sertifikasi MTCS T3 Singapura	Standar Keamanan Cloud Berlapis Singapura (MTCS) dirumuskan di bawah bimbingan Komite Standar Teknologi Informasi (ITSC) dari Otoritas Pengembangan Infokom Singapura (IMDA). Sebagai standar umum untuk cloud, penyedia layanan cloud dapat mengadopsi standar ini untuk mengatasi kekhawatiran pelanggan mengenai keamanan dan kerahasiaan data di cloud, serta dampak penggunaan layanan cloud terhadap bisnis. Tencent Cloud telah berhasil memperoleh sertifikasi standar tingkat T3 dari MTCS (Multi-Tier Cloud Security) Singapura. Sertifikasi ini menunjukkan bahwa Tencent Cloud telah menerapkan mekanisme manajemen risiko yang kuat untuk menjamin keamanan, kerahasiaan, serta transparansi operasional yang dapat diverifikasi bagi data pelanggan di cloud.
OSPAR Singapura	Laporan Audit Penyedia Layanan Outsourcing (Outsourced Service Provider Audit Report, OSPAR) adalah standar akses untuk layanan outsourcing di industri keuangan Singapura. Standar ini didasarkan pada SSAE 3000 Singapura, bertujuan memverifikasi desain kontrol dan efektivitas operasional terkait di tiga bidang bagi penyedia layanan institusi keuangan Singapura: kontrol tingkat entitas, kontrol teknologi informasi umum, dan kontrol layanan. Berbagai produk dan layanan Tencent Cloud telah lulus audit OSPAR Singapura, dan Tencent Cloud secara konsisten berupaya memastikan bahwa kontrolnya mematuhi pedoman dari Asosiasi Perbankan Singapura (ABS). Keberhasilan dalam audit ini menunjukkan bahwa kemampuan keamanan Tencent Cloud

	memenuhi persyaratan ketat industri jasa keuangan di Singapura bahkan Asia Tenggara.
Data Protection Trustmark Singapura	Data Protection Trustmark (DPTM) dikembangkan oleh Komisi Perlindungan Data Pribadi Singapura (PDPC) bersama Otoritas Pengembangan Infokom Media (IMDA), bertujuan menunjukkan praktik perlindungan data yang bertanggung jawab oleh organisasi. Tencent Cloud telah memperoleh sertifikasi Data Protection Trustmark (DPTM) Singapura. Hal ini menunjukkan bahwa Tencent Cloud telah mengadopsi praktik perlindungan data yang bertanggung jawab bagi pelanggan, mitra bisnis, dan regulator, serta memiliki kemampuan untuk melindungi data pribadi yang dikumpulkannya.
Cyber Trust Mark (CTM) Singapura	Cyber Trust Mark (CTM) adalah sertifikasi keamanan siber tingkat nasional yang diluncurkan oleh Badan Keamanan Siber Singapura (Cyber Security Agency/CSA). Kerangka kerja CTM mengadopsi metodologi berbasis risiko, mencakup 22 subdomain dalam 4 area inti: tata kelola dan manajemen risiko, operasi keamanan siber, ketahanan, keamanan rantai pasok dan sumber daya manusia, serta peningkatan berkelanjutan dan praktik-praktik terdepan. Tencent Cloud telah meraih tingkat tertinggi (Tier 5) dari Cyber Trust Mark (CTM). Sertifikasi ini menegaskan kemampuan Tencent Cloud yang unggul dalam tata kelola keamanan siber, manajemen risiko, dan ketahanan operasional, sekaligus memposisikannya sebagai penyedia layanan cloud terpercaya bagi sektor-sektor yang diregulasi ketat dan berkebutuhan tinggi di seluruh kawasan Asia-Pasifik.
Sertifikasi KISMS Korea	Sertifikasi Sistem Manajemen Keamanan Informasi Korea (K-ISMS) adalah sertifikasi keamanan informasi yang didukung pemerintah Korea, bertujuan membantu perusahaan dan organisasi Korea secara konsisten melindungi aset informasi mereka dengan aman sesuai hukum teknologi informasi dan komunikasi Korea yang berlaku. Perolehan sertifikasi KISMS oleh Tencent Cloud menunjukkan bahwa pelanggan cloud di Korea lebih mudah membuktikan

	kepatuhan mereka terhadap persyaratan hukum lokal, sehingga melindungi aset informasi digital kritis. Hal ini juga mencerminkan peningkatan kemampuan langkah-langkah penanganan keamanan informasi dan prosedur respons ancaman Tencent Cloud, yang dapat lebih efektif mengurangi dampak kerentanan keamanan.
Audit Kepatuhan TI Industri Keuangan Malaysia	Bank Negara Malaysia (BNM), Suruhanjaya Sekuriti Malaysia (SC), dan regulator keuangan Malaysia lainnya telah mengeluarkan peraturan terkait yang ditujukan bagi industri jasa keuangan, guna menstandardisasi penerapan teknologi informasi di perbankan, asuransi, sekuritas, dan layanan keuangan lainnya di Malaysia, serta menjamin keandalan, keamanan, dan stabilitas sistem informasi keuangan. Melalui audit pihak ketiga independen, Tencent Cloud dapat membuktikan bahwa layanan cloud yang disediakan bagi klien keuangan di Malaysia mematuhi secara ketat persyaratan regulasi industri keuangan Malaysia.
Audit Kepatuhan TI Industri Keuangan Hong Kong	Otoritas Moneter Hong Kong (HKMA), Komisi Sekuritas dan Berjangka (SFC), serta Otoritas Asuransi (IA) Hong Kong telah menerbitkan sejumlah persyaratan pengawasan kunci guna mengatur penerapan teknologi informasi di lembaga keuangan, asuransi, dan sekuritas. Melalui audit pihak ketiga independen, Tencent Cloud membuktikan dirinya sebagai penyedia layanan cloud yang dapat dipercaya di industri keuangan. Tencent Cloud telah mengambil pendekatan proaktif untuk memenuhi kewajiban kepatuhan yang paling ketat, sehingga lembaga keuangan dapat dengan percaya membangun layanan keuangan generasi berikutnya di atas platform Tencent Cloud.
Audit Kepatuhan TI Industri Keuangan Thailand	Audit Kepatuhan TI Industri Keuangan Thailand: Lembaga industri keuangan Thailand harus mematuhi peraturan terkait yang dikeluarkan oleh Bank Sentral Thailand (BoT), Kantor Komisi Sekuritas dan Bursa (OSEC), Kantor Komisi Asuransi (OIC), dan badan pengatur serta otoritas hukum terkait lainnya. Persyaratan pengawasan ini mencakup: manajemen risiko dalam penerapan

	teknologi informasi, perlindungan informasi pribadi, serta penerapan dan kontrol keamanan teknologi informasi dalam sistem perbankan, asuransi, sistem pemerintahan elektronik, uang elektronik, infrastruktur sistem pembayaran, penyedia layanan pembayaran, dan lain-lain. Melalui audit pihak ketiga independen, Tencent Cloud dapat membuktikan kemampuannya dalam mematuhi persyaratan pengawasan industri keuangan Thailand yang ketat, serta komitmen Tencent Cloud untuk menyediakan layanan cloud yang berkualitas dan sesuai dengan regulasi bagi klien industri keuangan Thailand.
Audit Kepatuhan TI Industri Keuangan Indonesia	Bank Indonesia (BI), Otoritas Jasa Keuangan (OJK), dan regulator keuangan Indonesia lainnya telah mengeluarkan peraturan terkait yang ditujukan bagi industri jasa keuangan. Persyaratan pengawasan ini mencakup: manajemen risiko dalam penerapan teknologi informasi, perlindungan informasi pribadi, serta penerapan dan kontrol keamanan teknologi informasi dalam sistem perbankan, asuransi, sistem pemerintahan elektronik, uang elektronik, infrastruktur sistem pembayaran, penyedia layanan pembayaran, dan lain-lain. Tencent Cloud telah lulus audit kepatuhan keuangan Indonesia yang dilaksanakan oleh lembaga audit pihak ketiga independen. Hal ini membuktikan bahwa layanan cloud yang disediakan Tencent Cloud bagi klien keuangan di Indonesia mematuhi secara ketat persyaratan regulasi industri keuangan Indonesia.
Sertifikasi Manajemen Keamanan Informasi SNI 27001 Indonesia	SNI 27001 Indonesia adalah standar nasional untuk Sistem Manajemen Keamanan Informasi (ISMS) yang diawasi oleh Badan Standardisasi Nasional (BSN) dan disertifikasi oleh lembaga audit pihak ketiga independen. Kerangka SNI 27001 mengadopsi pendekatan berbasis risiko, dengan persyaratan inti yang mencakup dimensi kunci: pembentukan dan operasi berkelanjutan ISMS formal, penilaian risiko komprehensif dan langkah pengendalian yang ditargetkan, kepatuhan terhadap regulasi keamanan informasi lokal serta 14 bidang keamanan utama, serta audit internal, tinjauan manajemen, dan peningkatan berkelanjutan secara berkala.

	Perolehan sertifikasi SNI 27001 Indonesia oleh Tencent Cloud membuktikan kemampuan unggul Tencent Cloud dalam melindungi kerahasiaan, integritas, dan ketersediaan aset informasi, yang juga mencakup skenario keamanan khusus di lingkungan cloud. Hal ini mencerminkan sistem manajemen keamanan Tencent Cloud yang matang serta kemampuannya dalam menghadapi risiko siber yang terus berkembang di pasar Indonesia.
Audit Kepatuhan TI Industri Keuangan Filipina	Lembaga industri keuangan Filipina harus mematuhi peraturan terkait yang ditetapkan oleh Bank Sentral Filipina (BSP) dan badan pengatur serta otoritas hukum terkait lainnya dalam sektor keuangan. Persyaratan pengawasan ini mencakup: manajemen risiko dalam penerapan teknologi informasi, perlindungan informasi pribadi, serta penerapan dan kontrol keamanan teknologi informasi dalam sistem perbankan, asuransi, sistem pemerintahan elektronik, uang elektronik, infrastruktur sistem pembayaran, penyedia layanan pembayaran, dan lainnya. Melalui audit pihak ketiga independen, Tencent Cloud dapat membuktikan kemampuannya dalam mematuhi persyaratan pengawasan industri keuangan Filipina yang ketat, serta komitmennya untuk menyediakan layanan cloud yang berkualitas dan sesuai regulasi bagi klien industri keuangan.
Asosiasi Gambar Bergerak Amerika MPAA	Asosiasi Gambar Bergerak Amerika (MPAA) telah menetapkan seperangkat standar praktik terbaik untuk penyimpanan, pemrosesan, dan transmisi konten media yang dilindungi yang aman. Panduan implementasi ini bertujuan untuk memberi pemahaman kepada penyedia aplikasi dan layanan cloud yang bermitra dengan anggota MPAA mengenai persyaratan yang harus dipatuhi dalam hal keamanan konten. Komponen templat keamanan konten MPAA mengacu pada standar ISO terkait (27001-27002), standar keamanan (seperti NIST, CSA, ISACA, dan SANS), serta praktik terbaik industri. Tencent Cloud telah memperoleh sertifikasi terkait seperti ISO 27001, ISO 27017, ISO 27018, PCI DSS, dan CSA STAR. Selain itu, melalui penilaian mandiri, Tencent Cloud memastikan bahwa prosedur pengelolaan konten pelanggannya mematuhi panduan

	model keamanan konten Asosiasi Gambar Bergerak Amerika (MPAA).
HIPAA Amerika Serikat	Salah satu tujuan dari Undang-Undang HIPAA Amerika Serikat adalah mendorong penggunaan rekam medis elektronik dengan meningkatkan efisiensi dan kualitas sistem perawatan kesehatan melalui peningkatan berbagi informasi. HIPAA berfokus dan menjamin keamanan (termasuk ketersediaan, integritas, dan kerahasiaan) serta privasi dari Informasi Kesehatan yang Dilindungi (Protected Health Information, PHI) dalam siklus pembuatan, penerimaan, pemeliharaan, dan transmisi oleh entitas yang tercakup serta mitra bisnisnya. Entitas yang tunduk pada HIPAA dan mitra bisnis mereka diharuskan menerapkan langkah-langkah keamanan yang sesuai dalam skenario pemrosesan, pemeliharaan, dan penyimpanan PHI. Tencent Cloud, melalui penilaian mandiri, memastikan bahwa kemampuan perlindungan keamanan informasi pribadi pengguna dan efektivitas langkah-langkah kontrolnya mematuhi persyaratan kepatuhan HIPAA.
Aturan SEC 17a-4 Amerika Serikat	Layanan Penyimpanan Objek Tencent Cloud (COS) telah disertifikasi oleh perusahaan penilaian pihak ketiga independen yang berspesialisasi dalam manajemen catatan dan tata kelola informasi, sesuai dengan persyaratan teknis dari Komisi Sekuritas dan Bursa AS (SEC), Otoritas Regulasi Industri Keuangan (FINRA), dan Komisi Perdagangan Berjangka Komoditas (CFTC). Sertifikasi ini menjamin bagi pelanggan yang beroperasi di lingkungan yang sangat diatur (seperti industri jasa keuangan) mengenai metode penyimpanan yang tidak dapat ditimpa dan tidak dapat dihapus serta kemampuan penguncian objek dari Tencent COS, menunjukkan komitmen Tencent Cloud untuk menyediakan produk cloud yang aman dan sesuai dengan standar industri bagi pelanggan.
FISC Jepang	Untuk meningkatkan keamanan lembaga keuangan, Panduan Keamanan Sistem Komputer Bank dan Lembaga Keuangan Terkait (FISC) memberikan arahan efektif bagi bank dan lembaga

	keuangan Jepang dalam membangun sistem informasi yang aman serta menjamin pengoperasian sistem informasi. Berdasarkan panduan ini, Tencent Cloud telah melakukan penilaian terhadap status kontrol saat ini untuk memastikan bahwa langkah-langkah terkait yang diterapkan Tencent Cloud memenuhi persyaratan yang ditetapkan dalam Panduan Keamanan Sistem Komputer Bank dan Lembaga Keuangan Terkait (FISC).
BS 10012: 2017 Inggris	BS 10012: 2017 diterbitkan oleh British Standards Institution (BSI) yang bertujuan menyediakan kerangka kepatuhan dan praktik terbaik perlindungan privasi bagi organisasi, serta membimbing perusahaan dalam membangun dan memelihara Sistem Manajemen Informasi Pribadi (PIMS) guna memastikan organisasi memiliki langkah-langkah pengendalian yang memadai dan tepat untuk melindungi informasi pribadi. Sistem ini telah diperbarui dan direvisi agar sesuai dengan General Data Protection Regulation (GDPR). Tencent Cloud telah memperoleh sertifikasi BS 10012: 2017, yang mencerminkan bahwa Sistem Manajemen Informasi Pribadi Tencent Cloud memenuhi persyaratan standar internasional dan praktik terbaik industri, sehingga memungkinkan pelanggan untuk lebih patuh terhadap persyaratan perlindungan privasi GDPR.
CISPE Uni Eropa	Kode Etik CISPE (Cloud Infrastructure Services Providers in Europe) adalah pedoman sektoral pan-Eropa khusus untuk penyedia layanan infrastruktur cloud berdasarkan Pasal 40 Peraturan Perlindungan Data Umum (GDPR) Uni Eropa. Kode etik ini membantu organisasi di seluruh Eropa mempercepat pengembangan layanan berbasis cloud yang sesuai dengan GDPR bagi konsumen, bisnis, dan institusi. Tencent Cloud telah diberikan label "Kandidat" untuk Kode Etik CISPE. Hal ini menunjukkan bahwa Tencent Cloud telah menyelesaikan penilaian mandiri sesuai dengan persyaratan Kode Etik CISPE, yang digunakan untuk membuktikan kepatuhan Tencent Cloud pada tingkat dokumentasi dan implementasi.

Sertifikasi NIST CSF	Kerangka Kerja Siber NIST (NIST CSF) adalah sebuah kerangka kerja yang berfokus pada penggunaan pendorong bisnis untuk mengarahkan aktivitas keamanan siber, memperlakukan risiko keamanan siber sebagai bagian dari proses manajemen risiko organisasi, serta membantu organisasi menyesuaikan dan memprioritaskan kegiatan keamanan siber mereka berdasarkan kebutuhan bisnis, toleransi risiko, dan sumber daya yang dimiliki. Organisasi dapat meningkatkan keamanan dan ketahanan mereka dengan menerapkan prinsip dan panduan manajemen risiko dari kerangka kerja ini. Tencent Cloud telah memperoleh sertifikasi NIST CSF yang diverifikasi oleh lembaga pihak ketiga. Hal ini tidak hanya merupakan pengakuan atas kemampuan sistem pertahanan keamanan siber Tencent Cloud, tetapi juga menunjukkan bahwa Tencent Cloud mampu secara efektif mengidentifikasi, menahan, merespons, dan menangani risiko keamanan, serta melindungi aset cloud dan data pelanggan. Hal ini selanjutnya meningkatkan kepercayaan pelanggan terhadap stabilitas dan keamanan Tencent Cloud.
Sertifikasi PCI DSS	Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS) dibuat dan dikelola oleh Dewan Standar Keamanan Industri Kartu Pembayaran (PCI SSC). Untuk meningkatkan keamanan data pemegang kartu, PCI DSS menyediakan tolok ukur global yang seragam untuk persyaratan teknis dan operasional dalam melindungi data akun, dengan ruang lingkup yang mencakup semua entitas yang terlibat dalam pemrosesan kartu pembayaran, seperti pedagang, pengolah, akuisitor, penerbit, dan penyedia layanan, serta entitas lain yang menyimpan, memproses, atau mengirimkan data pemegang kartu. Tencent Cloud telah lulus audit sertifikasi PCI DSS dan memperoleh kualifikasi Penyedia Layanan PCI DSS Level 1. Hal ini membuktikan bahwa Tencent Cloud dapat menyediakan layanan pembayaran yang aman dan andal bagi pelanggan serta melindungi keamanan data pemegang kartu.

