

KEPUTUSAN KEPALA BADAN PENYELENGGARA JAMINAN PRODUK HALAL
REPUBLIK INDONESIA
NOMOR 260 TAHUN 2026
TENTANG
KEBIJAKAN KEAMANAN INFORMASI, TEKNOLOGI INFORMASI, DAN KOMUNIKASI BADAN PENYELENGGARA JAMINAN PRODUK HALAL

DENGAN RAHMAT TUHAN YANG MAHA ESA

KEPALA BADAN PENYELENGGARA JAMINAN PRODUK HALAL
REPUBLIK INDONESIA,

Menimbang : a. bahwa untuk melaksanakan ketentuan Pasal 41 ayat (4) dan Pasal 48 ayat (5) Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik, serta penerapan keamanan informasi, teknologi informasi, dan komunikasi dalam mendukung penyelenggaraan tugas dan fungsi Badan Penyelenggara Jaminan Produk Halal, perlu menetapkan kebijakan keamanan informasi, teknologi informasi, dan komunikasi;

b. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, perlu menetapkan Keputusan Kepala Badan Penyelenggara Jaminan Produk Halal tentang Kebijakan Keamanan Informasi, Teknologi Informasi, dan Komunikasi Badan Penyelenggara Jaminan Produk Halal;

Mengingat : 1. Undang-Undang Nomor 33 Tahun 2014 tentang Jaminan Produk Halal (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 295, Tambahan Lembaran Negara Republik Indonesia Nomor 5604) sebagaimana telah beberapa kali diubah terakhir dengan Undang-Undang Nomor 6 Tahun 2023 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 2 Tahun 2 Tahun 2022 tentang Cipta Kerja Menjadi Undang-Undang (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 41, Tambahan Lembaran Negara Republik Indonesia Nomor 6856);

2. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843) sebagaimana telah beberapa kali diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2024 Nomor 1, Tambahan Lembaran Negara Republik Indonesia Nomor 6905);

3. Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 61, Tambahan Lembaran Negara Republik Indonesia Nomor 4846);
4. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185, Tambahan Lembaran negara Republik Indonesia Nomor 6400);
5. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
6. Peraturan Presiden Nomor 39 Tahun 2019 tentang Satu Data Indonesia (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 112);
7. Peraturan Presiden Nomor 82 Tahun 2023 tentang Percepatan Transformasi Digital dan Keterpaduan Layanan Digital Nasional (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 159);
8. Peraturan Presiden Nomor 153 Tahun 2024 tentang Badan Penyelenggara Jaminan Produk Halal (Lembaran Negara Republik Indonesia Tahun 2024 Nomor 349);
9. Peraturan Presiden Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 129);
10. Peraturan Presiden Nomor 12 Tahun 2025 tentang Rencana Pembangunan Jangka Menengah Nasional 2025–2029 (Lembaran Negara Republik Indonesia Tahun 2025 Nomor 19);
11. Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan lnformasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2021 Nomor 541);
12. Peraturan Badan Penyelenggara Jaminan Produk Halal Republik Indonesia Nomor 1 Tahun 2025 Tentang Satu Data Badan Penyelenggara Jaminan Produk Halal (Berita Negara Republik Indonesia Tahun 2025 Nomor 733);

MEMUTUSKAN:

Menetapkan : KEPUTUSAN KEPALA BADAN PENYELENGGARA JAMINAN PRODUK HALAL TENTANG KEBIJAKAN KEAMANAN INFORMASI, TEKNOLOGI INFORMASI, DAN KOMUNIKASI BADAN PENYELENGGARA JAMINAN PRODUK HALAL.

KESATU : Menetapkan kebijakan keamanan informasi, teknologi informasi, dan komunikasi Badan Penyelenggara Jaminan Produk Halal sebagaimana tercantum dalam Lampiran yang merupakan bagian tidak terpisahkan dari Keputusan ini.

KEDUA : Kebijakan keamanan informasi, teknologi informasi, dan komunikasi Badan Penyelenggara Jaminan Produk Halal sebagaimana dimaksud dalam Diktum KESATU merupakan acuan bagi seluruh unit kerja di lingkungan Badan Penyelenggara Jaminan Produk Halal dalam pelaksanaan Sistem Manajemen Keamanan Informasi pada Badan Penyelenggara Jaminan Produk Halal.

KETIGA : Keputusan ini mulai berlaku pada tanggal ditetapkan.

