PANDUAN MENGHADAPI
DATA BREACH

PUSAT OPERASI KEAMANAN SIBER NASIONAL

id-SIRTII
INDONESIA SECURITY INCIDENT RESPONSE TEAM ON INTERNET INFRASTRUCTURE

Panduan ini dipublikasikan oleh **Pusat Operasi Keamanan Siber Nasional (Pusopskamsinas) Badan Siber dan Sandi Negara (BSSN)**

DAFTAR ISI

BAGIAN 1: PENDAHULUAN

Kebocoran Data Pribadi

Berbicara mengenai data pribadi, merupakan hal yang cukup kompleks dikarenakan di Indonesia sendiri belum memiliki regulasi setingkat Undang-Undang yang mengatur hal tersebut. Sehingga pengaturannya tersebar di beberapa regulasi yang ada seperti UU Nomor 23 Tahun 2006 sebagaimana diubah oleh UU 24 Tahun 2013 tentang Administrasi Kependudukan, hingga Peraturan Menteri Kominfo Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik. Dalam Undang-Undang Nomor 14 Tahun 2008 Tentang Keterbukaan Informasi Publik, disampaikan bahwa setiap badan publik wajib membuka akses bagi setiap pemohon informasi publik untuk mendapatkan informasi publik, kecuali informasi publik yang apabila dibuka dan diberikan kepada pemohon dapat mengungkap rahasia pribadi. Namun demikian pendefinisian mengenai rahasia pribadi sendiri belum ada hal yang mengatur secara spesifik.

Adapun yang termasuk dalam rahasia pribadi adalah; riwayat dan kondisi anggota keluarga, riwayat kondisi dan perawatan, pengobatan, kesehatan fisik dan psikis seseorang, kondisi keuangan, aset, pendapatan, dan rekening bank seseorang, hasil evaluasi kapabilitas, intelektualitas, dan rekomendasi seseorang, dan/atau catatan menyangkut pribadi seseorang berkaitan dengan kegiatan satuan pendidikan formal dan satuan pendidikan nonformal.

Di era digital ini, sangat kecil kemungkinan bahwa pelaku bisnis tidak mengumpulkan atau memegang informasi mengenai identitas pribadi milik pelanggan, partner bisnis, siswa, atau pasien. Setidaknya, sebuah perusahaan atau badan pasti memiliki informasi mengenai karyawannya. Informasi mengenai identitias pribadi meliputi:

- NIK (Nomor Induk Kependudukan)
- Nama
- Alamat
- Tempat dan tanggal lahir
- Nomor rekening
- Email
- Password (bila terdaftar pada sistem internal)

Jika informasi pribadi ini jatuh ke pihak yang tidak bertanggung jawab, maka data pribadi tersebut menjadi resiko terhadap terjadinya pencurian identitas atau mungkin tindak kejahatan lainnya seperti penipuan, impersonasi, pemerasan dan lainnya. Meski tidak semua informasi pribadi yang terbuka dapat mengakibatkan pencurian identitias, namun informasi yang terbuka dapat menimbulkan dampak yang cukup besar.

Cara Bagaimana Kebocoran Data Terjadi

Terdapat 4 jenis cara bagaimana kebocoran data dapat terjadi, diantaranya adalah sebagai berikut:

1. Pencurian atau Hilangnya Perangkat Penyimpanan

Kebocoran data dapat disebabkan pencurian atau hilangnya peralatan fisik yang digunakan untuk menyimpan data, seperti hard disk, memory card, laptop, handphone, dan sebagainya.

2. Akses Ilegal Terhadap Sistem atau Informasi

Kebocoran data dapat terjadi ketika adanya akses terhadap sistem melalui cara yang melanggar hukum, seperti peretasan, virus, worms, ataupun trojan. Ketika dengan cara ini pelaku dapat memasuki sistem, ia dapat mencuri data, menginfeksi dengan mengubah atau menghapus data, ataupun merusak sistem agar data tidak dapat diakses.