Kepatuhan GxP	Dalam industri perawatan kesehatan, GxP mencakup beragam aktivitas terkait kepatuhan yang luas. Secara umum, GxP mengacu pada seperangkat peraturan, pedoman, atau praktik terbaik industri yang mengatur pengembangan, manufaktur, dan penjualan produk perawatan kesehatan seperti obat-obatan, perangkat medis, dan aplikasi perangkat lunak medis. Tencent Cloud telah menerbitkan Buku Putih Kepatuhan GxP, yang menjelaskan kepada pelanggan di industri perawatan kesehatan bahwa proses manajemen dan langkah-langkah teknis Tencent Cloud dapat membantu mereka memenuhi persyaratan sistem terkomputerisasi GxP. Selain itu, hal ini memastikan kerahasiaan, integritas, dan ketersediaan data bisnis pelanggan yang dihosting di Tencent Cloud.

03

Model Tanggung Jawab Bersama untuk Keamanan Cloud Tencent

Saat ini, semakin banyak pelanggan yang menjadikan keamanan sebagai salah satu faktor pertimbangan utama dalam memilih penyedia layanan komputasi awan beserta produk dan layanan yang ditawarkannya. Tencent Cloud berpegang pada karakteristik terbuka dan berbagi dari layanan komputasi awan, terus meningkatkan kemampuan keamanan platform dan layanan cloud, serta bersama-sama dengan pelanggan membangun sistem perlindungan keamanan yang lebih baik dan lebih lengkap untuk bisnis dan data di cloud. Sebagai penyedia layanan cloud, Tencent Cloud bertanggung jawab atas infrastruktur pusat data dan keamanan platform cloud. Mengingat bahwa ketika pelanggan memilih kategori layanan cloud yang berbeda (seperti layanan IaaS, PaaS, dan SaaS), tingkat kendali atas komponen yang berbeda juga akan bervariasi. Untuk itu, Tencent Cloud telah membangun model Tanggung Jawab Bersama untuk Keamanan Cloud berdasarkan berbagai kategori layanan cloud. Dalam model ini, area berwarna biru muda menjadi tanggung jawab Tencent Cloud, area berwarna abu-abu muda menjadi tanggung jawab pelanggan, sedangkan area berwarna hijau muda menunjukkan tanggung jawab bersama yang akan dipikul oleh Tencent Cloud dan pelanggan.

	IaaS	PaaS	SaaS	
Tanggung Jawab Klien	Keamanan Data Pelanggan Cloud	Keamanan Data Pelanggan Cloud	Keamanan Data Pelanggan Cloud	
	Kebijakan Akun dan Kontrol Akses Pelanggan Cloud	Kebijakan Akun dan Kontrol Akses Pelanggan Cloud	Kebijakan Akun dan Kontrol Akses Pelanggan Cloud	
	Kebijakan Konfigurasi Keamanan di Cloud	Kebijakan Konfigurasi Keamanan di Cloud	Kebijakan Konfigurasi Keamanan di Cloud	Tanggung Jawab Bersama untuk Layanan/Skenario Berbeda
	Keamanan Aplikasi di Cloud	Keamanan Aplikasi di Cloud	Keamanan Aplikasi di Cloud	
	Keamanan Jaringan Virtual dan Host di Cloud	Keamanan Jaringan Virtual dan Host di Cloud	Keamanan Jaringan Virtual dan Host di Cloud	Tanggung Jawab Tencent Cloud
	Kepatuhan dan Keamanan Platform Cloud serta Produk Cloud itu Sendiri	Kepatuhan dan Keamanan Platform Cloud serta Produk Cloud itu Sendiri	Kepatuhan dan Keamanan Platform Cloud serta Produk Cloud itu Sendiri	
	Keamanan Fisik dan Infrastruktur	Keamanan Fisik dan Infrastruktur	Keamanan Fisik dan Infrastruktur	

Gambar 1: Model Tanggung Jawab Bersama Keamanan Informasi Tencent Cloud

Penjelasan Tencent Cloud terhadap atribut keamanan yang berbeda dalam gambar di atas adalah sebagai berikut:

- **Keamanan Data Pelanggan Cloud**: Mengacu pada manajemen keamanan data bisnis pelanggan itu sendiri di lingkungan komputasi awan, termasuk data bisnis pelanggan yang diunggah, disimpan, didistribusikan, diproses, atau ditangani dengan cara lain.
- **Kebijakan Akun dan Kontrol Akses Pelanggan Cloud**: Mengacu pada informasi akun Tencent Cloud yang didaftarkan oleh pelanggan, serta semua tindakan otorisasi di bawah akun cloud, termasuk informasi akun, kata sandi, kebijakan kontrol akses, autentikasi, dan sebagainya.
- **Kebijakan Konfigurasi Keamanan di Cloud**: Mengacu pada produk keamanan dan kebijakan konfigurasi keamanan yang sesuai dengan persyaratan keamanan bisnis yang berbeda berdasarkan skenario tertentu, untuk mengembangkan atau menggunakan produk cloud (termasuk produk keamanan) dengan benar.
- **Keamanan Aplikasi di Cloud**: Mengacu pada manajemen keamanan sistem aplikasi terkait bisnis di lingkungan komputasi awan, termasuk desain, pengembangan, rilis, operasi, pemeliharaan, dan pemantauan aplikasi.
- **Keamanan Jaringan Virtual dan Host di Cloud**: Mengacu pada manajemen keamanan host dan jaringan di lingkungan komputasi awan. Pada tingkat jaringan, mencakup jaringan virtual, penyeimbangan beban, gateway keamanan, VPN, sambungan khusus, dan sebagainya; pada tingkat host, mencakup manajemen dasar (seperti lapisan kontrol virtualisasi, sistem manajemen basis data, jaringan disk array, dll.) dan manajemen penggunaan (seperti host virtual, citra, CDN, sistem file, dll.) untuk produk cloud seperti komputasi awan, penyimpanan awan, dan basis data awan.

- **Kepatuhan dan Keamanan Platform Cloud serta Produk Cloud itu Sendiri**: Mengacu pada keamanan dan kepatuhan platform cloud serta produk/layanan cloud yang disediakan di lingkungan komputasi awan.
- **Keamanan Fisik dan Infrastruktur**: Mengacu pada operasi keamanan pusat data, serta manajemen keamanan server fisik dan perangkat jaringan fisik di lingkungan komputasi awan.

Untuk informasi lebih lanjut tentang Model Tanggung Jawab Bersama Keamanan, silakan lihat Tencent Cloud Security White Paper.

04

Infrastruktur Global Tencent Cloud

Tencent Cloud telah menyebarkan banyak pusat data di seluruh dunia, membentuk jaringan infrastruktur yang luas yang mampu menyediakan layanan cepat, stabil, cerdas, dan andal di lokasi terdekat bagi pelanggan global. Tencent Cloud telah membuka 20+ wilayah geografis (Region) dan mengoperasikan 60+ zona ketersediaan (Availability Zone) di Tiongkok Daratan, kawasan Asia Pasifik, Amerika Utara, dan Eropa. Ini memberikan dukungan teknis yang kuat untuk lebih banyak perusahaan, membantu ekspansi bisnis yang pesat, memungkinkan pelanggan merespons persyaratan peraturan di berbagai wilayah secara fleksibel, memenuhi kebutuhan perusahaan industri keuangan akan penyimpanan data lokal dan globalisasi bisnis, serta memastikan kepatuhan, keamanan, dan efisiensi dalam pemrosesan data.

- Wilayah (Region) mengacu pada area geografis fisik tempat pusat data berada. Wilayah-wilayah Tencent Cloud sepenuhnya terisolasi satu sama lain, memastikan stabilitas dan toleransi kesalahan maksimum antarwilayah. Untuk mengurangi latensi akses dan meningkatkan kecepatan unduh, disarankan agar pelanggan memilih wilayah yang terdekat.
- Zona Ketersediaan (Zone) adalah pusat data fisik di dalam wilayah yang sama dengan pasokan listrik dan jaringan yang saling independen. Tujuannya adalah memastikan bahwa kegagalan di satu zona ketersediaan tidak menyebar ke zona lain (kecuali dalam kasus bencana besar atau gangguan listrik skala besar), sehingga layanan bisnis pengguna tetap berjalan. Dengan meluncurkan instans di zona ketersediaan yang terpisah, pengguna dapat melindungi aplikasi mereka dari dampak kegagalan di satu lokasi.

Tencent Cloud saat ini telah menerapkan 2.300+ node akselerasi di dalam Tiongkok, mencakup berbagai operator. Di luar Tiongkok, terdapat 900+ node akselerasi yang mencakup 70+ negara dan wilayah di seluruh dunia. Dengan mendistribusikan konten layanan ke seluruh node akselerasi di jaringan dan menggunakan sistem penjadwalan global, pengguna dapat mengakses konten

yang diperlukan dari node terdekat, sehingga mengurangi latensi akses. Tencent Cloud juga meningkatkan isolasi dan keamanan data dengan membangun situs independen serta menerapkan teknologi seperti enkripsi data, kontrol akses, dan pelacakan audit, mencegah kebocoran data dan akses tidak sah, serta memperkuat isolasi data berdasarkan wilayah dan penanganan yang sesuai dengan regulasi.

Untuk informasi lebih lanjut tentang infrastruktur Tencent Cloud, silakan kunjungi halamanTencent Cloud Global Infrastructure.

05

BagaimanaTencent Cloud Membantu Mematuhi dan Mendukung Pelanggan Dalam Memenuhi Undang-Undang Informasi dan Transaksi Elektronik Beserta Perubahannya

Globalisasi informasi telah menjadikan Indonesia bagian dari komunitas informasi dunia. Pemerintah Indonesia menilai perlu untuk menetapkan regulasi terkait informasi dan transaksi elektronik di tingkat nasional, guna mendorong perkembangan teknologi informasi di semua lapisan masyarakat secara optimal, seimbang, dan luas, sehingga memajukan kehidupan teknologi masyarakat. Oleh karena itu, Pemerintah Indonesia menerbitkan NOMOR 11 TAHUN 2008 Tentang Informasi dan Transaksi Elektronik pada tahun 2008, yang kemudian diubah melalui penerbitan NOMOR 19 TAHUN 2016 Tentang perubahan atas undang-undang perubahan atas undang-undang NOMOR 11 TAHUN 2008 pada tahun 2016. Tujuannya adalah untuk memperkuat kepastian hukum, manfaat, kehati-hatian, dan netralitas teknologi dalam penerapan teknologi informasi dan transaksi elektronik. Klausul-klausulnya terutama berkisar pada informasi elektronik[1], catatan elektronik dan tanda tangan elektronik[2], sertifikasi elektronik[3] dan sistem elektronik[4], transaksi elektronik[5], nama domain, serta perlindungan hak kekayaan intelektual dan privasi.

Dalam bab ini, Tencent Cloud akan menyaring dan merangkum persyaratan kontrol yang terkait dengan penyedia layanan cloud dalam NOMOR 11 TAHUN 2008 beserta perubahannya, serta menjelaskan bagaimana Tencent

---

1 "Informasi Elektronik" adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, electronic data interchange (EDI) surat elektronik (electronic mail), telegram, teleks, telecopy atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.

2 "Tanda Tangan Elektronik" adalah tanda tangan yang terdiri atas Informasi Elektronik yang dilekatkan, terasosiasi atau terkait dengan Informasi Elektronik lainnya yang digunakan sebagai alat verifikasi dan autentikasi.

3 Sertifikat Elektronik" adalah sertifikat yang bersifat elektronik yang memuat Tanda Tangan Elektronik dan identitas yang menunjukan status subyek hukum para pihak dalam Transaksi Elektronik yang dikeluarkan oleh Penyelenggara Sertifikasi Elektronik.

4 "Sistem Elektronik" adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi Elektronik.

5 "Transaksi Elektronik" adalah perbuatan hukum yang dilakukan dengan menggunakan Komputer, jaringan Komputer, dan/atau media elektronik lainnya.

Cloud, sebagai penyedia layanan cloud, dapat membantu Penyelenggara Sistem Elektronik[6] mematuhi persyaratan terkait.

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
15	Penyelenggaraan Sistem Elektronik	(1) Setiap Penyelenggara Sistem Elektronik harus menyelenggarakan Sistem Elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya Sistem Elektronik sebagaimana mestinya. (2) Penyelenggara Sistem Elektronik bertanggung jawab terhadap Penyelenggaraan Sistem Elektroniknya. (3) Ketentuan sebagaimana dimaksud pada ayat (2) tidak berlaku dalam hal dapat dibuktikan terjadinya keadaan memaksa, kesalahan, dan/atau kelalaian pihak pengguna Sistem Elektronik.	Sebagai penyelenggara sistem elektronik, pelanggan bertanggung jawab atas operasi normal sistem elektronik yang dijalankannya, serta harus memastikan keandalan dan keamanannya. Sebagai penyedia layanan cloud, Tencent Cloud telah memberikan dukungan produk dan layanan cloud yang terpercaya bagi jutaan klien tingkat perusahaan dan pengembang individu, memenuhi kebutuhan pengembangan di berbagai bidang seperti game, video, seluler, kesehatan, pemerintahan, keuangan, dan internet+. Tencent Cloud secara ketat mematuhi hukum dan peraturan terkait keamanan siber, privasi pengguna, serta keamanan data di yurisdiksi tempat operasi bisnis berlangsung. Tencent Cloud berpegang pada karakteristik terbuka dan berbagi dari layanan komputasi awan, terus meningkatkan kemampuan keamanan platform dan layanan cloud, serta bersama-sama dengan pelanggan membangun sistem perlindungan keamanan yang lebih baik dan lebih lengkap untuk bisnis dan data di cloud. Sebagai penyedia layanan cloud, Tencent Cloud bertanggung jawab atas infrastruktur

[6] Penyelenggara Sistem Elektronik" adalah setiap Orang, penyelenggara negara, Badan Usaha, dan masyarakat yang menyediakan, mengelola, dan/atau mengoperasikan Sistem Elektronik, baik secara sendiri-sendiri maupun bersama-sama kepada pengguna Sistem Elektronik untuk keperluan dirinya dan/atau keperluan pihak lain.

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			pusat data dan keamanan platform cloud. Mengingat bahwa ketika pelanggan memilih kategori layanan cloud yang berbeda (seperti layanan IaaS, PaaS, dan SaaS), tingkat kendali atas komponen yang berbeda juga akan bervariasi. Oleh karena itu, Tencent Cloud telah membangun model Tanggung Jawab Bersama untuk Keamanan Cloud berdasarkan kategori layanan cloud yang berbeda. Detail lebih lanjut dapat dilihat di Bab 3 panduan ini: "**Model Tanggung Jawab Bersama untuk Keamanan Cloud Tencent**". Berdasarkan tujuan di atas dan model tanggung jawab bersama, Tencent Cloud akan memperdalam kolaborasi dengan pelanggan untuk bersama-sama mengatasi berbagai masalah dan tantangan keamanan. Sebagai penyedia layanan cloud, Tencent Cloud menyediakan dokumen hukum secara online di situs web internasionalnya seperti KETENTUAN LAYANAN、General Service Level Agreement、Perjanjian Privasi dan Keamanan Data, yang secara jelas mengatur konten layanan dan tingkat layanan yang diberikan Tencent Cloud, perlindungan data pengguna dan kekayaan intelektual, serta tanggung jawab dan kewajiban keamanan antara pelanggan dan Tencent Cloud. Pelanggan juga dapat memilih untuk menandatangani perjanjian offline dengan Tencent Cloud guna merundingkan klausul dan ketentuan dalam perjanjian

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			tersebut.
16	Penyelenggara Sistem Elektronik	(1) Sepanjang tidak ditentukan lain oleh undang-undang tersendiri, setiap Penyelenggara Sistem Elektronik wajib mengoperasikan Sistem Elektronik yang memenuhi persyaratan minimum sebagai berikut: a. dapat menampilkan kembali Informasi Elektronik dan/atau Dokumen Elektronik secara utuh sesuai dengan masa retensi yang ditetapkan dengan Peraturan Perundang-undangan; b. dapat melindungi ketersediaan, keutuhan, keotentikan, kerahasiaan, dan keteraksesan, Informasi Elektronik dalam Penyelenggaraan Sistem Elektronik tersebut; c. dapat beroperasi sesuai dengan prosedur atau petunjuk dalam Penyelenggaraan Sistem Elektronik tersebut; d. dilengkapi dengan prosedur atau petunjuk yang diumumkan dengan bahasa, informasi, atau simbol yang dapat dipahami oleh pihak yang bersangkutan dengan	Sebagai penyelenggara sistem elektronik, pelanggan harus melindungi ketersediaan, integritas, kerahasiaan, keaslian, dan aksesibilitas informasi elektronik selama proses operasi sistem elektronik, serta memperjelas periode retensi yang ditetapkan oleh hukum. Pelanggan juga harus menyediakan petunjuk layanan operasional dalam versi bahasa yang dapat dipahami oleh pihak terkait, dan memastikan ketepatan waktu petunjuk layanan tersebut. Untuk mendukung kepatuhan pelanggan terhadap persyaratan regulasi, Tencent Cloud secara ketat memproses data pelanggan sesuai dengan KETENTUAN LAYANAN dan Kebijakan Privasi, serta mendukung pelanggan dalam menetapkan periode penyimpanan data sesuai dengan persyaratan hukum. Untuk memastikan kerahasiaan dan integritas data pelanggan, **Dalam hal perlindungan penyimpanan data**, berbagai produk penyimpanan dan basis data Tencent Cloud mendukung fungsi enkripsi data. Layanan ini menggunakan algoritma enkripsi yang aman dan kuat, serta mengintegrasikan **Key Management**