Ditetapkan di Jakarta
pada tanggal 3 Agustus 2026
KEPALA BADAN PENYELENGGARA
JAMINAN PRODUK HALAL
REPUBLIK INDONESIA,

ttd.

AHMAD HAIKAL HASAN

Salinan sesuai dengan aslinya
BADAN PENYELENGGARA JAMINAN
PRODUK HALAL
REPUBLIK INDONESIA
Kepala Biro Hukum, Sumber Daya Manusia
dan Hubungan Masyarakat,

Beny Cahyadie
NIP. 198204102000121001

LAMPIRAN
KEPUTUSAN KEPALA BADAN PENYELENGGARA JAMINAN PRODUK HALAL REPUBLIK INDONESIA
NOMOR 260 TAHUN 2026
TENTANG
KEBIJAKAN KEAMANAN INFORMASI, TEKNOLOGI INFORMASI, DAN KOMUNIKASI BADAN PENYELENGGARA JAMINAN PRODUK HALAL

KEBIJAKAN KEAMANAN INFORMASI, TEKNOLOGI INFORMASI, DAN KOMUNIKASI BADAN PENYELENGGARA JAMINAN PRODUK HALAL

BAB I
PENDAHULUAN

A. Latar Belakang

Badan Penyelenggara Jaminan Produk Halal (BPJPH) memiliki peran sentral dan strategis dalam ekosistem ekonomi syariah nasional sesuai mandat Undang-Undang Jaminan Produk Halal. Dalam era transformasi digital saat ini, seluruh layanan BPJPH mulai dari registrasi, audit, penetapan kehalalan produk, hingga penerbitan sertifikat halal telah bertransformasi menjadi layanan digital melalui Sistem Pemerintahan Berbasis Elektronik (SPBE). Transformasi ini membawa konsekuensi logis berupa peningkatan eksposur terhadap ancaman keamanan siber yang kian kompleks, dinamis, dan persisten.

Keamanan informasi bukan lagi sekadar isu teknis operasional melainkan telah menjadi isu strategis yang berdampak langsung pada kepercayaan publik (*public trust*), kedaulatan data, dan reputasi negara. Kegagalan dalam melindungi aset informasi dapat berakibat fatal, mulai dari terganggunya layanan publik, kebocoran data strategis, hingga potensi pemalsuan status kehalalan produk yang dapat meresahkan masyarakat. Oleh karena itu diperlukan sebuah landasan kebijakan yang kokoh, komprehensif, dan mengikat untuk menjamin keamanan informasi secara menyeluruh.

B. Maksud

Penetapan keputusan ini dimaksudkan sebagai kerangka kerja utama tata kelola keamanan informasi pada BPJPH. Kebijakan ini juga menjadi bukti komitmen manajemen puncak dalam mendukung penerapan SPBE yang aman dan terpercaya dan kepatuhan terhadap regulasi dengan memastikan seluruh aktivitas pengelolaan informasi di BPJPH patuh terhadap ketentuan perundang-undangan yang berlaku, khususnya terkait SPBE, persandian, dan perlindungan data pribadi.

C. Tujuan

1. Menjamin prinsip *confidentiality, integrity, availability, authentication, dan non-repudiation* (CIA-AN) guna untuk memastikan seluruh aset informasi BPJPH memenuhi prinsip kerahasiaan (*confidentiality*), keutuhan (*integrity*), ketersediaan (*availability*), keaslian (*authentication*), dan nirsangkal (*non-repudiation*) sepanjang siklus hidup data;
2. Mewujudkan Ketahanan Siber (*Cyber Resilience*) bertujuan untuk membangun kemampuan organisasi untuk mengantisipasi, menahan,

memulihkan diri, dan berevolusi dalam menghadapi kondisi gangguan siber atau bencana teknologi, guna menjamin keberlangsungan layanan jaminan produk halal;

3. Budaya keamanan bertujuan untuk membangun kesadaran dan budaya keamanan informasi yang kuat di seluruh lapisan organisasi, sehingga keamanan informasi menjadi tanggung jawab bersama, bukan hanya tanggung jawab tim teknis;
4. Tercapainya tingkat kematangan (*maturity level*) keamanan siber BPJPH dengan kategori minimal "Baik" berdasarkan evaluasi Indeks Keamanan Informasi (KAMI) dan/atau Instrumen Pengukuran Kematangan Keamanan Siber dan Sandi (IKASANDI) dari Badan Siber dan Sandi Negara (BSSN); dan
5. Terintegrasinya tata kelola risiko keamanan informasi ke dalam manajemen risiko BPJPH, sehingga setiap keputusan strategis turut mempertimbangkan aspek risiko siber.