3. Keterlibatan Orang Dalam

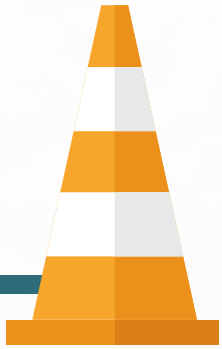
Kebocoran data dapat disebebkan oleh karyawan sebuah institusi itu sendiri, mantan karyawan, atau oleh karyawan yang berhasil dikelabui dengan social engineering sehingga tanpa sadar ia memberikan data ataupun akses terhadap data.

4. Kelalaian

Kebocoran data dapat disebabkan karena tidak memadainya sistem keamanan yang dimiliki. Hal ini termasuk juga tidak diterapkannya sistem atau protocol pengamanan dasar untuk pencegaahan terjadinya kebocoran data.

BAGIAN 2:

Persiapan Rencana Aksi Tanggap Kebocoran Data



Membentuk Incident Response Team

Sebuah institusi atau badan usaha yang memiliki atau memegang data mengani identitas pribadi, perlu melakukan langkah-langkah aksi cepat tanggap dalam menghadapi kemungkinan terjadinya kebocoran data. Untuk mempersiapkan aksi cepat tanggap terhadap kebocoran data, maka diperlukan langkah persiapan terlebih dahulu. Hal pertama yang perlu dimiliki oleh sebuah institusi adalah: *incident response team* atau tim cepat tanggap terhadap insiden.

Ketika insiden kebocoran data terjadi, tidak ada waktu untuk mencari atau menunjuk siapa yang bertanggung jawab atas insiden tersebut. Hal tercepat yang harus dilakukan adalah menangani insiden secara kolaboratif dengan tim yan terdiri dari berbagai ahli dan peran berbeda. *Incident response team* setidaknya terdiri dari:

1. Customer Care

Hal terpenting yang harus dilakukan oleh *customer care* adalah untuk selalu paham dan mengetahui insiden yang tengah terjadi serta perkembangan kasusnya karena mereka akan menjadi garda terdepan untuk menjawab pertanyaan-pertanyaan dari pelanggan. *Customer care* bertanggung jawab untuk:

- Menyusun dan mengembangkan draft untuk menjawab telepon, *frequently asked questions* (FAQ), dll.
- Mencatat volume panggilan dan pertanyaan atas kekhawatiran yang disampaikan oleh pelanggan.

2. Executive Leader

Executive Leader sebagai pembuat keputusan utama harus memiliki kepemimpinan dalam memberi dukungan dan sumber daya yang dibutuhkan dalam mengembangkan perencanaan, dan penanganan insiden. *Executive Leader* bertugas untuk:

- Memastikan keputusan yang dibuat oleh tim dapat disetujui oleh manajemen eksekutif.
- Memiliki jalur komunikasi yang baik dengan dewan direksi dan pemangku kepentingan lainnya seperti investor, dll.

3. Human Relation

Kebocoran data dapat juga mempengaruhi karyawan internal, untuk itu institusi perlu menunjuk perwakilan karyawan yang bertugas:

- Mengembangkan komunikasi internal untuk memberitahu seluruh karyawan atau mantan karyawan mengenai insiden.
- Mengatur rapat internal atau siaran web untuk karyawan untuk mengumpulkan informasi dari karyawan mengenai dampak dari kebocoran.

4. Incident Lead

Biasanya yang bertugas sebagai *incident leader* adalah *Chief Privacy Officer* dari internal atau departemen hukum eksternal yang akan memimpin dalam penanganan insiden dan bertugas untuk:

- Menentukan kapan *incident response team* akan diaktifkan secara penuh untuk menangani suatu insiden.
- Mengelola dan mengkoordinasikan aksi tanggap keseluruhan di perusahaan.
- Bertindak sebagai perantara antara *executive lead* dan anggota tim lain untuk melaporkan kemajuan serta permasalahan yang terjadi.
- Bertindak sebagai penghubung mitra eksternal.
- Memastikam dokumentasi yang tepat mengenai aksi cepat tanggap baik dalam hal proses maupun prosedur.