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
		Penyelenggaraan Sistem Elektronik tersebut; dan e. memiliki mekanisme yang berkelanjutan untuk menjaga kebaruan, kejelasan, dan kebertanggungjawaban prosedur atau petunjuk.	Service (KMS) untuk mengelola siklus hidup kunci secara menyeluruh, sehingga menjamin kerahasiaan data. Selain itu, Tencent Cloud menggunakan teknologi penyimpanan redundan multi-salinan dan kode penghapusan saat menyimpan data, serta segera mengambil tindakan pemulihan yang diperlukan ketika mendeteksi kesalahan integritas, sehingga sangat meningkatkan kemampuan toleransi kesalahan data. **Dalam hal perlindungan akses data**, data pelanggan di dalam Tencent Cloud termasuk dalam kategori data dengan tingkat keamanan tinggi. Hak kontrol atas data pelanggan sepenuhnya dipegang oleh pelanggan, dan Tencent Cloud tidak akan berusaha mengakses atau mengungkapkan konten pelanggan. Tencent Cloud secara internal telah menetapkan standar manajemen kontrol akses dan membangun mekanisme manajemen serta otorisasi hak akses. Lingkungan produksi Tencent Cloud telah sepenuhnya menggunakan bastion host, yang melakukan kontrol terpusat atas hak akses akun administrator dan aktivitas akun pada komponen sistem backend Tencent Cloud. **Dalam hal pencadangan data**, untuk data pelanggan di cloud, Tencent Cloud menyediakan beberapa salinan penyimpanan dan layanan

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			pencadangan berdasarkan fungsionalitas produk atau layanan cloud, serta bertanggung jawab atas layanan pencadangan data yang diberikan sesuai dengan kesepakatan dalam Service Level Agreement (SLA) produk. Ketika pelanggan perlu mengakhiri perjanjian kontrak karena perubahan bisnis atau perencanaan TI di masa depan, pelanggan dapat memilih untuk melakukan pencadangan dan migrasi data cloud serta lingkungan produksi kapan saja. Setelah layanan cloud diakhiri, Tencent Cloud akan mengikuti metode penghapusan data yang ketat dan menghapus sepenuhnya data pelanggan, termasuk salinan dan cadangannya, setelah periode retensi berakhir. Data yang telah dihapus tidak dapat dipulihkan. Prosedur operasional dan panduan pengguna produk Tencent Cloud telah didokumentasikan dan disediakan bagi pelanggan melalui situs web resmi. Tencent Cloud juga menawarkan Tencent Cloud Training and Certification berbasis pengetahuan produk Tencent Cloud serta keahlian profesional terkait, guna meningkatkan kemampuan teknis dan penguasaan cloud pelanggan.

06

BagaimanaTencent Cloud Membantu Mematuhi dan Mendukung Pelanggan Dalam Memenuhi Penyelenggaraan Sistem dan Transaksi Elektronik

Untuk mendorong pertumbuhan ekonomi digital dan mempertahankan kedaulatan negara atas informasi elektronik, Pemerintah Indonesia menerbitkan NOMOR 71 TAHUN 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik pada tahun 2019. Peraturan ini secara komprehensif mengatur penerapan teknologi informasi dan transaksi elektronik. Dari berbagai aspek seperti penyelenggaraan sistem elektronik, penyelenggaraan agen elektronik, pelaksanaan transaksi elektronik, sertifikasi elektronik, lembaga sertifikasi keandalan, dan pengelolaan nama domain, peraturan ini membimbing penyelenggara sistem elektronik di sektor publik dan swasta untuk menjalankan aktivitas operasional dengan cara yang andal dan aman.

Dalam bab ini, Tencent Cloud akan merangkum dan menyaring persyaratan kontrol yang terkait dengan penyedia layanan cloud dalam NOMOR 71 TAHUN 2019, serta menjelaskan bagaimana Tencent Cloud, sebagai penyedia layanan cloud, dapat membantu penyelenggara sistem elektronik mematuhi persyaratan terkait.

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
6	Pendaftaran Sistem Elektronik	(1) Setiap Penyelenggara Sistem Elektronik sebagaimana wajib melakukan pendaftaran. (2) Kewajiban melakukan pendaftaran bagi Penyelenggara Sistem Elektronik dilakukan sebelum Sistem Elektronik mulai digunakan oleh Pengguna Sistem Elektronik. (3) Pendaftaran Penyelenggara Sistem Elektronik sebagaimana dimaksud pada ayat (1) diajukan kepada Menteri melalui pelayanan	Sebagai penyelenggara sistem elektronik, pelanggan harus melakukan pendaftaran dan mematuhi norma, standar, serta prosedur yang ditetapkan dalam peraturan. Sebagai penyedia layanan cloud, Tencent Cloud juga telah menyerahkan dokumen yang diperlukan untuk pendaftaran kepada otoritas pengawas setempat di Indonesia dan menyelesaikan proses registrasi sebagai penyelenggara sistem elektronik di sektor swasta.

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
		perizinan berusaha terintegrasi secara elektronik sesuai dengan ketentuan peraturan perundang-undangan.	
7	Perangkat Keras	(1) Perangkat Keras yang digunakan oleh Penyelenggara Sistem Elektronik harus: a. memenuhi aspek keamanan, interkonektivitas dan kompatibilitas dengan sistem yang digunakan; b. mempunyai layanan dukungan teknis, pemeliharaan, dan/ atau purnajual dari penjual atau penyedia; dan c. memiliki jaminan keberlanjutan layanan. (2) Pemenuhan terhadap persyaratan sebagaimana dimaksud pada ayat (1) harus dilakukan melalui sertifikasi atau bukti-bukti sejenis lainnya.	Sebagai penyelenggara sistem elektronik, pelanggan harus memastikan keamanan dan interoperabilitas perangkat keras yang digunakan, serta kompatibilitas sistem yang dioperasikan, serta memiliki akses terhadap dukungan teknis dan layanan pasca penjualan, guna menjamin keberlanjutan layanan. Dalam rangka mendukung pelanggan memenuhi persyaratan regulasi, **khususnya terkait keamanan pusat data**, infrastruktur Tencent Cloud tersebar di berbagai lokasi global, yang terdiri atas wilayah (region) dan zona ketersediaan (availability zone). Setiap wilayah merupakan area geografis yang independen, sedangkan setiap zona ketersediaan merupakan domain pemeliharaan kegagalan yang terpisah dan terisolasi secara fisik. Pelanggan dapat secara fleksibel menempatkan data dan sistem di wilayah atau zona ketersediaan yang berbeda sesuai dengan kebutuhan pengembangan bisnis dan persyaratan keamanan data, guna memenuhi kebutuhan ketahanan bencana (disaster recovery) bagi operasional bisnis.

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			Dalam hal kontrol akses fisik, Tencent Cloud mewajibkan operator untuk menetapkan prosedur akses formal untuk akses fisik ke pusat data, melakukan verifikasi identitas terhadap individu yang memasuki pusat data, serta memeriksa dan mencatat barang bawaan. Tencent Cloud juga mensyaratkan operator pusat data untuk secara berkala melakukan tinjauan hak akses ke pusat data guna memastikan distribusi hak akses yang tepat dan menonaktifkan hak akses yang tidak relevan atau tidak diperlukan secara tepat waktu. Untuk kunjungan eksternal ke pusat data, Tencent Cloud meminta operator untuk membangun mekanisme permohonan dan otorisasi pengunjung terkait, hanya mengizinkan pengunjung yang telah disetujui untuk mengakses area tertentu di pusat data pada waktu yang ditentukan dan didampingi oleh staf terkait. Selain itu, Tencent Cloud mensyaratkan operator untuk menetapkan prosedur persetujuan dan pemeriksaan untuk perangkat yang masuk atau keluar dari ruang server (seperti untuk instalasi, operasi, atau pemindahtanganan dan penonaktifan). **Dalam hal keamanan dan pengawasan**, Tencent Cloud mewajibkan personel keamanan operator pusat data untuk

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			melakukan inspeksi harian yang ketat terhadap setiap ruang server dan kondisi peralatan sesuai dengan daftar dan rencana inspeksi, menandatangani serta mencatat waktu pemeriksaan di setiap titik pemeriksaan, dan segera mengaktifkan prosedur tanggap darurat pusat data jika ditemukan kegagalan infrastruktur atau insiden keamanan. Tencent Cloud mewajibkan operator pusat data untuk melengkapi pusat data dengan sistem alarm pemantauan video 7*24 jam tanpa titik buta, yang dijaga oleh pos keamanan, serta memastikan rekaman pengawasan disimpan secara aman untuk jangka waktu yang cukup. **Dalam hal pemeliharaan perangkat keras komputer,** departemen terkait manajemen perangkat keras Tencent Cloud secara terpusat mengelola pengajuan tiket, konfirmasi penerimaan, penyimpanan, dan distribusi sesuai rencana untuk perangkat keras. Departemen yang membutuhkan secara ketat menggunakan perangkat keras sesuai dengan petunjuk yang ditetapkan dan melakukan pemeliharaan rutin terhadap perangkat keras sesuai persyaratan yang berlaku. Jika terjadi kerusakan pada perangkat keras, departemen manajemen perangkat keras akan menilai sifat kerusakan dan tingkat kerusakan untuk menentukan apakah perlu perbaikan. Untuk perangkat komputer baru yang

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			mengalami kerusakan selama masa garansi, penanganan dilakukan sesuai ketentuan garansi dengan mengajukan laporan permohonan yang menjelaskan penyebab kerusakan, yang pelaksanaannya diawasi oleh departemen manajemen perangkat keras. Tencent Cloud telah memperoleh berbagai sertifikasi dan kualifikasi kepatuhan keamanan serta privasi melalui audit atau penilaian independen oleh pihak ketiga, seperti ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, ISO/IEC 22301, NIST CSF, dan SOC. Untuk memastikan kebijakan, prosedur, proses, dan langkah pengendalian teknologi informasi Tencent Cloud memenuhi persyaratan regulasi keuangan Indonesia, Tencent Cloud telah lolos audit kepatuhan IT industri keuangan Indonesia yang dilakukan oleh pihak ketiga independen dan sertifikasi SNI 27001. Pelanggan dapat mengunduh laporan terbaru secara mandiri dari Pusat Dokumen Kepatuhan Tencent Cloud.
8	Perangkat Lunak	Perangkat Lunak yang digunakan oleh Penyelenggara Sistem Elektronik harus: a. terjamin keamanan dan keandalan operasi sebagaimana mestinya; b. memastikan keberlanjutan layanan.	Sebagai penyelenggara sistem elektronik, pelanggan harus memastikan keamanan perangkat lunak yang digunakan, keandalan operasional, serta keberlanjutan layanan. Dalam rangka mendukung pelanggan memenuhi persyaratan regulasi, **khususnya dalam memastikan keamanan perangkat**

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			lunak, Tencent Cloud telah membangun seperangkat standar pengembangan keamanan sistem informasi internal. Tencent Cloud berupaya mengintegrasikan standar ISO/IEC 20000 Manajemen Layanan Teknologi Informasi, ISO/IEC 27001 Sistem Manajemen Keamanan Informasi, dan ISO/IEC 9001 Sistem Manajemen Mutu ke dalam seluruh siklus hidup pengembangan keamanan produk. Hal ini dilakukan dengan memperhatikan berbagai tahapan seperti analisis kebutuhan, desain, pengembangan, pengujian, penerapan, dan pemeliharaan, untuk menghilangkan masalah keamanan informasi dan privasi pada setiap tahap pengembangan produk, serta memastikan bahwa produk cloud mendapatkan pengendalian keamanan yang memadai selama siklus hidupnya. Tindakan pengendalian keamanan terkait meliputi: • Pelatihan Keamanan: Meningkatkan kesadaran pemrograman aman di kalangan pengembang, dan secara ketat mewajibkan personel terkait untuk mematuhi standar pengkodean yang aman. • Analisis Kebutuhan: Berkomunikasi mengenai konten bisnis, alur proses bisnis, dan kerangka teknologi untuk menemukan cara optimal dalam mengintegrasikan keamanan.

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			• Desain Sistem: Melakukan pemodelan ancaman terhadap desain sistem, serta menilai keamanan teknologi dari arsitektur yang digunakan. • Pengembangan Sistem: Selama proses pengembangan, menyediakan komponen pengembangan aman yang dirancang sendiri oleh Tencent untuk digunakan oleh tim pengembang, dan melakukan pengkodean sesuai dengan standar pengkodean aman Tencent Cloud. • Verifikasi Keamanan: Mendeteksi kerentanan melalui pemeriksaan keamanan kode, pemindaian keamanan aset, pemindaian web, penilaian keamanan manual, pengujian penetrasi, dan audit kode. • Rilis: Sistem hanya dapat dirilis ke lingkungan produksi setelah semua risiko tinggi diperbaiki, guna mencegah produk dijalankan di lingkungan produksi dengan membawa kerentanan keamanan. **Dalam hal memastikan keberlanjutan layanan dan keandalan operasional**, untuk memastikan ketersediaan berkelanjutan dari bisnis pelanggan, Tencent Cloud telah merancang dan menerapkan kerangka manajemen kelangsungan

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			bisnis yang sesuai dengan lingkungan komputasi awannya sendiri, serta telah memperoleh sertifikasi internasional ISO/IEC 22301 untuk Sistem Manajemen Kelangsungan Bisnis. Tencent Cloud melakukan analisis dampak bisnis terhadap produk dan layanan cloud, menetapkan target waktu pemulihan (Recovery Time Objective/RTO) dan target titik data pemulihan (Recovery Point Objective/RPO) untuk setiap bisnis, serta menyusun strategi respons dan rencana kelangsungan bisnis yang berbeda berdasarkan hasil analisis dampak bisnis. Rencana pemulihan bencana yang rinci juga telah disusun untuk produk cloud dan proses kritis. Tencent Cloud secara berkala melakukan uji latihan kelangsungan bisnis untuk produk cloud berdasarkan rencana kelangsungan bisnis, guna memastikan kelayakan rencana, prosedur, dan elemen lainnya. **Dalam hal pelanggan melaporkan masalah atau menghubungi** **Tencent Cloud secara aktif**, konsol resmi Tencent Cloud menyediakan layanan tiket yang mendukung pelanggan untuk melaporkan gangguan, insiden, masalah, dan keluhan terkait keamanan, ketersediaan, dan kerahasiaan. Tencent Cloud menyediakan layanan pelanggan online dan saluran telepon melalui konsol cloud serta situs web resminya untuk mendukung pelanggan

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			dalam memberikan umpan balik terkait masalah yang dihadapi saat menggunakan layanan Tencent Cloud. Tencent Cloud memiliki pusat layanan pelanggan dengan cadangan lintas wilayah yang mampu menangani permintaan pelanggan secara non-stop 7 * 24 jam, menyediakan dukungan teknis sepanjang waktu untuk produk cloud, serta respons dan penanganan layanan yang tepat waktu dan berkualitas tinggi. Pelanggan juga dapat memilih paket layanan yang sesuai untuk mendapatkan dukungan eksklusif yang terdiri dari grup dukungan khusus, manajer layanan teknis khusus, layanan bernilai tambah, dan komponen lainnya.
10	Tenaga Ahli	(1) Tenaga ahli yang digunakan oleh Penyelenggara Sistem Elektronik harus memiliki kompetensi di bidang Sistem Elektronik atau Teknologi Informasi. (2) Tenaga ahli sebagaimana dimaksud pada ayat (1) wajib memenuhi ketentuan peraturan perundang-undangan.	Sebagai penyelenggara sistem elektronik, pelanggan harus memastikan bahwa tenaga profesional yang dipekerjakan melalui proses pemeriksaan latar belakang, guna menjamin kompetensi mereka di bidang sistem elektronik atau teknologi informasi. Dalam rangka mendukung kepatuhan pelanggan terhadap persyaratan regulasi, Tencent Cloud telah membangun standar dan prosedur manajemen sumber daya manusia yang komprehensif secara internal, guna memastikan perekrutan dan penempatan personel sesuai dengan persyaratan posisi. Selama proses rekrutmen, Tencent Cloud melakukan pemeriksaan latar belakang

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			terhadap kandidat, termasuk verifikasi latar belakang pendidikan dan sertifikasi, guna memastikan kemampuan mereka memenuhi tanggung jawab posisi. Selain itu, Tencent Cloud secara internal telah membangun mekanisme pelatihan yang matang, menyediakan berbagai kursus pelatihan seperti pelatihan wajib untuk seluruh staf, pelatihan khusus untuk posisi kunci, serta pelatihan mata pelajaran pilihan, guna memastikan peningkatan berkelanjutan keahlian profesional karyawan.
11	Tata Kelola Sistem Elektronik	(1) Penyelenggara Sistem Elektronik harus menjamin: a. tersedianya perjanjian tingkat layanan; b. tersedianya perjanjian keamanan informasi terhadap jasa layanan Teknologi Informasi yang digunakan; dan c. keamanan informasi dan sarana komunikasi internal yang diselenggarakan. (2) Penyelenggara Sistem Elektronik sebagaimana dimaksud pada ayat (1) harus menjamin setiap komponen dan keterpaduan seluruh Sistem Elektronik beroperasi sebagaimana mestinya.	Sebagai penyelenggara sistem elektronik, pelanggan harus menyediakan perjanjian tingkat layanan (Service Level Agreement/SLA), menandatangani perjanjian keamanan informasi dengan penyedia layanan teknologi informasi yang digunakan, serta menjamin keamanan informasi fasilitas komunikasi dan memastikan sistem elektronik beroperasi normal sesuai yang diharapkan. Sebagai penyedia layanan cloud, Tencent Cloud menyediakan dokumen hukum secara online di situs web internasionalnya seperti KETENTUAN LAYANAN、General Service Level Agreement、Perjanjian Privasi dan Keamanan Data, yang secara jelas mengatur konten layanan dan tingkat layanan yang diberikan Tencent Cloud, perlindungan data pengguna dan kekayaan intelektual, serta tanggung jawab dan kewajiban

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			keamanan antara pelanggan dan Tencent Cloud. Pelanggan juga dapat memilih untuk menandatangani perjanjian offline dengan Tencent Cloud guna merundingkan klausul dan ketentuan dalam perjanjian tersebut. Selain itu，layanan cloud yang disediakan Tencent Cloud untuk pelanggan disampaikan berdasarkan Service Level Agreement (SLA) yang disepakati untuk setiap layanan. Indikator kinerja, standar pengukuran, serta persyaratan pelaporan untuk setiap layanan dijelaskan secara jelas dalam SLA setiap produk dan dipublikasikan di situs web resmi Tencent Cloud. Tencent Cloud secara berkelanjutan melacak kinerja dan ketersediaan layanan cloud, serta menyediakan pemantauan real-time bagi pelanggan melalui konsol manajemen.
12	Manajemen Risiko	Penyelenggara Sistem Elektronik harus menerapkan manajemen risiko terhadap kerusakan atau kerugian yang ditimbulkan.	Sebagai penyelenggara sistem elektronik, pelanggan harus menerapkan manajemen risiko guna memastikan bahwa risiko dapat dikelola dengan tepat dan tepat waktu ketika potensi gangguan atau kerugian muncul. Dalam rangka mendukung kepatuhan pelanggan terhadap persyaratan regulasi, Tencent Cloud telah menetapkan kerangka tata kelola risiko dan prosedur terkait, serta terus menyempurnakan langkah-langkah manajemen risiko dan sistem pemantauan internal.