D. Sasaran

Sasaran kebijakan keamanan informasi adalah acuan tertinggi bagi seluruh unit kerja di lingkungan BPJPH dalam merancang prosedur, standard teknis, dan instruksi kerja terkait pengelolaan informasi. Hal ini akan menjamin keamanan seluruh aset informasi yang dikelola BPJPH sekaligus menjadi pedoman operasional bagi seluruh unit kerja di lingkungan BPJPH dalam pengembangan dan penyelenggaraan layanan yang selaras dengan kebijakan SPBE dan arah transformasi digital pemerintah.

E. Ruang Lingkup

Ruang lingkup Keputusan ini meliputi:

1. Prinsip, strategi, dan manajemen risiko;
2. Pengendalian keamanan informasi;
3. Monitoring, evaluasi, dan audit; dan
4. Perbaikan berkelanjutan

F. Pengertian

Beberapa istilah yang digunakan dalam Keputusan ini yang dimaksud dengan:

1. Sistem pemerintahan berbasis elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada pengguna SPBE.
2. Keamanan Informasi adalah upaya sistematis untuk melindungi kerahasiaan, integritas, dan ketersediaan data dan informasi dalam penyelenggaraan SPBE dari ancaman, gangguan, atau penyalahgunaan.
3. Keamanan Siber adalah upaya yang dilakukan untuk menjaga kerahasiaan, keutuhan, dan ketersediaan informasi serta infrastruktur informasi di ruang siber dari serangan siber.
4. Aset Informasi adalah segala sesuatu yang memiliki nilai bagi organisasi, mencakup data, informasi, perangkat lunak (*software*), perangkat keras (*hardware*), sumber daya manusia, dan fasilitas pendukung lainnya.
5. Manajemen Risiko adalah aktivitas terkoordinasi untuk mengarahkan dan mengendalikan organisasi terkait dengan risiko.

6. Risiko Keamanan Informasi adalah potensi terjadinya suatu peristiwa yang dapat berdampak negatif terhadap Keamanan Informasi yang diukur dari kemungkinan kejadian dan dampak yang ditimbulkan.
7. Insiden Siber/Keamanan Informasi adalah satu atau serangkaian kejadian Keamanan Informasi yang tidak diinginkan atau tidak terduga yang berpeluang signifikan mengganggu operasi bisnis dan mengancam Keamanan Informasi.
8. Pusat Data Nasional (PDN) adalah infrastruktur pusat data yang diselenggarakan oleh Pemerintah Pusat untuk digunakan secara bagi pakai oleh Instansi Pusat dan Pemerintah Daerah.
9. Kriptografi adalah disiplin ilmu yang mencakup prinsip, cara, dan metode untuk mentransformasi data dengan tujuan menyembunyikan isi informasinya, mencegah modifikasi tanpa terdeteksi, atau mencegah penggunaan tanpa izin.
10. Enkripsi adalah proses teknis mengonversi informasi menjadi kode rahasia sehingga mengaburkan data yang dikirim, diterima, atau disimpan.
11. Badan Penyelenggara Jaminan Produk Halal yang selanjutnya disebut BPJPH, merupakan Lembaga Pemerintah Nonkementerian yang menyelenggarakan tugas pemerintahan di bidang penyelenggaraan jaminan produk halal.
12. Pihak Ketiga adalah perseorangan, perusahaan, atau badan hukum di luar struktur organisasi BPJPH yang memiliki akses untuk memproses, menyimpan, atau mengelola Aset Informasi BPJPH berdasarkan perjanjian kerja sama, termasuk vendor, konsultan, dan penyedia jasa.
13. Pemilik Data (*Data Owner*) adalah unit kerja atau pejabat di lingkungan BPJPH yang memiliki kewenangan dan tanggung jawab terhadap pembuatan, pengklasifikasian, dan penggunaan data/informasi tertentu.
14. Pengguna (*User*) adalah pegawai BPJPH atau Pihak Ketiga yang diberikan hak akses untuk menggunakan sistem informasi dan Aset Informasi BPJPH untuk keperluan pekerjaan.