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			Dengan secara berkelanjutan memperkuat budaya manajemen risiko, Tencent Cloud secara efektif meningkatkan kemampuan manajemen risiko internal, memastikan kesehatan dan keberlanjutan bisnis. Tencent Cloud telah membangun kerangka manajemen risiko yang komprehensif berdasarkan standar ISO/IEC 27001:2022， Tencent Cloud secara berkala melakukan penilaian risiko, mengidentifikasi risiko berdasarkan skenario risiko serta alur proses bisnis, produk, atau layanan. Terhadap risiko yang telah diidentifikasi, Tencent Cloud akan mengevaluasi kemungkinan terjadinya dan tingkat dampak setiap risiko untuk menentukan tingkat risiko, serta mengambil tindakan lanjutan yang sesuai. Seluruh aktivitas proses ini tercatat dengan baik. Tencent Cloud juga secara berkelanjutan melakukan tindak lanjut terhadap penanganan risiko, menilai risiko residual, dan memastikan bahwa pihak yang bertanggung jawab telah mengelola risiko dengan tepat sesuai dengan persyaratan manajemen risiko Tencent Cloud.
13	Kebijakan Tata Kelola	Penyelenggara Sistem Elektronik harus memiliki kebijakan tata kelola, prosedur kerja pengoperasian, dan mekanisme audit yang dilakukan berkala terhadap Sistem Elektronik.	Sebagai penyelenggara sistem elektronik, pelanggan harus menetapkan kebijakan tata kelola, prosedur, dan alur kerja operasional, serta secara berkala melakukan audit terhadap sistem elektronik. Guna mendukung kepatuhan pelanggan terhadap persyaratan

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			regulasi, Tencent Cloud telah menetapkan kebijakan manajemen keamanan informasi yang terdiri dari strategi keseluruhan keamanan informasi, struktur organisasi keamanan, dan sistem manajemen keamanan. Kebijakan ini secara efektif mendukung operasi yang aman dan manajemen risiko platform cloud. Kebijakan keamanan informasi Tencent Cloud ditinjau secara berkala setiap tahun untuk memastikan bahwa tujuan pengendalian, prosedur pengendalian, serta tindakan pengendalian sistem manajemen keamanan cloud sesuai dengan strategi keamanan, standar, prosedur, dan persyaratan hukum terkait, sehingga menjamin kecukupan dan efektivitas kebijakan keamanan informasi. Tim keamanan Tencent Cloud secara berkelanjutan memantau dan mengevaluasi risiko keamanan internal untuk menjaga efektivitas dan keandalan sistem manajemen keamanan informasi. Tim keamanan Tencent Cloud melakukan audit keamanan internal setidaknya sekali setahun, dan secara terus-menerus memantau kondisi platform cloud dan sistem internal, memastikan bahwa mereka mempertahankan postur keamanan yang baik dan mematuhi peraturan dan persyaratan standar manajemen keamanan serta peraturan perundang-undangan yang berlaku. Tencent Cloud juga menjalani audit

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			profesional oleh pihak ketiga independen setiap tahun. Melalui laporan Sistem dan Kontrol Organisasi (SOC) yang bersifat asersi, Tencent Cloud mengungkapkan kondisi terkini pengendalian internal organisasi layanannya kepada lembaga pengguna cloud, auditor independen, regulator, pemegang saham perusahaan, serta pihak-pihak terkait lainnya.
14	Data Pribadi	(1) Penyelenggara Sistem Elektronik wajib melaksanakan prinsip pelindungan Data Pribadi dalam melakukan pemrosesan Data Pribadi meliputi: a. pengumpulan Data Pribadi dilakukan secara terbatas dan spesifik, sah secara hukum, adil, dengan sepengetahuan dan persetqluan dari pemilik Data Pribadi; b. pemrosesan Data Pribadi dilakukan sesuai dengan tqiuannya; c. pemrosesan Data Pribadi dilakukan dengan menjamin hak pemilik Data Pribadi; d. pemrosesan Data Pribadi dilakukan secara alurat, lengkap, tidak menyesatkan, mutakhir, dapat dipertanggungjawabkan, dan memperhatikan tu-	Sebagai penyelenggara sistem elektronik, pelanggan harus mematuhi prinsip perlindungan data pribadi dalam memproses data pribadi. Pemrosesan data pribadi harus didasarkan pada persetujuan hukum yang diberikan oleh subjek data, dan ketika subjek data terkait mengajukan permintaan, informasi elektronik dan/atau dokumen elektronik yang tidak relevan lagi di bawah kendalinya harus dihapus. Jika terjadi kebocoran data pribadi, pelanggan wajib memberitahukan secara tertulis kepada subjek data yang terdampak. Untuk mendukung kepatuhan pelanggan terhadap persyaratan regulasi, **Dalam hal pemrosesan data pribadi dan perlindungan data pribadi**, Tencent Cloud menyediakan Kebijakan Privasi daring yang secara jelas menyatakan bahwa Tencent Cloud akan memproses data sesuai dengan hukum dan peraturan yang

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
		iuan pemrosesan Data Pribadi; e. pemrosesan Data Pribadi dilakukan dengan melindungi keamanan Data Pribadi dari kehilangan, penyalahgunaan, Akses dan pengungkapan yang tidak sah, serta pengubahan atau perusakan Data Pribadi; f. pemrosesan Data Pribadi dilakukan dengan memberitahukan tqiuan pengumpulan, aktivitas pemrosesan, dan kegagalan pelindungan Data Pribadi; dan g. pemrosesan Data Pribadi dimusnahkan dan/ atau dihapus kecuali masih dalam masa retensi sesuai dengan kebutuhan berdasarkan ketentuan peraturan perundang-undangan. (2) Pemrosesan Data Pribadi sebagaimana dimaksud pada ayat (1) meliputi: a. perolehan dan pengumpulan; b. pengolahan dan penganalisisan; c. penyimpanan; d. perbaikan dan pembaruan; e. penampilan,	berlaku selama penyediaan layanan Tencent Cloud serta dalam situasi lainnya. Berdasarkan hal ini, Tencent Cloud menganggap kepatuhan data pribadi sebagai faktor utama dalam proses penyediaan layanan, dan menjadikan prinsip-prinsip kepatuhan data pribadi yang diakui secara umum (seperti legalitas, keadilan, transparansi, pembatasan tujuan, minimalisasi data, integritas, akurasi, kerahasiaan, akuntabilitas, dll.) sebagai panduan kepatuhan privasi. Prinsip-prinsip ini diintegrasikan ke dalam setiap tahap desain dan pengembangan produk serta sepanjang siklus hidup data pribadi, menjadikan kepatuhan privasi sebagai atribut inheren dari produk. Selain itu, Tencent Cloud secara ketat mematuhi undang-undang perlindungan privasi di berbagai negara dan wilayah yang berlaku, dengan fokus utama pada manajemen siklus hidup lengkap data pribadi, serta mengintegrasikan persyaratan kepatuhan kunci seperti Privasi by Design (PbD), respons terhadap hak subjek data, dan pengungkapan data pribadi. Pengalaman dan akumulasi keamanan Tencent Cloud selama bertahun-tahun telah memastikan keamanan infrastruktur platform cloud dan memberikan fondasi yang kuat untuk kepatuhan privasi bisnis pelanggan. **Saat memperoleh persetujuan pelanggan untuk pemrosesan**

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
		pengumuman, transfer, penyebarluasan, atau pengungkapan; dan/ atau f. penghapusan atau pemusnahan. (3) Pemrosesan Data Pribadi harus memenuhi ketentuan adanya persetujuan yang sah dari pemilik Data Pribadi untuk 1 (satu) atau beberapa tujuan tertentu yang telah disampaikan kepada pemilik Data Pribadi. (4) Selain adanya persetujuan sebagaimana dimaksud pada ayat (3), pemrosesan Data Pribadi harus memenuhi ketentuan yang diperlukan untuk: a. pemenuhan kewajiban perjanjian dalam hal pemilik Data Pribadi merupakan salah satu pihak atau untuk memenuhi permintaan pemilik Data Pribadi pada saat akan melakukan perjanjian; b. pemenuhan kewajiban hukum dari pengendali Data Pribadi sesuai dengan ketentuan peraturan perundang-undangan; c. pemenuhan pelindungan	**data,** Tencent Cloud bertindak sebagai pengendali data (data controller) dengan mengumpulkan informasi yang diberikan pelanggan saat mendaftar layanan Tencent Cloud melalui situs web resmi, serta data yang dihasilkan selama interaksi dengan Tencent Cloud dalam proses tersebut. Dalam situasi ini, Tencent Cloud akan memenuhi kewajiban sebagai pengendali data sesuai dengan Kebijakan Privasi-nya. Sebagai pemroses data (data processor), pelanggan menggunakan produk atau layanan Tencent Cloud untuk memproses data yang dikumpulkan sesuai dengan tujuan bisnis mereka sendiri. Dalam hal ini, Tencent Cloud tidak hanya bertanggung jawab atas fungsionalitas dan keamanan produk atau layanan, tetapi juga memenuhi kewajiban terkait sebagai pemroses data berdasarkan Perjanjian Privasi dan Keamanan Data. Untuk penggunaan, penyimpanan, dan penghapusan data pribadi pelanggan, Tencent Cloud telah menjelaskan tujuan pengumpulan dan pemrosesan berbagai jenis data secara jelas melalui Kebijakan Privasi. Tencent Cloud tidak akan memproses data terkait dengan cara yang tidak sesuai dengan tujuan tersebut, serta telah menjelaskan mekanisme retensi untuk setiap jenis data, menetapkan periode penyimpanan data yang wajar sesuai dengan jenis

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
		kepentingan yang sah (uital interest) pemilik Data Pribadi; d. pelaksanaan kewenangan pengendali Data Pribadi berdasarkan ketentuan peraturan perundangundangan; e. pemenuhan kewajiban pengendali Data Pribadi dalam pelayanan publik untuk kepentingan umum; f. pemenuhan kepentingan yang sah lainnya dari pengendali Data Pribadi dan/atau pemilik Data Pribadi. (5) Jika terjadi kegagalan dalam pelindungan terhadap Data Pribadi yang dikelolanya, Penyelenggara Sistem Elektronik wajib memberitahukan secara tertulis kepada pemilik Data Pribadi tersebut. (6) Ketentuan mengenai teknis pemrosesan Data Pribadi diatur sesuai dengan ketentuan peraturan pemndangundangan.	data, dan Tencent Cloud tidak akan menyimpan data lebih lama dari periode yang diperlukan untuk mencapai tujuan atau sesuai dengan hukum yang berlaku. Jika pelanggan memberitahukan bahwa tujuannya telah tercapai atau periode retensi telah berakhir, Tencent Cloud akan menghapus data pelanggan terkait. Tencent Cloud telah memastikan akurasi data yang ditransmisikan melalui layanannya dengan menerapkan kontrol akses, verifikasi integritas, dan langkah-langkah lainnya. **Dalam hal respons terhadap hak subjek data,** dalam situasi yang wajar, Tencent Cloud dapat memenuhi permintaan subjek data pribadi untuk menghapus informasi terkait. Selain itu, Tencent Cloud juga menyediakan saluran komunikasi bagi pelanggan untuk mengidentifikasi hak subjek data yang sesuai dengan persyaratan hukum yang berlaku, termasuk namun tidak terbatas pada hak akses, hak koreksi, hak penghapusan, dan sebagainya, serta memberikan hak subjek data yang berlaku, sehingga pelanggan dapat secara mandiri memperbaiki atau menghapus data yang tidak akurat. Pelanggan dapat meminta dukungan yang diperlukan dari Tencent Cloud melalui email (cloudlegalnotices@tencentcom). **Untuk insiden keamanan yang**
15	Data Pribadi	(1) Setiap Penyelenggara Sistem Elektronik wajib menghapus Informasi Elektronik dan/atau Dokumen Elektronik yang tidak relevan yang	

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
		berada di bawah kendalinya atas permintaan orang yang bersanglmtan. (2) Kewajiban penghapusan Informasi Elektronik dan/atau Dokumen Elektronik yang tidak relevan sebagaimana dimaksud pada ayat (1) terdiri dari: a. penghapu san (right to erasurel; dan b. pengeluaran dari daftar mesin pencari. (3) Penyelenggara Sistem Elektronik yang wajib menghapus Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud pada ayat (1) merupakan Penyelenggara Sistem Elektronik yang memperoleh dan/atau memproses Data Pribadi di bawah kendalinya.	**mungkin memengaruhi** **pelanggan**, Tencent Cloud akan menilai cakupan dan tingkat dampak insiden keamanan informasi, dan setelah melalui tinjauan internal, hasil penanganan dan analisis insiden tersebut akan diberitahukan kepada pelanggan melalui saluran yang sesuai. Dukungan teknis juga akan disediakan untuk membantu pelanggan mengambil langkah perbaikan guna meminimalkan kerugian.
18	Data Pribadi	(1) Setiap Penyelenggara Sistem Elektronik wajib menyediakan mekanisme penghapusan Informasi Elektronik dan/ atau Dokumen Elektronik yang sudah tidak relevan sesuai dengan ketentuan peraturan perundang-undangan. (2) Mekanisme penghapusan	

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
		sebagaimana dimaksud pada ayat (1) paling sedikit memuat ketentuan mengenai: a. penyediaan saluran komunikasi antara Penyelenggara Sistem Elektronik dengan pemilik Data Pribadi; b. fitur penghapusan Informasi Elektronik dan/atau Dokumen Elektronik yang tidak relevan yang memungkinkan pemilik Data Pribadi melakukan penghapusan Data Pribadinya; dan c. pendataan atas permintaan penghapusan Informasi Elektronik dan/atau Dokumen Elektronik yang tidak relevan.	
19	Tata kelola Sebagaimana	(1) Penyelenggara Sistem Elektronik harus menerapkan tata kelota Sistem Elektronik yang baik dan akuntabel. (2) Tata kelola sebagaimana dimaksud pada ayat (1) paling sedikit memenuhi persyaratan: a. tersedianya prosedur atau petunjuk dalam penyelenggaraan Sistem Elektronik yang didokumentasikan	Sebagai penyelenggara sistem elektronik, pelanggan harus membangun sistem tata kelola sistem elektronik yang baik dan akuntabel, memastikan adanya prosedur atau pedoman tertulis yang diperbarui secara berkelanjutan, membentuk organisasi yang sesuai dengan staf yang memadai, serta menyusun rencana untuk menjamin keberlanjutan operasional sistem elektronik guna memastikan sistem berjalan sesuai yang diharapkan. Dalam rangka mendukung pelanggan memenuhi persyaratan

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
		dan/atau diumumkan dengan bahasa, informasi, atau simbol yang dimengerti oleh pihak yang terkait dengan penyelenggaraan Sistem Elektronik tersebut; b. adanya mekanisme yang berkelanjutan untuk menjaga kebaruan dan kejelasan prosedur pedoman pelaksanaan; c. adanya kelembagaan dan kelengkapan personel pendukung bagi pengoperasian Sistem Elektronik sebagaimana mestinya; d. adanya penerapan manajemen kinerja pada Sistem Elektronik yang. diselenggarakannya untuk memastikan Srstem Elektronik beroperasi sebagaimana mestinya; e. adanya rencana menjaga keberlangsungan penyelenggaraan Sistem Elektronik yang dikelolanya.	regulasi, **terkait sistem tata kelola sistem elektronik**, guna mendukung kepatuhan pelanggan terhadap persyaratan regulasi, Tencent Cloud telah menetapkan kebijakan manajemen keamanan informasi yang terdiri dari strategi keseluruhan keamanan informasi, struktur organisasi keamanan, dan sistem manajemen keamanan. Kebijakan ini secara efektif mendukung operasi yang aman dan manajemen risiko platform cloud. Kebijakan keamanan informasi Tencent Cloud ditinjau secara berkala setiap tahun untuk memastikan bahwa tujuan pengendalian, prosedur pengendalian, serta tindakan pengendalian sistem manajemen keamanan cloud sesuai dengan strategi keamanan, standar, prosedur, dan persyaratan hukum terkait, sehingga menjamin kecukupan dan efektivitas kebijakan keamanan informasi. Selain itu, layanan cloud yang disediakan Tencent Cloud untuk pelanggan disampaikan berdasarkan Service Level Agreement (SLA) yang disepakati untuk setiap layanan. Indikator kinerja, standar pengukuran, serta persyaratan pelaporan untuk setiap layanan dijelaskan secara jelas dalam SLA setiap produk dan dipublikasikan di situs web resmi Tencent Cloud. Prosedur operasional dan panduan