BAB II
PRINSIP, STRATEGI, DAN MANAJEMEN RISIKO

Dalam dunia Keamanan Siber, tidak ada kondisi yang benar-benar aman 100% (seratus persen). Ancaman, kerentanan, serta teknik serangan terus berkembang, sehingga organisasi harus mampu beradaptasi dan membangun ketahanan yang berkelanjutan. Menyadari realitas tersebut, BPJPH menerapkan pendekatan berbasis risiko (*Risk-Based Approach*) sebagai landasan utama dalam pengelolaan Keamanan Informasi. Pendekatan ini menekankan bahwa setiap tindakan pengamanan, investasi teknologi, maupun penerapan pengendalian tidak dilakukan secara seragam, tetapi harus proporsional dengan nilai aset yang dilindungi, tingkat risiko yang dihadapi, serta dampak potensial terhadap layanan dan keberlangsungan operasional.

A. Penerapan prinsip *Confidentiality, Integrity, Availability, Authentication,* dan *Non-repudiation* (CIA-AN)

Seluruh arsitektur sistem dan proses bisnis BPJPH wajib dirancang dengan menerapkan prinsip dasar keamanan secara ketat, sebagai berikut:

1. Kerahasiaan (*Confidentiality*)
   Mencegah pengungkapan informasi secara tidak sah. Kontrol diterapkan melalui Enkripsi data, pemisahan tugas (*segregation of duties*), dan klasifikasi data;
2. Keutuhan (*Integrity*)
   Menjamin keakuratan dan kelengkapan informasi. Kontrol diterapkan melalui *hashing*, validasi input, dan manajemen perubahan sistem yang ketat;
3. Ketersediaan (*Availability*)
   Memastikan informasi dan layanan tersedia saat dibutuhkan. Kontrol diterapkan melalui redundansi server, *load balancing*, dan rencana pemulihan bencana atau *Disaster Recovery Plan* (DRP);
4. Otentikasi (*Authentication*)
   Memastikan validitas identitas pengakses sistem. Penerapan MFA (*Multi-Factor Authentication*) adalah wajib bagi sistem kritis; dan
5. Nirsangkal (*Non-repudiation*)
   Menjamin suatu tindakan elektronik tidak dapat disangkal pembuktiannya. Wajib diterapkan menggunakan Tanda Tangan Elektronik (TTE) tersertifikasi pada dokumen legal seperti Sertifikat Halal.

B. Strategi infrastruktur:

Strategi infrastruktur *cloud first policy* untuk mendukung skalabilitas dan efisiensi SPBE, BPJPH menetapkan strategi infrastruktur *cloud first* dengan ketentuan pelaksanaan, meliputi:

1. *Platform* utama
   Menggunakan layanan *Public Cloud* yang telah memiliki akreditasi keamanan ISO 27001:2022 dan terdaftar di Kementerian Komunikasi dan Digital sebagai *platform* utama untuk aplikasi layanan publik;
2. Kedaulatan data
   Lokasi pusat data dan pusat pemulihan bencana penyedia layanan *cloud* wajib berada di dalam wilayah hukum Negara Kesatuan Republik Indonesia; dan
3. Integrasi PDN
   Sebagai strategi jangka panjang, BPJPH akan menyusun peta jalan migrasi data dan sistem ke PDN sesuai kesiapan infrastruktur pemerintah pusat.

C. Manajemen risiko terintegrasi

Pengelolaan risiko Keamanan Informasi dilaksanakan secara terintegrasi dengan manajemen risiko BPJPH melalui tahapan:

1. Identifikasi risiko dilakukan sebagai langkah awal untuk menemukan potensi ancaman, kerentanan, dan Aset Informasi yang terdampak. Kegiatan ini mencakup:
   a. Mengidentifikasi seluruh Aset Informasi yang mendukung layanan SPBE BPJPH, termasuk data, aplikasi, infrastruktur, dan sumber daya manusia;
   b. Mengidentifikasi ancaman (seperti *malware, human error,* dan bencana alam) serta kerentanan sistem yang berpotensi mengganggu kerahasiaan, integritas, dan ketersediaan informasi;
   c. Mengidentifikasi kerentanan yang dapat dimanfaatkan oleh ancaman, baik yang bersifat teknis maupun non-teknis; dan
   d. Menyusun daftar awal risiko berdasarkan keterkaitan antara aset, ancaman, dan kerentanan.