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			pengguna produk Tencent Cloud telah didokumentasikan dan disediakan bagi pelanggan melalui situs web resmi. Tencent Cloud juga menawarkan Tencent Cloud Training and Certification berbasis pengetahuan produk Tencent Cloud serta keahlian profesional terkait, guna meningkatkan kemampuan teknis dan penguasaan cloud pelanggan. **Untuk memastikan ketersediaan berkelanjutan dari bisnis pelanggan**, Tencent Cloud telah merancang dan menerapkan kerangka manajemen kelangsungan bisnis yang sesuai dengan lingkungan komputasi awannya sendiri, serta telah memperoleh sertifikasi internasional ISO/IEC 22301 untuk Sistem Manajemen Kelangsungan Bisnis. Tencent Cloud melakukan analisis dampak bisnis terhadap produk dan layanan cloud, menetapkan target waktu pemulihan (Recovery Time Objective/RTO) dan target titik data pemulihan (Recovery Point Objective/RPO) untuk setiap bisnis, serta menyusun strategi respons dan rencana kelangsungan bisnis yang berbeda berdasarkan hasil analisis dampak bisnis. Rencana pemulihan bencana yang rinci juga telah disusun untuk produk cloud dan proses kritis. Tencent Cloud secara berkala melakukan uji latihan kelangsungan bisnis untuk produk cloud berdasarkan rencana kelangsungan bisnis, guna

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			memastikan kelayakan rencana, prosedur, dan elemen lainnya.
20	Penyelenggara Sistem Elektronik Lingkup Publik	(1) Penyelenggara Sistem Elektronik Lingkup Publik wajib memiliki rencana keberlangsungan kegiatan untuk menanggulangi gangguan atau bencana sesuai dengan risiko dari dampak yang ditimbulkannya. (2) Penyelenggara Sistem Elektronik Lingkup Publik wajib melakukan pengelolaan, pemrosesan, dan/atau penyimpanan Sistem Elektronik dan Data Elektronik di wilayah Indonesia. (3) Penyelenggara Sistem Elektronik Lingkup Publik dapat melakukan pengelolaan, pemrosesan, dan/atau penyimpanan Sistem Elektronik dan Data Elektronik di luar wilayah Indonesia dalam hal teknologi penyimpanan tidak tersedia di dalam negeri. (6) Dalam hal Penyelenggara Sistem Elektronik Lingkup Pubtik menggunakan layanan pihak ketiga, Penyelenggara Sistem Elektronik Lingkup Publik	Sebagai Penyelenggara Sistem Elektronik Lingkup Publik, pelanggan harus menyusun rencana kelangsungan bisnis untuk menghadapi gangguan atau bencana yang mungkin terjadi. Pelanggan wajib mengelola, memproses, dan/atau menyimpan sistem elektronik serta data elektroniknya di dalam wilayah Indonesia. Jika teknologi penyimpanan di dalam negeri tidak tersedia, pengelolaan di luar negeri hanya dapat dilakukan setelah mendapatkan persetujuan dari komite yang terdiri dari lembaga negara terkait. Selain itu, jika pelanggan menggunakan layanan pihak ketiga, data harus diklasifikasikan berdasarkan risiko yang mungkin timbul. Dalam rangka mendukung pelanggan memenuhi persyaratan regulasi，untuk memastikan ketersediaan berkelanjutan dari bisnis pelanggan, Tencent Cloud telah merancang dan menerapkan kerangka manajemen kelangsungan bisnis yang sesuai dengan lingkungan komputasi awannya sendiri, serta telah memperoleh sertifikasi internasional ISO/IEC 22301 untuk Sistem Manajemen Kelangsungan Bisnis. Tencent Cloud melakukan analisis dampak bisnis terhadap produk dan layanan cloud, menetapkan target waktu pemulihan (Recovery Time Objective/RTO) dan target titik data

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
		wajib melakukan klasifikasi data sesuai risiko yang ditimbulkan.	pemulihan (Recovery Point Objective/RPO) untuk setiap bisnis, serta menyusun strategi respons dan rencana kelangsungan bisnis yang berbeda berdasarkan hasil analisis dampak bisnis. Rencana pemulihan bencana yang rinci juga telah disusun untuk produk cloud dan proses kritis. Tencent Cloud secara berkala melakukan uji latihan kelangsungan bisnis untuk produk cloud berdasarkan rencana kelangsungan bisnis, guna memastikan kelayakan rencana, prosedur, dan elemen lainnya. Untuk persyaratan bahwa Penyelenggara Sistem Elektronik Lingkup Publik harus mengelola, memproses, dan menyimpan data di dalam wilayah Indonesia, Tencent Cloud memiliki tiga pusat data di Indonesia yang menyediakan beragam layanan komputasi awan, termasuk server awan (cloud server), basis data awan (cloud database), penyimpanan awan (cloud storage), dan lainnya. Pelanggan di Indonesia dapat memilih untuk menyimpan dan memproses data mereka secara lokal di Indonesia. **Data Security Governance Center (DSGC)** dapat membantu pelanggan secara otomatis mengelola aset data, melakukan klasifikasi, serta menilai risiko keamanan data perusahaan di cloud. Layanan ini merupakan platform operasional keamanan data yang mengintegrasikan

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			deteksi dan klasifikasi data sensitif, pemetaan data, dan analisis akses data abnormal, serta berkolaborasi dengan berbagai kemampuan keamanan Tencent Cloud untuk membentuk jaringan perlindungan data tertutup. Hal ini membantu perusahaan memaksimalkan manfaat keamanan. Dengan izin dari perusahaan, DSGC terhubung mendalam dengan berbagai jenis aset data di cloud, memperoleh informasi aset data secara real-time dari dimensi inti. Berdasarkan karakteristik data, DSGC secara khusus membantu perusahaan mendeteksi data sensitif dan mengelola aset data dari perspektif keamanan. Sesuai standar klasifikasi data nasional, industri, atau perusahaan, DSGC membantu perusahaan melakukan klasifikasi data. Melalui visualisasi, perusahaan dapat melihat status keamanan aset dari berbagai dimensi seperti ikhtisar aset, klasifikasi data, hak akses akun, penyimpanan data, dan data sensitif. Tencent Cloud secara internal telah menetapkan standar klasifikasi dan penilaian tingkat data yang komprehensif. Data diklasifikasikan dan dinilai secara seragam sesuai standar ini sejak awal pembuatannya. Data pelanggan di dalam Tencent Cloud termasuk dalam kategori data dengan tingkat keamanan tinggi. Bagi karyawan internal Tencent Cloud, kecuali layanan yang dipilih pelanggan memerlukan pemrosesan data

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			pelanggan, karyawan Tencent Cloud tidak akan berusaha mengakses data pelanggan apa pun.
21	Penyelenggara Sistem Elektronik Lingkup Privat	(1) Penyelenggara Sistem Elektronik Lingkup Privat dapat melakukan pengelolaan, pemrosesan, dan/atau penyimpanan Sistem Elektronik dan Data Elektronik di wilayah Indonesia dan/atau di luar wilayah Indonesia. (2) Dalam hal Sistem Elektronik dan Data Elektronik dilakukan pengelolaan, pemrosesan, dan/atau penyimpanan di luar wilayah Indonesia, Penyelenggara Sistem Elektronik Lingkup Privat wajib memastikan efektivitas pengawasan oleh Kementerian atau Lembaga dan penegakan hukum. (3) Penyelenggara Sistem Elektronik Lingkup Privat wajib memberikan Akses terhadap Sistem Elektronik dan Data Elektronik dalam rangka pengawasan dan penegakan hukum sesuai dengan ketentuan peraturan perundangundangan. (4) Ketentuan mengenai	Sebagai Penyelenggara Sistem Elektronik Lingkup Privat, pelanggan dapat melakukan pengelolaan, pemrosesan, dan/atau penyimpanan sistem elektronik serta data elektronik di dalam atau di luar wilayah Indonesia. Jika pengelolaan dilakukan di luar negeri, pelanggan harus memastikan bahwa otoritas pengawas terkait dapat melaksanakan pengawasan yang efektif dan memberikan akses kepada otoritas tersebut terhadap sistem elektronik dan data elektroniknya. Untuk mendukung kepatuhan pelanggan terhadap persyaratan regulasi, Tencent Cloud memiliki tiga pusat data di Indonesia yang menyediakan beragam layanan komputasi awan, termasuk server awan (cloud server), basis data awan (cloud database), penyimpanan awan (cloud storage), dan lainnya. Pelanggan di Indonesia dapat memilih untuk menyimpan dan memproses data mereka secara lokal di Indonesia. **Jika pelanggan perlu memberikan akses ke sistem elektronik atau data elektronik kepada regulator**, pelanggan dapat menggunakan **Cloud Object Storage (COS)** yang disediakan oleh Tencent Cloud.

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
		pengelolaan, pemrosesan, dan penyimpanan Sistem Elektronik dan Data Elektronik bagi Penyelenggara Sistem Elektronik Lingkup Privat di sektor keuangan diatur lebih lanjut oleh otoritas pengatur dan pengawas spktor keuangan.	Layanan ini merupakan penyimpanan terdistribusi untuk file berskala besar, memungkinkan pengguna menyimpan dan melihat data kapan saja melalui jaringan. Pengguna dapat mengelola hak akses ke bucket dan objek. Ketika menerima permintaan untuk suatu sumber daya, COS akan memeriksa Access Control List (ACL) yang relevan untuk memverifikasi apakah peminta memiliki hak akses yang diperlukan. Setelah akun sub-Tencent Cloud dibuat, pengguna dapat memberikan otorisasi kepada akun sub melalui kebijakan akses; jika perlu membuka sumber daya kepada pengguna non-Tencent Cloud, hal ini dapat dilakukan dengan mengatur izin publik (baca publik) pada sumber daya (bucket, objek, direktori). Melalui fungsi-fungsi di atas, pelanggan dapat memberikan data elektronik kepada regulator sesuai persyaratan untuk diakses. Selain itu, Tencent Cloud berkomitmen untuk melindungi keamanan data pelanggan global dan mematuhi hukum dan peraturan yang berlaku di negara atau wilayah tempat bisnis beroperasi. Pelanggan memiliki kepemilikan dan kendali tunggal atas konten data mereka sendiri. Data pelanggan di dalam Tencent Cloud dikategorikan sebagai data dengan tingkat keamanan tinggi. Kecuali untuk keperluan penyediaan layanan atau pemecahan masalah, dan setelah

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			mendapatkan otorisasi eksplisit dari pelanggan, atau dalam situasi seperti investigasi peristiwa kriminal oleh otoritas pemerintah nasional atau lokal yang sesuai dengan peraturan perundang-undangan, karyawan internal Tencent Cloud tidak akan secara aktif mengakses data pelanggan mana pun.
22	Rekam Jejak Audit Terhadap	(1) Penyelenggara Sistem Elektronik wajib menyediakan rekam jejak audit terhadap seluruh kegiatan penyelenggaraan Sistem Elektronik. (2) Rekam jejak audit sebagaimana dimaksud pada ayat (1) digunakan untuk keperluan pengawasan, penegakan hukum, penyelesaian sengketa, verifikasi, pengujian, dan pemeriksaan lainnya.	Sebagai penyelenggara sistem elektronik, pelanggan harus menyimpan catatan jejak audit untuk seluruh aktivitas operasional sistem elektronik dan menyediakannya ketika diperlukan oleh otoritas pengawas. Tencent Cloud menyediakan **Cloud Log Service (CLS)**. Sebagai platform layanan log terpadu, CLS menawarkan berbagai layanan mulai dari pengumpulan log, penyimpanan log, hingga pencarian dan analisis log, konsumsi real-time, serta pengiriman log. Layanan ini membantu pelanggan menyelesaikan berbagai masalah seperti operasi bisnis, pemantauan keamanan, audit log, dan analisis log. **Cloud Security Center (CSC)** juga mendukung pengumpulan berbagai data keamanan cloud, seperti data peringatan dari produk keamanan cloud, data perubahan konfigurasi aset cloud, data perilaku operasional pengguna di cloud, serta data log dari beberapa produk cloud. Layanan ini

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			menyediakan platform pencarian dan investigasi terpadu untuk membantu pelanggan mencapai audit dan investigasi log cloud yang komprehensif. Selain itu, **Elasticsearch Service (ES)** mengumpulkan dan mentransmisikan log real-time dari cloud server, kontainer, serta produk cloud lainnya, atau data bisnis yang ada dan yang bertambah, ke kluster ES Tencent Cloud untuk penyimpanan terdistribusi, pencarian, dan analisis data. Untuk mendukung kepatuhan pelanggan terhadap persyaratan regulasi, Tencent Cloud telah menetapkan standar dan mekanisme pengumpulan serta pengelolaan log, yang mengontrol pencatatan, ekstraksi, penyimpanan, perlindungan, analisis, dan audit berbagai jenis log seperti log masuk, log operasi, log sistem rutin, dan log insiden keamanan sistem. Tujuannya adalah untuk mendeteksi dan mencegah aktivitas sistem yang tidak normal serta potensi risiko. Semua log dikonsolidasikan ke dalam Platform Manajemen Log Tencent Cloud untuk dikelola secara terpusat, dengan menerapkan langkah-langkah pencadangan dan perlindungan ketat terhadap informasi log terkait guna mencegah modifikasi atau penghapusan tanpa izin. Tencent Cloud melakukan audit log menggunakan alat audit

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			otomatisasi keamanan operasional dan tim audit internal untuk mendeteksi anomali sistem atau operasi, sehingga mengurangi risiko operasional.
24	Pengamanan Penyelenggaraan Sistem Elektronik	(1) Penyelenggara Sistem Elektronik wajib memiliki dan menjalankan prosedur dan sarana untuk pengamanan Sistem Elektronik dalam menghindari gangguan, kegagalan, dan kerugian. (2) Penyelenggara Sistem Elektronik wajib menyediakan sistem pengamanan yang mencakup prosedur dan sistem pencegahan dan penanggulangan terhadap ancaman dan serangan yang menimbulkan gangguan, kegagalan, dan kerugian. (3) Dalam hal terjadi kegagalan atau gangguan sistem yang berdampak serius sebagai akibat perbuatan dari pihak lain terhadap Sistem Elektronik, Penyelenggara Sistem Elektronik wajib mengamankan Informasi Elektronik dan/atau Dokumen Elektronik dan segera melaporkan dalam kesempatan pertama kepada aparat penegak hukum dan Kementerian atau	Sebagai penyelenggara sistem elektronik, pelanggan harus menetapkan dan menerapkan langkah-langkah perlindungan keamanan sistem elektronik untuk mencegah sistem dari gangguan, malfungsi, dan kerugian, serta membangun sistem keamanan untuk mencegah dan menanggapi ancaman serta serangan. Ketika terjadi insiden serius pada sistem akibat tindakan pihak ketiga, pelanggan harus segera melindungi informasi elektronik dan melaporkannya kepada otoritas pengawas secepatnya. **Untuk mencegah sistem dari ancaman dan serangan**, Tencent Cloud menyediakan **EdgeOne (EO) platform** untuk pelanggan. Berbasis pada simpul global Tencent Edge, layanan ini memberikan perlindungan keamanan dan layanan percepatan kepada pelanggan, dengan kemampuan seperti perlindungan DDoS, perlindungan Web cerdas, perlindungan serangan BOT/crawler, resolusi DNS, serta dukungan bagi pelanggan untuk mengonfigurasi aturan kontrol akses kustom sesuai kebutuhan bisnis. Pelanggan juga dapat

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
		Lembaga terkait.	memilih alat perlindungan batas jaringan seperti Cloud Firewall, Web Application Firewall (WAF), dan Anti-DDoS. Di antaranya, **Cloud Firewall (CFW)** terutama menyediakan perlindungan di berbagai batas jaringan untuk pelanggan. Layanan ini mendukung fungsi seperti kontrol aktif ACL firewall, penyaringan IPS real-time, patching virtual, dan deteksi kode berbahaya. Dengan kemampuan ini, CFW dapat memenuhi kebutuhan zona DMZ dalam jaringan tradisional, memberikan perlindungan fokus pada aset inti, serta mencapai kontrol isolasi granular antar VPC. **Web Application Firewall (WAF)** membantu pengguna di dalam maupun di luar Tencent Cloud dalam menangani masalah keamanan situs web dan layanan web, seperti serangan web, intrusi, eksploitasi kerentanan, injeksi malware, pemalsuan, backdoor, dan serangan crawler. Sementara itu, **Anti-DDoS** mengatasi masalah serangan DDoS dengan memanfaatkan sumber daya perlindungan DDoS yang memadai dan berkualitas tinggi, dikombinasikan dengan algoritma pembersihan yang terus berkembang berbasis "teknologi mandiri + identifikasi cerdas AI". **Untuk mendukung pelanggan**

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			dalam mendeteksi dan menganalisis ancaman, Tencent Cloud menyediakan **Threat Intelligence Center (TIX)**. Sebagai platform layanan intelijen terpadu, TIX menyediakan tiga kemampuan intelijen utama: intelijen dasar, intelijen permukaan serangan, dan intelijen bisnis. Platform ini mendukung fungsi seperti kueri intelijen, analisis dan penilaian IOC, serta manajemen permukaan serangan. Kemampuan ini membantu pelanggan menganalisis dan menilai insiden keamanan dengan lebih efisien, serta menilai risiko paparan aset perusahaan secara lebih komprehensif, sehingga mendukung pembangunan sistem pertahanan keamanan multidimensi yang efektif. TIX membangun jaringan titik kontak intelijen yang lengkap, mengumpulkan dan menganalisis intelijen ancaman dari berbagai sumber seperti komunitas kerentanan, lembaga keamanan, penyedia alat keamanan, media sosial, dan blog keamanan. Platform ini juga terintegrasi dengan algoritma dan daya komputasi cloud untuk menghilangkan alarm palsu, sehingga memastikan keakuratan intelijen. **Dalam hal pengendalian dan pengelolaan keamanan jaringan,** Tencent Cloud secara internal telah

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			membangun standar manajemen keamanan jaringan dan sistem pertahanan berlapis jaringan. Melalui kebijakan dan prosedur manajemen, Tencent Cloud menetapkan standar kontrol dan perlindungan keamanan jaringan serta peran dan tanggung jawab yang sesuai, guna memastikan operasi yang aman dari layanan yang dijalankan di atas jaringan Tencent Cloud. Secara bersamaan, Tencent Cloud menerapkan arsitektur keamanan jaringan yang matang, yang meliputi mekanisme perlindungan berlapis seperti firewall, sistem deteksi/pencegahan intrusi (IDS/IPS), perlindungan DDoS, isolasi logis jaringan, dan keamanan aplikasi web. Mekanisme ini secara aktif mendeteksi, menyaring, dan memblokir lalu lintas jaringan berbahaya untuk melindungi keamanan jaringan Tencent Cloud. Berdasarkan dukungan dan pemberdayaan dari Threat Intelligence Center, Tencent Cloud berkomitmen untuk membangun sistem kemampuan keamanan pertahanan proaktif yang mencakup "intelijen - serangan dan pertahanan - manajemen - perencanaan". Dengan mengintegrasikan teknologi seperti intelijen ancaman, kecerdasan buatan, dan big data, Tencent Cloud meningkatkan kemampuan dan efisiensi respons terhadap insiden keamanan. Pusat operasi keamanan 7*24 jam juga telah

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			didirikan, yang berfokus pada deteksi, investigasi, dan respons ancaman, guna mencapai visibilitas, keterlihatan, dan kendali yang jelas atas postur keamanan. **Untuk insiden keamanan yang berpotensi memengaruhi pelanggan**, Tencent Cloud akan menilai cakupan dan tingkat dampak insiden keamanan informasi, kemudian setelah melalui tinjauan internal, hasil penanganan dan analisis insiden tersebut akan disampaikan kepada pelanggan melalui saluran yang sesuai. Dukungan teknis juga akan disediakan untuk membantu pelanggan mengambil langkah perbaikan guna meminimalkan kerugian.
25	Penyimpanan Informasi Elektronik	Penyelenggara Sistem Elektronik wajib menampilkan kembali Informasi Elektronik dan/ atau Dokumen Elektronik secara utuh sesuai dengan format dan masa retensi yang ditetapkan berdasarkan kdtentuan peraturan perundang-undangan.	Sebagai penyelenggara sistem elektronik, pelanggan harus melindungi ketersediaan, integritas, kerahasiaan, keaslian, serta aksesibilitas informasi elektronik selama proses operasional sistem elektronik, dan memperjelas periode penyimpanan yang diwajibkan oleh hukum. **Dalam hal perlindungan akses data,** data pelanggan di dalam Tencent Cloud termasuk dalam kategori data dengan tingkat keamanan tinggi. Hak kontrol atas data pelanggan sepenuhnya dipegang oleh pelanggan, dan Tencent Cloud tidak akan berusaha mengakses atau mengungkapkan konten pelanggan. Tencent Cloud
26	Penyimpanan Informasi Elektronik	(1) Penyelenggara Sistem Elektronik wajib menjaga kerahasiaan, keutuhan, keautentikan, keteraksesan, ketersediaan, dan dapat ditelusurinya suatu Informasi Elektronik	

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
		dan/atau Dokumen Elektronik sesuai dengan ketentuan peraturan perundang-undangan. (2) Dalam penyelenggaraan Sistem Elektronik yang ditujukan untuk Informasi Elektronik dan/atau Dokumen Elektronik yang dapat dipindahtangankan, Informasi Elektronik dan/atau Dokumen Elektronik harus unik serta menjelaskan penguasaan dan kepemilikannya.	secara internal telah menetapkan standar manajemen kontrol akses dan membangun mekanisme manajemen serta otorisasi hak akses. Lingkungan produksi Tencent Cloud telah sepenuhnya menggunakan bastion host, yang melakukan kontrol terpusat atas hak akses akun administrator dan aktivitas akun pada komponen sistem backend Tencent Cloud. Untuk memastikan kerahasiaan dan integritas data pelanggan，**Dalam hal perlindungan penyimpanan data**，berbagai produk penyimpanan dan basis data Tencent Cloud mendukung fungsi enkripsi data. Layanan ini menggunakan algoritma enkripsi yang aman dan kuat, serta mengintegrasikan **Key Management Service (KMS)** untuk mengelola siklus hidup kunci secara menyeluruh, sehingga menjamin kerahasiaan data. Selain itu, Tencent Cloud menggunakan teknologi penyimpanan redundan multi-salinan dan kode penghapusan saat menyimpan data, serta segera mengambil tindakan pemulihan yang diperlukan ketika mendeteksi kesalahan integritas, sehingga sangat meningkatkan kemampuan toleransi kesalahan data. **Dalam hal pencadangan data, untuk data pelanggan di cloud,** Tencent Cloud menyediakan

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			beberapa salinan penyimpanan dan layanan pencadangan berdasarkan fungsionalitas produk atau layanan cloud, serta bertanggung jawab atas layanan pencadangan data yang diberikan sesuai dengan kesepakatan dalam Service Level Agreement (SLA) produk. Sebagai penyedia layanan cloud, Tencent Cloud menyediakan dokumen hukum secara online di situs web internasionalnya seperti KETENTUAN LAYANAN、General Service Level Agreement、Perjanjian Privasi dan Keamanan Data, yang secara jelas mengatur konten layanan dan tingkat layanan yang diberikan Tencent Cloud, perlindungan data pengguna dan kekayaan intelektual, serta tanggung jawab dan kewajiban keamanan antara pelanggan dan Tencent Cloud. Ketika pelanggan perlu mengakhiri perjanjian kontrak karena perubahan bisnis atau perencanaan TI di masa depan, pelanggan dapat memilih untuk melakukan pencadangan dan migrasi data cloud serta lingkungan produksi kapan saja. Setelah layanan cloud diakhiri, Tencent Cloud akan mengikuti metode penghapusan data yang ketat dan menghapus sepenuhnya data pelanggan, termasuk salinan dan cadangannya, setelah periode retensi berakhir. Data yang telah dihapus tidak dapat dipulihkan.
28	Pelatihan Pengguna	(1) Penyelenggara Sistem Elektronik wajib melakukan edukasi	Sebagai penyelenggara sistem elektronik, pelanggan harus menyediakan pelatihan kepada

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
		kepada Pengguna Sistem Elektronik. (2) Edukasi sebagaimana dimaksud pada ayat (1) paling sedikit mengenai hak, kewajiban, dan tanggung jawab seluruh pihak terkait, serta prosedur pengajuan komplain.	pengguna, yang mencakup hak, kewajiban, dan tanggung jawab pihak terkait serta prosedur pengaduan. Selain itu, pelanggan juga harus mengungkapkan informasi seperti identitas penyelenggara, keamanan sistem, ketentuan kontrak, kebijakan perlindungan data pribadi, cara pengaduan, dan sebagainya kepada pengguna, serta memberikan kejelasan kepada pengguna mengenai kewenangan, kewajiban, dan tanggung jawab masing-masing pihak terkait. Sebagai penyedia layanan cloud, Tencent Cloud menyediakan dokumen hukum secara online di situs web internasionalnya seperti KETENTUAN LAYANAN、General Service Level Agreement、Perjanjian Privasi dan Keamanan Data, yang secara jelas mengatur konten layanan dan tingkat layanan yang diberikan Tencent Cloud, perlindungan data pengguna dan kekayaan intelektual, serta tanggung jawab dan kewajiban keamanan antara pelanggan dan Tencent Cloud. Pelanggan juga dapat memilih untuk menandatangani perjanjian offline dengan Tencent Cloud guna merundingkan klausul dan ketentuan dalam perjanjian tersebut. Selain itu, dalam Kebijakan Privasi daring Tencent Cloud, dijelaskan secara jelas jenis informasi pribadi apa yang dikumpulkan oleh Tencent Cloud, bagaimana
29	Pengungkapan Informasi	Penyelenggara Sistem Elektronik wajib menyampaikan informasi kepada Pengguna Sistem Elektronik paling sedikit mengenai: a. identitas Penyelenggara Sistem Elektronik; b. objek yang ditransaksikan; c. kelaikan atau keamanan Sistem Elektronik; d. tata cara penggunaan perangkat; e. syarat kontrak; f. prosedur mencapai kesepakatan; g. jaminan privasi dan/atau pelindungan Data Pribadi; dan h. nomor telepon pusat pengaduan.	

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			informasi pribadi yang dikumpulkan digunakan, dengan siapa informasi pribadi yang dikumpulkan dibagikan, di mana informasi pribadi yang dikumpulkan diproses, berapa lama informasi pribadi yang dikumpulkan disimpan, serta bagaimana pengguna dapat menggunakan hak mereka atas informasi mereka sendiri. Prosedur operasional dan panduan pengguna produk Tencent Cloud telah didokumentasikan dan disediakan bagi pelanggan melalui situs web resmi. Tencent Cloud juga menawarkan Tencent Cloud Training and Certification berbasis pengetahuan produk Tencent Cloud serta keahlian profesional terkait, guna meningkatkan kemampuan teknis dan penguasaan cloud pelanggan.
32	Pelatihan Personel	(1) Setiap orang yang bekerja di lingkungan penyelenggaraan Sistem Elektronik wajib mengamankan dan melindungi sarana dan prasarana Sistem Elektronik atau informasi yang disalurkan melalui Sistem Elektronik. (2) Penyelenggara Sistem Elektronik wajib menyediakan, mendidik, dan melatih personel yang bertugas dan bertanggung jawab terhadap pengamanan dan pelindungan sarana	Pelanggan harus memberikan pelatihan dan pendidikan kepada personel yang terlibat dalam lingkungan operasional sistem elektronik, untuk melindungi dan menjaga fasilitas serta infrastruktur sistem elektronik, serta informasi yang ditransmisikan oleh sistem elektronik. Dalam rangka mendukung pelanggan memenuhi persyaratan regulasi, Tencent Cloud melindungi data pelanggan dengan menerapkan kontrol akses dan manajemen izin, serta menandatangani perjanjian kerahasiaan dengan karyawan. Selain itu, Tencent Cloud secara

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
		dan prasarana Sistem Elektronik.	internal telah membangun mekanisme pelatihan keamanan informasi yang komprehensif. Tencent Cloud mewajibkan karyawan tetap, konsultan, magang, dan karyawan outsourcing untuk mengikuti kursus pelatihan keamanan informasi. Kursus-kursus terkait mencakup pelatihan wajib untuk semua staf, pelatihan khusus untuk posisi kunci, serta pelatihan mata pelajaran pilihan. Materi yang diajarkan meliputi aspek-aspek seperti kesadaran keamanan dasar, keamanan kantor, identifikasi dan pertahanan kerentanan, perlindungan privasi, tanggap darurat, standar keamanan pengembangan, dan persyaratan keamanan data. Tencent Cloud secara konsisten mengintegrasikan manajemen keamanan informasi ke dalam pekerjaan manajemen sehari-hari, memastikan bahwa karyawan memahami dan mematuhi kebijakan serta persyaratan keamanan informasi internal.
33	Penyediaan Informasi Elektronik untuk Penyidikan Pidana	Untuk keperluan proses peradilan pidana, Penyelenggara Sistem Elektronik wajib memberikan Informasi Elektronik dan/atau Data Elektronik yang terdapat di dalam Sistem Elektronik atau Informasi Elektronik dan/ atau Data Elektronik yang dihasilkan oleh Sistem Elektronik atas	Sebagai penyelenggara sistem elektronik, pelanggan harus memastikan penyediaan informasi atau data elektronik yang disimpan dalam sistem elektroniknya kepada penyidik yang mengajukan permintaan sah untuk keperluan penyidikan pidana. Tencent Cloud berkomitmen untuk melindungi keamanan data pelanggan global dan mematuhi hukum dan peraturan yang berlaku di negara atau wilayah tempat

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
		permintaan yang sah dari penyrdik untuk tindak pidana tertentu sesuai dengan kewenangan yang diatur dalam undang-undang.	bisnis beroperasi. Pelanggan memiliki kepemilikan dan kendali tunggal atas konten data mereka sendiri. Data pelanggan di dalam Tencent Cloud dikategorikan sebagai data dengan tingkat keamanan tinggi. Kecuali untuk keperluan penyediaan layanan atau pemecahan masalah, dan setelah mendapatkan otorisasi eksplisit dari pelanggan, atau dalam situasi seperti investigasi peristiwa kriminal oleh otoritas pemerintah nasional atau lokal yang sesuai dengan peraturan perundang-undangan, karyawan internal Tencent Cloud tidak akan secara aktif mengakses data pelanggan mana pun.
34	Uji Kelaikan Sistem Elektronik	(1) Penyelenggara Sistem Elektronik wajib melakukan Uji Kelaikan Sistem Elektronik. (2) Kewajiban sebagaimana dimaksud pada ayat (1) dapat dilaksanakan terhadap seluruh komponen atau sebagian komponen dalam Sistem Elektronik sesuai dengan karakteristik kebutuhan pelindungan dan sifat strategis penyelenggaraan Sistem Elektronik.	Sebagai penyelenggara sistem elektronik, pelanggan harus melakukan uji kelayakan terhadap sistem elektroniknya. Setelah tim pengembangan Tencent Cloud menyelesaikan pengembangan produk baru atau ketika produk mengalami perubahan signifikan, personel penguji menyusun rencana pengujian dan kasus uji yang sesuai berdasarkan kebutuhan produk, serta mengorganisir tim proyek untuk meninjau kasus uji tersebut. Setelah kasus uji dikonfirmasi, tim pengujian melakukan pengujian fungsional pada produk proyek untuk memastikan fungsionalitas produk tersedia, andal, dan memenuhi persyaratan kualitas produk yang ditetapkan secara internal oleh Tencent Cloud. Setelah

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			pengujian fungsional selesai, tim keamanan melakukan pengujian keamanan pada produk. Cacat atau kerentanan yang ditemukan selama proses pengujian ditangani sesuai dengan alur manajemen kerentanan internal Tencent Cloud. Personel penguji menghasilkan laporan pengujian berdasarkan hasil pengujian dan menyerahkannya kepada berbagai tim terkait untuk konfirmasi.

07

BagaimanaTencent Cloud Membantu Mematuhi dan Mendukung Pelanggan Dalam Memenuhi Penyelenggara Sistem Elektronik Lingkup Privat Beserta Perubahannya

Untuk mengatur penyelenggara sistem elektronik lingkup privat dan melaksanakan NOMOR 71 TAHUN 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik, Kementerian Komunikasi dan Informatika Republik Indonesia menetapkan Nomor 5 Tahun 2020 Tentang Penyelenggara Sistem Elektronik Lingkup Privat pada tahun 2020. Peraturan ini memperjelas persyaratan pendaftaran bagi penyelenggara sistem elektronik lingkup privat, tata kelola dan peninjauan konten informasi serta dokumen elektronik, prosedur pengajuan pemutusan akses jaringan untuk konten ilegal, serta pemberian akses terhadap sistem elektronik dan data elektronik untuk kepentingan penegakan hukum pidana. Pada tahun 2021, Kementerian Komunikasi dan Informatika Republik Indonesia lebih lanjut menerbitkan Nomor 10 Tahun 2021 , yang mengubah Peraturan Menteri Nomor 5 Tahun 2020.

Dalam bab ini, Tencent Cloud akan menyaring dan merangkum persyaratan kontrol yang terkait dengan penyedia layanan cloud dalam Nomor 5 Tahun 2020 beserta perubahannya, serta menjelaskan bagaimana Tencent Cloud, sebagai penyedia layanan cloud, dapat membantu penyelenggara sistem elektronik lingkup privat mematuhi persyaratan terkait.