2. Analisis risiko dilakukan untuk menilai besarnya risiko yang muncul dari ancaman dan kerentanan yang teridentifikasi, dengan mempertimbangkan kemungkinan terjadinya dan dampak yang ditimbulkannya. Kegiatan meliputi:
   a. Menilai tingkat kemungkinan (*likelihood*) terjadinya risiko berdasarkan kondisi teknis, historis, operasional, dan lingkungan sistem;
   b. Menilai dampak (*impact*) risiko terhadap layanan SPBE, data halal, proses sertifikasi, reputasi organisasi, serta aspek hukum dan pelayanan publik;
   c. Menentukan tingkat risiko awal (*inherent risk*) dengan menggunakan matriks risiko yang ditetapkan; dan
   d. Menilai pengendalian yang sudah ada (*existing controls*) dan menghitung risiko sisa (*residual risk*).

   Hasil analisis berupa tingkat risiko yang terukur untuk setiap risiko yang teridentifikasi.

3. Evaluasi risiko dilakukan untuk menetapkan prioritas penanganan risiko berdasarkan tingkat risiko dan kriteria penerimaan risiko (*risk appetide*) yang telah ditetapkan BPJPH. Kegiatan meliputi:
   a. Membandingkan tingkat risiko dengan kriteria risiko BPJPH;
   b. Menentukan prioritas penanganan risiko sesuai tingkat risiko (tinggi, sedang, rendah);
   c. Menetapkan risiko yang dapat diterima serta risiko yang memerlukan intervensi segera; dan
   d. Menyusun daftar prioritas risiko dalam bentuk *risk register* sebagai dasar perencanaan penanganan.

4. Perlakuan risiko (*Risk Treatment*) dilakukan melalui pemilihan dan penerapan langkah pengendalian yang tepat untuk menurunkan risiko hingga berada pada tingkat yang dapat diterima. Strategi penanganan risiko, meliputi:
   a. Mitigasi risiko
      Menerapkan atau meningkatkan pengendalian teknis dan administratif, antara lain:
      1) pengamanan jaringan dan aplikasi;
      2) Enkripsi data;
      3) autentikasi berlapis;
      4) pembaruan sistem dan *patching*;
      5) pencadangan dan pemulihan bencana; dan
      6) audit dan pengujian keamanan.
   b. Pengalihan risiko
      Mengalihkan sebagian risiko kepada pihak lain melalui penggunaan layanan ber-SLA, *outsourcing*, atau mekanisme asuransi.
   c. Penghindaran Risiko
      Menghilangkan proses, fungsi, atau teknologi yang menimbulkan risiko apabila dinilai tidak dapat dikelola dengan efektif.
   d. Penerimaan Risiko
      Menerima risiko yang berada pada tingkat rendah atau risiko yang tidak *cost-effective* untuk ditangani, sesuai dengan kebijakan penerimaan risiko.

   Pelaksanaan perlakuan risiko harus terdokumentasi, terukur, diawasi, dan dievaluasi secara berkala.

5. Integrasi SPBE
   Laporan Risiko Keamanan Informasi menjadi bagian tak terpisahkan dari laporan manajemen risiko SPBE instansi.

BAB III
PENGENDALIAN KEAMANAN INFORMASI

Kebijakan strategis harus diturunkan menjadi langkah pengendalian operasional yang konkret (*fase do*) dalam siklus *Plan Do Check Act* (PDCA). Pengendalian Keamanan Informasi di BPJPH mencakup aspek administratif, teknis, dan fisik untuk memberikan perlindungan berlapis (*defense in depth*). Beberapa cara pengendalian yang harus dilakukan oleh BPJPH adalah:

A. Pengendalian kebijakan dan prosedur
   Pengendalian kebijakan dan prosedur, yaitu penyusunan, penetapan, dan penerapan kebijakan, standard, serta prosedur operasional Keamanan Informasi yang wajib dipatuhi oleh seluruh unit kerja. Pengendalian ini mencakup mekanisme pengelolaan akses, pengelolaan insiden, tata kelola penggunaan sistem, serta koordinasi Keamanan Informasi agar pelaksanaan SPBE berjalan konsisten dan sesuai dengan ketentuan perundang undangan.