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
2	Pendaftaran Penyelenggara Sistem Elektronik Lingkup Privat	(1) Setiap PSE Lingkup Privat wajib melakukan pendaftaran. (3) Kewajiban melakukan pendaftaran bagi PSE Lingkup Privat dilakukan sebelum Sistem Elektronik mulai digunakan oleh Pengguna Sistem Elektronik. (4) Pendaftaran ISP[7]	Sebagai penyelenggara sistem elektronik lingkup privat, pelanggan harus melakukan pendaftaran dan mematuhi norma, standar, serta prosedur yang ditetapkan dalam peraturan. Sebagai penyedia layanan cloud, Tencent Cloud juga telah menyerahkan dokumen yang diperlukan untuk pendaftaran kepada otoritas pengawas setempat di Indonesia dan menyelesaikan proses registrasi

[7] Penyelenggara Jasa Akses Internet (Internet Service Provider) yang selanjutnya disingkat ISP adalah

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
		sebagai PSE Lingkup Privat dilaksanakan melalui perizinan yang diselenggarakan oleh Kementerian sesuai dengan ketentuan peraturan perundang-undangan.	sebagai penyelenggara sistem elektronik lingkup privat.
9	Tata Kelola dan Tinjauan Konten Informasi dan/atau Dokumen Elektronik	(1) PSE Lingkup Privat bertanggung jawab atas penyelenggaraan Sistem Elektronik dan pengelolaan Informasi Elektronik dan/atau Dokumen Elektronik di dalam Sistem Elektronik secara andal, aman, dan bertanggung jawab. (2) PSE Lingkup Privat wajib menyediakan petunjuk penggunaan layanan dalam bahasa Indonesia sesuai dengan ketentuan perundang-undangan. (3) PSE Lingkup Privat wajib memastikan: a. Sistem Elektroniknya tidak memuat Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang; dan b. Sistem Elektroniknya tidak memfasilitasi penyebarluasan Informasi Elektronik dan/atau Dokumen	Sebagai penyelenggara sistem elektronik lingkup privat, pelanggan harus memastikan keamanan dan stabilitas sistem elektroniknya, serta menyediakan petunjuk penggunaan layanan dalam bahasa Indonesia sesuai ketentuan hukum. Selain itu, pelanggan harus memastikan bahwa sistem elektronik tidak mengandung atau menyebarkan informasi dan/atau dokumen yang melanggar aturan. Tencent Cloud, dengan memegang prinsip keterbukaan dan berbagi dalam layanan komputasi awan, terus meningkatkan kemampuan keamanan platform dan layanan cloud, serta bersama-sama dengan pelanggan membangun sistem perlindungan keamanan yang lebih baik dan lebih lengkap untuk bisnis dan data di cloud. Tencent Cloud secara ketat mematuhi hukum dan peraturan terkait keamanan siber, privasi pengguna, serta keamanan data di yurisdiksi tempat operasi bisnis berlangsung, guna menjamin keamanan cloud. Sebagai penyelenggara sistem elektronik lingkup privat, Tencent Cloud menyediakan situs web resmi,

penyelenggara jasa multimedia yang menyelenggarakan jasa layanan akses internet untuk terhubung dengan jaringan internet publik.

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
		Elektronik yang dilarang. (4) Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang sebagaimana dimaksud pada ayat (3) dengan klasifikasi: a. melanggar ketentuan peraturan perundangundangan; b. meresahkan masyarakat dan mengganggu ketertiban umum; dan c. memberitahukan cara atau menyediakan akses terhadap Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang. (5) Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang sebagaimana dimaksud pada ayat (4) huruf b ditetapkan oleh Kementerian atau Lembaga sesuai dengan ketentuan peraturan perundang-undangan. (6) PSE Lingkup Privat yang tidak melakukan kewajiban sebagaimana dimaksud pada ayat (3) diputus akses terhadap Sistem Elektroniknya (access blocking) sesuai dengan ketentuan dalam Peraturan Menteri ini.	ketentuan layanan, perjanjian pemrosesan dan keamanan data, kebijakan privasi, dan dokumen lainnya dalam versi bahasa lokal bagi pelanggan di Indonesia. Selain itu, Tencent Cloud menyediakan Acceptable Use Policy secara daring yang menetapkan aturan perilaku yang baik yang berlaku bagi pelanggan dalam menggunakan Tencent Cloud. Pelanggan tidak dapat, tidak diizinkan, atau menyebabkan siapa pun (termasuk pengguna akhir) untuk melakukan atau mendorong kegiatan terlarang berikut di Tencent Cloud atau terkait dengan Tencent Cloud, termasuk: melanggar ketentuan layanan Tencent Cloud; menggunakan Tencent Cloud dengan cara atau tujuan yang melanggar ketentuan layanan Tencent Cloud atau ketentuan layanan produk atau layanan Tencent lainnya; penggunaan atau konten yang ilegal, berbahaya, atau menyinggung; serta yang mengandung kerentanan keamanan atau penyalahgunaan jaringan.

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
10	Kewajiban Penyelenggara Sistem Elektronik Lingkup Privat User Generated Content	(1) Dalam rangka memenuhi kewajiban sebagaimana dimaksud dalam Pasal 9 ayat (3), PSE Lingkup Privat User Generated Content wajib: a. memiliki tata kelola mengenai Informasi Elektronik dan/atau Dokumen Elektronik; b. menyediakan sarana pelaporan. (2) Tata kelola sebagaimana dimaksud pada ayat (1) huruf a paling sedikit memuat ketentuan sebagai berikut: a. kewajiban dan hak Pengguna Sistem Elektronik dalam menggunakan layanan Sistem Elektronik; b. kewajiban dan hak PSE Lingkup Privat dalam melaksanakan operasional Sistem Elektronik; c. ketentuan mengenai pertanggungjawaban terhadap Informasi Elektronik dan/atau Dokumen Elektronik yang diunggah Pengguna Sistem Elektronik; dan d. ketersediaan sarana dan layanan serta	Sebagai PSE Lingkup Privat User Generated Content, pelanggan harus memastikan bahwa sistem elektronik membangun tata kelola keamanan informasi elektronik, dengan memperjelas kewajiban dan hak pengguna sistem elektronik dalam menggunakan layanan sistem elektronik, kewajiban dan hak operator sistem elektronik swasta dalam menjalankan operasi sistem elektronik, ketentuan tanggung jawab pengguna sistem elektronik dalam mengunggah informasi/dokumen, serta penanganan keluhan dan penyelesaian sengketa. Sebagai penyedia layanan cloud, Tencent Cloud menyediakan dokumen hukum secara online di situs web internasionalnya seperti KETENTUAN LAYANAN、General Service Level Agreement、Perjanjian Privasi dan Keamanan Data, yang secara jelas mengatur konten layanan dan tingkat layanan yang diberikan Tencent Cloud, perlindungan data pengguna dan kekayaan intelektual, serta tanggung jawab dan kewajiban keamanan antara pelanggan dan Tencent Cloud. Pelanggan juga dapat memilih untuk menandatangani perjanjian offline dengan Tencent Cloud guna merundingkan klausul dan ketentuan dalam perjanjian tersebut. **Dalam hal pelanggan melaporkan masalah atau menghubungi Tencent Cloud secara aktif**, konsol resmi Tencent Cloud menyediakan layanan tiket yang mendukung pelanggan untuk melaporkan gangguan, insiden, masalah, dan keluhan terkait

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
		penyelesaian pengaduan. (3) Sarana pelaporan sebagaimana dimaksud pada ayat (1) huruf b harus dapat diakses oleh publik dan digunakan untuk penyampaian aduan dan/atau laporan atas Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang yang termuat pada Sistem Elektronik yang dikelolanya. (4) Terhadap aduan dan/atau laporan atas Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang sebagaimana dimaksud pada ayat (3), PSE Lingkup Privat wajib: a. memberikan tanggapan terhadap aduan dan/atau laporan kepada pihak yang mengadukan dan/atau melaporkan; b. melakukan pemeriksaan secara mandiri atas aduan dan/atau laporan dan/atau meminta verifikasi aduan dan/atau laporan kepada Menteri dan/atau Kementerian atau Lembaga terkait; c. memberikan	keamanan, ketersediaan, dan kerahasiaan. Sistem tiket Tencent Cloud akan mengalokasikan prioritas untuk tiket pelanggan melalui mekanisme respons berjenjang. Ketika tim teknis lini pertama tidak dapat menyelesaikan masalah secara efektif, sistem secara otomatis akan memicu proses peningkatan layanan, di mana tim produk atau tim teknis akan turun tangan untuk menangani secara kolaboratif, guna memastikan kebutuhan atau umpan balik pelanggan mendapatkan respons dan penanganan yang tepat waktu. Tencent Cloud menyediakan layanan pelanggan online dan saluran telepon melalui konsol cloud serta situs web resminya untuk mendukung pelanggan dalam memberikan umpan balik terkait masalah yang dihadapi saat menggunakan layanan Tencent Cloud. Tencent Cloud memiliki pusat layanan pelanggan dengan cadangan lintas wilayah yang mampu menangani permintaan pelanggan secara non-stop 7 * 24 jam, menyediakan dukungan teknis sepanjang waktu untuk produk cloud, serta respons dan penanganan layanan yang tepat waktu dan berkualitas tinggi. Pelanggan juga dapat memilih paket layanan yang sesuai untuk mendapatkan dukungan eksklusif yang terdiri dari grup dukungan khusus, manajer layanan teknis khusus, layanan bernilai tambah, dan komponen lainnya.

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
		pemberitahuan kepada Pengguna Sistem Elektronik mengenai aduan dan/atau laporan terhadap Informasi Elektronik dan/atau Dokumen Elektronik yang diunggah oleh Pengguna Sistem Elektronik; dan d. menolak aduan dan/atau laporan apabila Informasi Elektronik dan/atau Dokumen Elektronik yang dilaporkan bukan merupakan Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang. (5) PSE Lingkup Privat yang tidak melakukan kewajiban sebagaimana dimaksud ayat (1) dan ayat (4) diputus akses terhadap Sistem Elektroniknya (access blocking) sesuai dengan ketentuan dalam Peraturan Menteri ini.	
12	Kewajiban Penyelenggara Komputasi Awan	(1) Dalam rangka memenuhi kewajiban sebagaimana dimaksud dalam Pasal 9 ayat (3), Penyelenggara Komputasi Awan wajib memiliki tata kelola mengenai Informasi Elektronik dan/atau Dokumen Elektronik.	Sebagai penyelenggara sistem elektronik lingkup privat, pelanggan harus membangun tata kelola keamanan informasi elektronik, memperjelas kewajiban dan hak pengguna sistem elektronik dalam menggunakan layanan sistem elektronik, kewajiban dan hak operator sistem elektronik swasta selama menjalankan operasi sistem elektronik, serta ketentuan tanggung jawab

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
		(2) Tata kelola sebagaimana dimaksud pada ayat (1) paling sedikit memuat hal-hal sebagai berikut: a. kewajiban dan hak pengguna layanan Penyelenggara Komputasi Awan dalam menggunakan Komputasi Awan; b. kewajiban dan hak Penyelenggara Komputasi Awan dalam melaksanakan operasional Komputasi Awan; c. ketentuan mengenai pertanggungjawaban pengguna layanan Penyelenggara Komputasi Awan dalam hal menyimpan Informasi Elektronik dan/atau Dokumen Elektronik pada Komputasi Awan. (3) Penyelenggara Komputasi Awan wajib memberikan Informasi Elektronik dan/atau Data Elektronik mengenai pengguna layanan Penyelenggara Komputasi Awan yang dikuasainya untuk kepentingan pengawasan dan penegakan hukum.	pengguna sistem elektronik dalam mengunggah informasi/dokumen. Selain itu, untuk tujuan pengawasan dan penegakan hukum, pelanggan wajib menyediakan informasi elektronik pengguna layanan cloud yang dimilikinya kepada otoritas pengawas terkait. Tencent Cloud berpegang pada karakteristik terbuka dan berbagi dari layanan komputasi awan, terus meningkatkan kemampuan keamanan platform dan layanan cloud, serta bersama-sama dengan pelanggan membangun sistem perlindungan keamanan yang lebih baik dan lebih lengkap untuk bisnis dan data di cloud. Sebagai penyedia layanan cloud, Tencent Cloud bertanggung jawab atas infrastruktur pusat data dan keamanan platform cloud. Mengingat bahwa ketika pelanggan memilih kategori layanan cloud yang berbeda (seperti layanan IaaS, PaaS, dan SaaS), tingkat kendali atas komponen yang berbeda juga akan bervariasi. Oleh karena itu, Tencent Cloud telah membangun model Tanggung Jawab Bersama untuk Keamanan Cloud berdasarkan kategori layanan cloud yang berbeda. Detail lebih lanjut dapat dilihat di Bab 3 panduan ini: "**Model Tanggung Jawab Bersama untuk Keamanan Cloud Tencent**". Berdasarkan tujuan di atas dan model tanggung jawab bersama, Tencent Cloud akan memperdalam kolaborasi dengan pelanggan untuk bersama-sama mengatasi berbagai masalah dan

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			tantangan keamanan. Sebagai penyedia layanan cloud, Tencent Cloud menyediakan dokumen hukum secara online di situs web internasionalnya seperti KETENTUAN LAYANAN、General Service Level Agreement、Perjanjian Privasi dan Keamanan Data, yang secara jelas mengatur konten layanan dan tingkat layanan yang diberikan Tencent Cloud, perlindungan data pengguna dan kekayaan intelektual, serta tanggung jawab dan kewajiban keamanan antara pelanggan dan Tencent Cloud. Pelanggan juga dapat memilih untuk menandatangani perjanjian offline dengan Tencent Cloud guna merundingkan klausul dan ketentuan dalam perjanjian tersebut. Selain itu, Tencent Cloud menyediakan Acceptable Use Policy secara daring yang menetapkan aturan perilaku yang baik yang berlaku bagi pelanggan dalam menggunakan Tencent Cloud, serta memperjelas kegiatan yang dilarang bagi pelanggan dan batasan dalam menggunakan perangkat lunak Tencent Cloud. Tencent Cloud berkomitmen untuk melindungi keamanan data pelanggan global dan mematuhi hukum dan peraturan yang berlaku di negara atau wilayah tempat bisnis beroperasi. Pelanggan memiliki kepemilikan dan kendali tunggal atas konten data mereka sendiri. Data pelanggan di dalam Tencent Cloud dikategorikan sebagai data dengan tingkat keamanan tinggi. Kecuali untuk keperluan penyediaan layanan atau pemecahan masalah, dan

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			setelah mendapatkan otorisasi eksplisit dari pelanggan, atau dalam situasi seperti investigasi peristiwa kriminal oleh otoritas pemerintah nasional atau lokal yang sesuai dengan peraturan perundang-undangan, karyawan internal Tencent Cloud tidak akan secara aktif mengakses data pelanggan mana pun.
13	Permohonan Pemutusan Akses Informasi Elektronik dan/atau Dokumen Elektronik yang Dilarang	(1) PSE Lingkup Privat wajib melakukan Pemutusan Akses (take down) terhadap Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang sebagaimana dimaksud dalam Pasal 9 ayat (4). (2) Kewajiban melakukan Pemutusan Akses (take down) sebagaimana dimaksud pada ayat (1) termasuk Pemutusan Akses terhadap Informasi Elektronik dan/atau Dokumen Elektronik yang dapat memfasilitasi penyebarluasan Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang.	Sebagai penyelenggara sistem elektronik lingkup privat, pelanggan harus memperhatikan permohonan pemutusan akses terhadap informasi elektronik yang melanggar aturan yang diajukan oleh publik, departemen atau lembaga, penegak hukum, dan institusi peradilan melalui situs web/aplikasi, email, atau cara lainnya. Pelanggan harus segera memutuskan akses terhadap informasi/dokumen elektronik yang melanggar aturan. Tencent Cloud menyediakanAcceptable Use Policy secara daring yang memperjelas bahwa ketika Tencent Cloud mengantisipasi, mempertimbangkan, atau menduga bahwa akun Tencent Cloud pelanggan telah atau mungkin digunakan untuk penggunaan layanan Tencent Cloud mana pun yang tidak sah, ilegal, atau tidak pantas yang melanggar kebijakan penggunaan, Tencent Cloud dapat mengambil tindakan yang diperlukan sesuai kebijakannya sendiri, menangguhkan atau mengakhiri akses pelanggan ke Tencent Cloud, dan/atau memblokir pesan atau konten dari alamat IP atau domain tertentu. Tencent Cloud dapat menangguhkan atau mengakhiri
14	Permohonan Pemutusan Akses Informasi Elektronik dan/atau Dokumen Elektronik	(1) Permohonan Pemutusan Akses terhadap Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang sebagaimana dimaksud dalam Pasal 13 dapat	

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
	yang Dilarang	diajukan oleh: a. masyarakat; b. Kementerian atau Lembaga; c. Aparat Penegak Hukum; dan/atau d. lembaga peradilan. (2) Permohonan sebagaimana dimaksud pada ayat (1) dapat disampaikan melalui: a. situs web (website) dan/atau aplikasi; b. surat non elektronik; dan/atau c. surat elektronik (electronic mail). (3) Permohonan sebagaimana dimaksud pada ayat (1) bersifat mendesak dalam hal: a. terorisme; b. pornografi anak; atau c. konten yang meresahkan masyarakat dan mengganggu ketertiban umum.	penggunaan atau akses pengguna mana pun ke Tencent Cloud sesuai dengan ketentuan layanan Tencent Cloud.
21	Pemberian Akses Terhadap Sistem Elektronik dan/atau Data Elektronik untuk Kepentingan Pengawasan dan Penegakan Hukum Pidana	(1) PSE Lingkup Privat wajib memberikan akses terhadap Sistem Elektronik dan/atau Data Elektronik kepada Kementerian atau Lembaga dalam rangka pengawasan sesuai dengan peraturan perundang-undangan. (2) PSE Lingkup Privat wajib memberikan akses terhadap Sistem	Sebagai penyelenggara sistem elektronik lingkup privat, pelanggan harus menyediakan akses ke sistem elektronik kepada otoritas pengawas sesuai dengan ketentuan hukum ketika diperlukan untuk pengawasan. **Jika pelanggan perlu memberikan akses ke sistem elektronik atau data elektronik kepada regulator**, pelanggan dapat menggunakan **Cloud**