B. Peningkatan kesadaran Keamanan Informasi
   Peningkatan kesadaran yaitu penyelenggaraan kegiatan edukasi, sosialisasi, dan pelatihan Keamanan Informasi secara terencana dan berkelanjutan bagi seluruh pegawai BPJPH. Pengendalian ini bertujuan menumbuhkan budaya Keamanan Informasi, meningkatkan pemahaman terhadap risiko, serta memperkuat kapasitas SDM dalam menjaga keamanan layanan SPBE.

C. Klasifikasi dan penanganan Aset Informasi
   Setiap Pemilik Data wajib melakukan klasifikasi terhadap Aset Informasi yang dikelolanya ke dalam empat kategori berikut:
   1. Sangat rahasia (*top secret*)
      Informasi yang jika bocor dapat membahayakan stabilitas nasional, hubungan internasional, atau keamanan negara, dapat dicontohkan sebagai berikut:
      a. contohnya pada kunci Enkripsi utama (*Root CA Keys*), data intelijen kerentanan sistem kritis; dan
      b. penanganannya wajib Enkripsi kuat, akses fisik terbatas biometrik, dilarang disimpan di *public cloud*.

   2. Rahasia (*Confidential*)
      Informasi yang jika bocor dapat merugikan BPJPH secara hukum, finansial, atau reputasi, serta melanggar hak privasi individu atau pelaku usaha, dapat dicontohkan sebagai berikut:
      a. contohnya pada draf keputusan penetapan kehalalan produk sebelum sidang, data spesifik formula produk pelaku usaha, data pribadi pegawa; dan
      b. penanganannya berupa akses *Need-to-Know*, wajib Enkripsi saat transmisi, wajib *Non Disclosure Agreement* (NDA) bagi pengakses.

   3. Terbatas (*Internal Use*)
      Informasi untuk kalangan internal BPJPH yang tidak dimaksudkan untuk publik, dapat dicontohkan sebagai berikut:

a. contohnya pada memo, Standard Operasional Prosedur (SOP), notulensi rapat manajemen rutin; dan
b. penanganannya berupa distribusi terbatas pada email instansi, dilarang diunggah ke media sosial publik.

4. Umum (*Public*)
Informasi yang memang disediakan untuk konsumsi publik, dapat dicontohkan sebagai berikut:
a. contohnya pada daftar produk bersertifikat halal, regulasi JPH, berita kegiatan; dan
b. penanganannya berupa dijaga integritasnya agar tidak dimodifikasi oleh pihak tidak berwenang (*defacement*).

D. Retensi dan pemusnahan data

Siklus hidup data harus dikelola mulai dari penciptaan hingga pemusnahan, sebagai berikut:

1. Masa retensi
Data disimpan sesuai dengan Jadwal Retensi Arsip (JRA) BPJPH. Untuk data transaksi sertifikasi halal, retensi wajib menjamin ketersediaan data untuk keperluan audit dan penelusuran (*traceability*) jangka panjang.
2. Mekanisme pemusnahan:
a. data digital pada media penyimpanan yang sudah tidak digunakan wajib dimusnahkan menggunakan metode menimpa data berulang kali (*secure wiping)* atau *degaussing*; dan
b. media fisik (kertas) kategori rahasia atau sangat rahasia wajib dimusnahkan dengan mesin penghancur kertas atau dilebur.

E. Pengendalian akses

Akses terhadap sistem dan data diberikan berdasarkan prinsip hak akses minimal (*least privilege*), sebagai berikut:

1. *Registrasi* Pengguna
Setiap pemberian akses harus didasarkan pada permintaan resmi atasan dan disetujui oleh Pemilik Data.
2. Pengelolaan kata sandi
Wajib menerapkan kebijakan kata sandi yang kompleks (kombinasi huruf, angka, simbol) dan diganti secara berkala.
3. Otentikasi Multifaktor (MFA)
Seluruh akses administratif dan akses ke sistem kritis SIHALAL wajib menggunakan MFA.
4. Tinjauan akses
Hak akses Pengguna harus ditinjau ulang minimal setiap 6 (enam) bulan. Hak akses pegawai yang mutasi atau berhenti harus dicabut segera pada hari terakhir kerja.

F. Perlindungan Kriptografi data kritis

BPJPH menerapkan standard Kriptografi tinggi untuk melindungi integritas data Jaminan Produk Halal, meliputi:

1. Data Pengguna wajib dilindungi dengan Enkripsi; dan
2. Data sertifikat halal pada dokumen elektronik sertifikat halal wajib ditandatangani menggunakan sertifikat elektronik yang diterbitkan oleh Penyelenggara Sertifikasi Elektronik (PSrE) yang diakui Pemerintah Republik Indonesia. Hal ini untuk menjamin keabsahan hukum dan mencegah pemalsuan dokumen.