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
		Elektronik dan/atau Data Elektronik kepada Aparat Penegak Hukum dalam rangka penegakan hukum sesuai dengan peraturan perundang-undangan.	**Object Storage (COS)** yang disediakan oleh Tencent Cloud. Layanan ini merupakan penyimpanan terdistribusi untuk file berskala besar, memungkinkan pengguna menyimpan dan melihat data kapan saja melalui jaringan. Pengguna dapat mengelola hak akses ke bucket dan objek. Ketika menerima permintaan untuk suatu sumber daya, COS akan memeriksa Access Control List (ACL) yang relevan untuk memverifikasi apakah peminta memiliki hak akses yang diperlukan. Setelah akun sub-Tencent Cloud dibuat, pengguna dapat memberikan otorisasi kepada akun sub melalui kebijakan akses; jika perlu membuka sumber daya kepada pengguna non-Tencent Cloud, hal ini dapat dilakukan dengan mengatur izin publik (baca publik) pada sumber daya (bucket, objek, direktori). Melalui fungsi-fungsi di atas, pelanggan dapat memberikan data elektronik kepada regulator sesuai persyaratan untuk diakses. **Cloud Access Management (CAM)** membantu pelanggan mengelola akses ke produk dan sumber daya Tencent Cloud dengan aman dan terperinci. Secara default, akun utama pengguna memiliki hak akses penuh atas sumber daya di bawah namanya, dapat membuat sub-pengguna, serta mengalokasikan ID identitas, kredensial identitas, dan izin kepada sub-pengguna tersebut. CAM juga mendukung berbagai metode verifikasi identitas dua faktor, termasuk penggunaan perangkat MFA atau kode verifikasi melalui ponsel, untuk

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			mengonfirmasi keamanan identitas dan lingkungan sebelum login dan melakukan operasi sensitif. Selain itu, Tencent Cloud berkomitmen untuk melindungi keamanan data pelanggan global dan mematuhi hukum dan peraturan yang berlaku di negara atau wilayah tempat bisnis beroperasi. Pelanggan memiliki kepemilikan dan kendali tunggal atas konten data mereka sendiri. Data pelanggan di dalam Tencent Cloud dikategorikan sebagai data dengan tingkat keamanan tinggi. Kecuali untuk keperluan penyediaan layanan atau pemecahan masalah, dan setelah mendapatkan otorisasi eksplisit dari pelanggan, atau dalam situasi seperti investigasi peristiwa kriminal oleh otoritas pemerintah nasional atau lokal yang sesuai dengan peraturan perundang-undangan, karyawan internal Tencent Cloud tidak akan secara aktif mengakses data pelanggan mana pun.
25	Narahubung	(1) PSE Lingkup Privat harus menunjuk paling sedikit seorang Narahubung yang berdomisili di wilayah Indonesia yang bertugas untuk memfasilitasi permintaan akses terhadap Sistem Elektronik dan/atau Data Elektronik yang disampaikan oleh Kementerian atau Lembaga. (2) Narahubung sebagaimana dimaksud	Sebagai penyelenggara sistem elektronik lingkup privat, pelanggan harus menunjuk setidaknya satu kontak yang berdomisili di wilayah Indonesia untuk mengoordinasikan dan menangani permintaan akses terhadap sistem elektronik dan/atau data yang diajukan oleh otoritas pengawas. Dalam rangka membantu pelanggan memenuhi persyaratan regulasi, Tencent Cloud menunjuk Penghubung Keamanan Informasi. Penghubung Keamanan Informasi akan menjaga komunikasi yang lancar dengan otoritas pengawas setempat sesuai

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
		pada ayat (1) menerima permintaan akses terhadap Sistem Elektronik dan/atau Data Elektronik dari Narahubung yang telah ditetapkan oleh Kementerian atau Lembaga dan disampaikan kepada PSE Lingkup Privat.	dengan persyaratan kepatuhan dan bisnis, serta menangani permintaan akses terhadap sistem elektronik dan/atau data elektronik yang diajukan untuk tujuan pengawasan atau penegakan hukum pidana.
30、40	Keamanan Data	(1) Akses terhadap Sistem Elektronik yang disampaikan oleh PSE Lingkup Privat bersifat terbatas dan rahasia. (2) Akses terhadap Sistem Elektronik hanya dapat digunakan oleh pejabat Kementerian atau Lembaga sebagaimana ditentukan. (3) Pemberian akses terhadap Sistem Elektronik harus menjaga dan melindungi: a. integritas, ketersediaan, dan kerahasiaan dari Data Elektronik; b. keandalan dan keamanan Sistem Elektronik; c. Data Pribadi yang disimpan, ditransmisikan, atau diproses di dalam Sistem	Sebagai penyelenggara sistem elektronik lingkup privat, pelanggan harus memastikan bahwa akses yang diberikan terhadap sistem elektronik bersifat terbatas dan rahasia, hanya dapat digunakan oleh petugas pengawas yang mengajukan permintaan. Saat memberikan hak akses, pelanggan harus menjamin integritas, ketersediaan, dan kerahasiaan data, serta keandalan dan keamanan sistem elektronik, sekaligus melindungi data pribadi di dalam sistem. Untuk mendukung pelanggan memenuhi persyaratan regulasi, **khususnya dalam hal perlindungan data pribadi**, Tencent Cloud menganggap kepatuhan data pribadi sebagai faktor utama dalam proses penyediaan layanan, dan menjadikan prinsip-prinsip kepatuhan data pribadi (seperti legalitas, keadilan, transparansi, pembatasan tujuan, minimalisasi data, integritas, akurasi, kerahasiaan, akuntabilitas, dll.) sebagai panduan kepatuhan privasi. Prinsip-prinsip ini diintegrasikan ke dalam setiap tahap desain dan

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
		Elektronik.	pengembangan produk serta sepanjang siklus hidup data pribadi, menjadikan kepatuhan privasi sebagai atribut inheren dari produk. Selain itu, Tencent Cloud secara ketat mematuhi hukum dan peraturan perlindungan privasi di berbagai negara dan wilayah yang berlaku. Pengalaman dan akumulasi keamanan Tencent Cloud selama bertahun-tahun telah memastikan keamanan infrastruktur platform cloud dan memberikan fondasi yang kuat untuk kepatuhan privasi bisnis pelanggan. Pelanggan memiliki kepemilikan dan kendali tunggal atas konten data mereka sendiri. Data pelanggan di dalam Tencent Cloud dikategorikan sebagai data dengan tingkat keamanan tinggi. Kecuali untuk keperluan penyediaan layanan atau pemecahan masalah, dan setelah mendapatkan otorisasi eksplisit dari pelanggan, atau dalam situasi seperti investigasi peristiwa kriminal oleh otoritas pemerintah nasional atau lokal yang sesuai dengan peraturan perundang-undangan, karyawan internal Tencent Cloud tidak akan secara aktif mengakses data pelanggan mana pun. Untuk memastikan kerahasiaan dan integritas data pelanggan, **Dalam hal perlindungan penyimpanan data**, berbagai produk penyimpanan dan basis data Tencent Cloud mendukung fungsi enkripsi data. Layanan ini menggunakan algoritma enkripsi yang aman dan kuat, serta

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			mengintegrasikan Key Management Service (KMS) untuk mengelola siklus hidup kunci secara menyeluruh, sehingga menjamin kerahasiaan data. Selain itu, Tencent Cloud menggunakan teknologi penyimpanan redundan multi-salinan dan kode penghapusan saat menyimpan data, serta segera mengambil tindakan pemulihan yang diperlukan ketika mendeteksi kesalahan integritas, sehingga sangat meningkatkan kemampuan toleransi kesalahan data. **Dalam hal perlindungan transmisi data**, komunikasi pelanggan di konsol Tencent Cloud dilindungi oleh enkripsi protokol keamanan HTTPS. Antarmuka API cloud yang disediakan oleh produk-produk cloud Tencent Cloud juga dilengkapi dengan kemampuan keamanan seperti enkripsi HTTPS, verifikasi tanda tangan, dan pemantauan status, memberikan jaminan keamanan komunikasi pada tingkat port untuk bisnis pelanggan. **Jika pelanggan perlu memberikan akses ke sistem elektronik atau data elektronik kepada regulator**, pelanggan dapat menggunakan Cloud Object Storage (COS) yang disediakan oleh Tencent Cloud. Layanan ini merupakan penyimpanan terdistribusi untuk file berskala besar, memungkinkan pengguna menyimpan dan melihat data kapan saja melalui

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			jaringan. Pengguna dapat mengelola hak akses ke bucket dan objek. Ketika menerima permintaan untuk suatu sumber daya, COS akan memeriksa Access Control List (ACL) yang relevan untuk memverifikasi apakah peminta memiliki hak akses yang diperlukan. Setelah akun sub-Tencent Cloud dibuat, pengguna dapat memberikan otorisasi kepada akun sub melalui kebijakan akses; jika perlu membuka sumber daya kepada pengguna non-Tencent Cloud, hal ini dapat dilakukan dengan mengatur izin publik (baca publik) pada sumber daya (bucket, objek, direktori). **Cloud Access Management (CAM)** membantu pelanggan mengelola akses ke produk dan sumber daya Tencent Cloud dengan aman dan terperinci. Secara default, akun utama pengguna memiliki hak akses penuh atas sumber daya di bawah namanya, dapat membuat sub-pengguna, serta mengalokasikan ID identitas, kredensial identitas, dan izin kepada sub-pengguna tersebut.
27、31、37、41	Periode Permintaan	Permintaan sebagaimana dimaksud oleh PSE Lingkup Privat dalam waktu paling lambat 5 (lima) hari kalender sejak permintaan tersebut disampaikan oleh Narahubung Kementerian atau Lembaga.	Sebagai penyelenggara sistem elektronik lingkup privat, pelanggan harus menyediakan akses terhadap data elektronik kepada otoritas pengawas dalam waktu 5 hari kalender setelah menerima permintaan dari kontak kementerian atau lembaga. Tencent Cloud, dalam menerima permintaan akses terhadap sistem elektronik dan/atau data elektronik yang diajukan oleh otoritas pengawas atau penegak hukum untuk tujuan

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			pengawasan atau penegakan hukum pidana, akan berkomunikasi dengan otoritas terkait melalui Penghubung Keamanan Informasi regional, serta bekerja sama dengan pelanggan dan otoritas pengawas untuk menyelesaikan permintaan yang relevan.
42	Penyelenggara Komputasi Awan	(1) Penyelenggara Komputasi Awan wajib memberikan Akses terhadap Sistem Elektronik dan/atau Data Elektronik dalam rangka penegakan hukum sebagaimana dimaksud dalam Pasal 21 ayat (2). (2) Kewajiban pemberian Akses sebagaimana dimaksud pada ayat (1) hanya untuk keperluan situasi darurat terkait: a. terorisme; b. pornografi anak; c. perdagangan orang (human trafficking); d. organized crime; dan/atau e. situasi darurat yang mengancam nyawa dan cedera fisik, sesuai dengan peraturan perundang-undangan. (3) Kewajiban pemberian Akses sebagaimana dimaksud pada ayat (1) dan ayat (2) dipenuhi paling lambat 5 (lima) hari kalender sejak tanggal permohonan dari Aparat Penegak	Sebagai penyelenggara sistem elektronik lingkup privat, pelanggan harus menyediakan akses terhadap sistem elektronik kepada otoritas pengawas sesuai dengan ketentuan hukum, ketika diperlukan untuk pengawasan dan hanya dalam situasi darurat yang terbatas pada tindakan terorisme, pornografi anak, perdagangan manusia, kejahatan terorganisir, serta keadaan darurat lain yang mengancam nyawa dan menimbulkan cedera tubuh sesuai dengan peraturan perundang-undangan. Sebagai penyedia layanan komputasi awan, Tencent Cloud dalam menerima permintaan akses terhadap sistem elektronik dan/atau data elektronik yang diajukan oleh otoritas pengawas atau penegak hukum untuk tujuan pengawasan atau penegakan hukum pidana, akan berkomunikasi dengan otoritas terkait melalui Penghubung Keamanan Informasi regional, serta bekerja sama dengan pelanggan dan otoritas pengawas untuk menyelesaikan permintaan yang relevan.

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
		Hukum diterima.	
43、44	Rekam Jejak Akses terhadap Sistem Elektronik dan/atau Data Elektronik untuk Kepentingan Pengawasan dan Penegakan Hukum Pidana	(1) PSE Lingkup Privat wajib memiliki rekam jejak audit mengenai penggunaan akses terhadap Sistem Elektronik yang dilakukan oleh Kementerian atau Lembaga. (2) PSE Lingkup Privat dapat melakukan penilaian (assessment) mengenai dampak penggunaan akses terhadap Sistem Elektronik oleh Kementerian atau Lembaga terhadap: a. kualitas layanan yang diberikan PSE Lingkup Privat kepada Pengguna Sistem Elektroniknya; b. pelindungan Data Pribadi dari Pengguna Sistem Elektroniknya; dan/atau c. pemenuhan kewajiban PSE Lingkup Privat yang diatur dalam peraturan perundang-undangan Indonesia.	Sebagai penyelenggara sistem elektronik lingkup privat, pelanggan wajib menyimpan catatan audit penggunaan akses sistem elektronik oleh otoritas pengawas atau penegak hukum, serta menetapkan batas waktu yang wajar untuk pemberian hak akses tersebut. Pelanggan juga harus melakukan penilaian terhadap dampak yang ditimbulkan dari akses otoritas pengawas terhadap sistem elektroniknya. Untuk menyimpan catatan akses otoritas pengawas terhadap sistem elektronik atau data elektronik, Tencent Cloud menyediakan **Cloud Log Service (CLS)**. Sebagai platform layanan log terpadu, CLS menawarkan berbagai layanan mulai dari pengumpulan log, penyimpanan log, hingga pencarian dan analisis log, konsumsi real-time, serta pengiriman log. Layanan ini membantu pelanggan menyelesaikan berbagai masalah seperti operasi bisnis, pemantauan keamanan, audit log, dan analisis log. Untuk data elektronik pelanggan yang disimpan dalam layanan **Cloud Object Storage (COS)**, COS menyediakan fungsi manajemen log yang mampu mencatat informasi akses rinci untuk bucket penyimpanan sumber tertentu, seperti pengunggahan, pengunduhan, penghapusan objek, pembuatan atau

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
		(3) Penggunaan akses untuk kepentingan pengawasan dilakukan dalam jangka waktu wajar dan dapat dipertanggungjawabkan.	penghapusan bucket, serta modifikasi konfigurasi bucket yang dimulai oleh pengguna. Informasi ini disimpan dalam bentuk file log di bucket yang ditentukan, guna mencapai pengelolaan bucket yang lebih baik. Selain itu, pelanggan dapat mengaktifkan fungsi **Cloud Log Service (CLS)** untuk bucket. CLS menyediakan kemampuan kuat untuk pelaporan log terkait operasi objek bucket dengan granularitas menit, pencarian real-time, visualisasi, dan peringatan. Pengguna dapat mengidentifikasi operasi bucket oleh akun pengguna yang berwenang dari log yang memiliki stempel waktu, membantu menganalisis kondisi akses bucket saat ini dengan lebih baik, serta dengan cepat melacak masalah saat akses abnormal terjadi. Selain itu, **Cloud Access Management (CAM)** menyediakan kontrol izin yang terperinci, memberikan hak akses spesifik kepada personel berbeda untuk sumber daya yang berbeda. Pelanggan juga dapat menggunakan **CloudAudit** untuk memantau aktivitas akun Tencent Cloud, melakukan pemeriksaan kepatuhan, audit operasi, dan audit risiko.
47	Ketentuan Peralihan	PSE Lingkup Privat yang diatur dalam Peraturan Menteri ini wajib melakukan pendaftaran dalam jangka waktu	Sebagai penyelenggara sistem elektronik lingkup privat, pelanggan harus melakukan pendaftaran dan mematuhi norma, standar, serta prosedur yang ditetapkan dalam

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
		paling lambat 6 (enam) bulan sejak Peraturan Menteri ini berlaku.	peraturan. Tencent Cloud juga telah menyerahkan dokumen yang diperlukan untuk pendaftaran kepada otoritas pengawas setempat di Indonesia dan menyelesaikan proses registrasi sebagai penyelenggara sistem elektronik lingkup privat.

08 Penutup

Tencent Cloud adalah merek komputasi awan yang dibangun dengan dedikasi oleh Tencent Group, mewarisi akumulasi teknologi dan kemampuan praktik keamanan Tencent selama bertahun-tahun. Tencent Cloud berkomitmen untuk terus menyediakan awan yang aman, terpercaya, dan cerdas bagi pelanggan, membantu lebih banyak perusahaan menyambut gelombang digital dengan efisien, serta mendorong perkembangan bisnis yang aman.

Panduan ini didasarkan pada persyaratan regulasi penting dari Pemerintah Indonesia dan Kementerian Komunikasi dan Digital, yang secara komprehensif dan transparan menunjukkan kepada pelanggan bagaimana Tencent Cloud dapat membantu mereka mencapai kepatuhan sistem dan data di awan, serta mendukung klien perusahaan dengan percaya diri dan tenang menempatkan sistem dan data mereka di awan. Tencent Cloud berharap melalui panduan ini dapat mendukung klien perusahaan dalam memenuhi standar kepatuhan Pemerintah Indonesia dan Kementerian Komunikasi dan Digital secara efektif, sekaligus mencapai peningkatan digital dan inovasi bisnis secara efisien.

Panduan ini hanya sebagai referensi. Untuk informasi dalam panduan ini, pelanggan dapat menggunakannya sesuai dengan kondisi aktual mereka sendiri guna memastikan kepatuhan regulasi selama menggunakan layanan awan Tencent Cloud.

09

Riwayat Versi

Tanggal	Versi	Detail
April 2016	V1.0	Rilis Perdana