G. Pencadangan dan pemulihan bencana

Audit dan pengujian keamanan, yaitu pelaksanaan pengawasan berkala atas kepatuhan penerapan Keamanan Informasi melalui audit internal, audit eksternal, uji penetrasi, penilaian kerentanan, serta mekanisme monitoring keamanan yang berkelanjutan. Pengendalian ini bertujuan memastikan efektivitas kontrol dan mendeteksi potensi kelemahan sejak dini.

BAB IV
MONITORING, EVALUASI, DAN AUDIT

Dalam siklus manajemen mutu PDCA, tahap monitoring dan evaluasi memegang peranan yang sangat krusial dalam memastikan efektivitas keseluruhan sistem. Tahap ini bukan hanya sekadar aktivitas pengecekan rutin tetapi merupakan proses yang menentukan apakah setiap kebijakan, prosedur, dan pengendalian Keamanan Informasi benar-benar berjalan sesuai tujuan. Tanpa adanya pengukuran yang valid, objektif, dan terstruktur, BPJPH tidak akan mampu menilai level kebijakan keamanan yang diterapkan telah berfungsi mengurangi risiko, meningkatkan ketahanan layanan, atau bahkan terdapat dampak samping berupa penurunan efisiensi dan produktivitas. Melalui proses monitoring dan evaluasi yang tepat, BPJPH dapat memperoleh gambaran kinerja yang akurat, mengidentifikasi area yang perlu perbaikan, serta memastikan bahwa seluruh pengendalian keamanan informasi tetap relevan, efektif, dan selaras dengan tujuan strategis organisasi.

A. Pemantauan kinerja keamanan (*Security Metrics*)

BPJPH menetapkan Indikator Kinerja Utama (IKU) Keamanan Informasi yang harus diukur dan dilaporkan secara berkala, sebagai berikut:

1. Tingkat ketersediaan sistem (*Availability*)
   Target ketersediaan layanan sistem inti (SIHALAL) adalah minimal 99,9% (sembilan puluh sembilan koma sembilan persen) per bulan;
2. Waktu Tanggap Insiden (*Incident Response Time*)
   Target waktu respon awal terhadap insiden keamanan kategori Kritis adalah kurang dari 1 (satu) jam setelah deteksi;
3. Tingkat kepatuhan regulasi
   Target pemenuhan 100% (seratus persen) terhadap parameter kepatuhan SPBE dan rekomendasi audit eksternal; dan
4. Efektivitas *Patching*
   Persentase kerentanan kritis (*critical vulnerabilities*) yang ditutup (di *patch*) dalam waktu kurang dari 14 (empat belas) hari sejak rilis perbaikan.

B. Audit dan asesmen teknis

Untuk menjamin objektivitas, evaluasi keamanan dilakukan melalui berbagai metode sebagai berikut:

1. *Vulnerability Assessment* (VA)
   Dilakukan pemindaian kerentanan secara otomatis minimal setiap 3 (tiga) bulan sekali pada seluruh sistem yang terpublikasi ke internet (*public facing*); dan
2. *Penetration Testing* (*Pentest*)
   Dilakukan uji penetrasi mendalam minimal 1 (satu) kali setahun pada aplikasi kritis SIHALAL, khususnya setelah adanya perubahan fitur mayor (*major changes*), untuk mensimulasikan serangan peretas sungguhan.
3. Audit internal

Dilakukan minimal 1 (satu) kali dalam setahun oleh tim auditor internal yang independen dari unit operasional TIK, mencakup pemeriksaan kepatuhan prosedur dan kontrol teknis.

4. Audit eksternal
   BPJPH secara proaktif mengikuti audit keamanan SPBE yang diselenggarakan oleh BSSN atau auditor eksternal terakreditasi lainnya sesuai ketentuan regulasi.

C. Tinjauan manajemen (*Management review*)

Komite Keamanan Informasi wajib melaksanakan rapat tinjauan manajemen minimal 1 (satu) kali dalam setahun dengan agenda pembahasan sebagai berikut:

1. Hasil audit keamanan informasi dan status tindak lanjut perbaikan;
2. Umpan balik dari pemangku kepentingan (pelaku usaha, pendamping PPH, lembaga pemeriksa halal, lembaga pendamping PPH, Komite Fatwa Majelis Ulama Indonesia) terkait keamanan layanan;
3. Kinerja proses dan kesesuaian kebijakan keamanan informasi;
4. Status tindakan pencegahan dan perbaikan; dan
5. Perubahan isu eksternal dan internal yang relevan dengan Sistem Manajemen Keamanan Informasi.

BAB V
PERBAIKAN BERKELANJUTAN

Lanskap ancaman siber bersifat sangat dinamis, ditandai dengan munculnya metode, teknik, dan pola serangan baru yang berkembang hampir setiap hari. Kondisi ini menuntut organisasi untuk tidak bergantung pada pendekatan keamanan yang statis atau sekali jadi. Dalam konteks tersebut, Sistem Manajemen Keamanan Informasi (SMKI) BPJPH harus dirancang agar mampu beradaptasi dan merespons perubahan ancaman secara berkelanjutan. Hal ini sejalan dengan prinsip *Continuous Improvement* pada fase *Act* dalam siklus PDCA, organisasi wajib melakukan penyesuaian, perbaikan, dan penyempurnaan berdasarkan hasil evaluasi, temuan insiden, perubahan teknologi, serta kebutuhan operasional.

A. Tindakan perbaikan (*Corrective Action*)

Apabila ditemukan ketidaksesuaian (*non conformity*) dari hasil audit, monitoring, atau insiden keamanan, BPJPH wajib melakukan langkah-langkah sistematis, sebagai berikut:

1. Koreksi segera
   Melakukan tindakan instan untuk menghentikan dampak ketidaksesuaian;
2. Analisis akar masalah (*Root Cause Analysis*)
   Melakukan investigasi mendalam untuk menemukan penyebab fundamental masalah, bukan hanya gejala permukaan;
3. Rencana perbaikan
   Menyusun *Corrective Action Plan* yang memuat langkah spesifik, penanggung jawab, dan tenggat waktu penyelesaian;
4. Verifikasi efektivitas
   Memastikan tindakan perbaikan yang diambil telah efektif menghilangkan akar masalah dan mencegah kejadian serupa terulang di masa depan.

B. Peningkatan kapabilitas dan inovasi
BPJPH berkomitmen untuk meningkatkan maturitas Keamanan Informasi secara berkelanjutan melalui:
1. Pengembangan kompetensi SDM
Melaksanakan program pelatihan dan sertifikasi keamanan profesional (seperti *CISA, CISM, CISSP*) bagi tim teknis, serta program kesadaran keamanan (*Security Awareness*) rutin bagi seluruh pegawai;
2. Adopsi teknologi baru
Mengevaluasi dan mengadopsi teknologi pengamanan terkini (seperti *AI-based Threat Detection, Zero Trust Architecture*) yang relevan untuk meningkatkan efektivitas perlindungan; dan
3. *Benchmarking*
Melakukan studi banding dengan instansi pemerintah lain atau standard internasional terbaik untuk mengadopsi praktik-praktik unggulan dalam pengamanan data produk halal.

BAB VI
PENUTUP

Kebijakan ini disusun sebagai wujud komitmen BPJPH dalam menghadirkan layanan jaminan produk halal yang tidak hanya mudah dan cepat, namun juga aman dan terpercaya.

Kebijakan ini mulai berlaku secara efektif pada tanggal ditetapkan. Agar kebijakan ini dapat dilaksanakan secara operasional di lapangan, BPJPH akan segera menerbitkan dokumen turunan berupa pedoman pelaksanaan, SOP, dan instruksi kerja teknis.

Segala ketentuan terdahulu yang bertentangan dengan materi kebijakan ini dinyatakan tidak berlaku. Apabila di kemudian hari terdapat kekeliruan atau perubahan regulasi nasional yang signifikan, akan dilakukan peninjauan dan perbaikan sebagaimana mestinya.

KEPALA BADAN PENYELENGGARA
JAMINAN PRODUK HALAL
REPUBLIK INDONESIA,

ttd.

AHMAD HAIKAL HASAN

Salinan sesuai dengan aslinya
BADAN PENYELENGGARA JAMINAN
PRODUK HALAL
REPUBLIK INDONESIA
Kepala Biro Hukum, Sumber Daya Manusia
dan Hubungan Masyarakat,

Beny Cahyadie
NIP. 198204102000121001