5. Legal

Terdiri dari pakar hukum, privasi, dan kepatuhan internal yang dapat membantu tim untuk meminimalkan resiko dan denda setelah terjadinya kebocoran data. Tim legal bertugas untuk:

- Menentukan strategi dan cara memberi tahu individu yan terpengaruh, media, penegak hukum, Lembaga pemerintah, dan pihak ketiga lainnya.
- Membangun hubungan dengan hukumeksternal yang diperlukan.
- Memberi nasihat atau masukan sebelum terjadi kebocoran data.
- Memeriksa semua dokumen atau materi tertulis yang terkait dengan insiden.

6. Information Technology (IT)

Tim IT dan Tim Keamanan IT akan memimpin dalam menghentikan kebocoran data, selain itu juga bertugas untuk:

- Mengidentifikasi risiko keamanan teratas untuk organisasi yang harus dimasukkan ke dalam rencana aksi cepat tanggap terhadap insiden.
- Melatih personil dalam melakukan aksi cepat tanggap terhadap insiden kebocoran data, termasuk mengamankan tempat dan mesin-mesin atau peralatan yang terinfeksi secara *offline*, dan menyimpan bukti-buktinya.
- Bekerja dengan pihak yang bergerak di bidang *forensic digital* untuk mengidentifikasi data yang bocor dan menghapus alat yang digunakan peretas (virus, malware, dll) tanpa merusak bukti-bukti kebocoran data.

7. Public Relation (PR)

Jika kebocoran data perlu dilaporkan ke media atau harus dipublikasikan dengan tujuan memberitahu individu yang terkena dampak, perwakilan PR bertugas untuk:

- Mengidentifikasi dan menyusun notifikasi atau pemberitahuan terbaik, serta menyusun strategi manajemen krisis sebelum insiden terjadi.
- Melacak dan menganalisis liputan media dengan cepat untuk setiap pemberitaan negative selama insiden terjadi.
- Membuat materi publikasi untuk konsumen/pelanggan mengenai insiden yang terjadi (melalui *website, media statement*, media sosial, dan lain-lain).

Menjalin Kerjasama Eksternal

Sebelum terjadinya insiden, maka kerjasama dengan pihak luar sangatlah diperlukan untuk membantu anda untuk lebih siap menghadapi insiden. Beberapa bidang yang perlu diperhatikan untuk menjadi partner eksternal adalah:

1. Komunikasi

Pihak eksternal dalam hal komunikasi sangat diperlukan untuk membantu anda dalam mengontrol publikasi isu, serta memberi nasihat untuk menghadapi pertanyaan media, publik, maupun konsumen mengenai insiden.

2. Forensik

Perusahaan yang menyediakan jasa di bidang forensik, khususnya *forensic digital*, akan membantu anda menelusuri penyebab kebocoran data. Selain itu juga dapat memberi anda nasihat bagaimana menghentikan kebocoran data serta mengamankan aset agar insiden tidak terjadi.

3. Penyedia Resolusi Kebocoran Data

Partner eksternal ini dapat membantu anda untuk menangani seluruh aspek mulai dari notifikasi atau pemberitahuan, *drafting, emailing*, dan sebagainya. Selain itu juga dapat membantu untuk memberikan rekomendasi produk perlindungan terhadap pencurian data.

4. Penasehat Hukum

Perusahaan harus bekerja sama dengan penasehat hukum yang sudah terkemuka utuk menjembatani tempo terjadinya insiden hingga tahap komunikasi. Mulai dari meminimalisir resiko secara hukum, hingga mendokumentasikan segala hal yang terjadi selama proses penanganan insiden.

5. Penegak Hukum dan Regulator Keamanan Siber

Koordinasi dengan pihak ini menjadi penting selain sebagai bentuk tanggung jawab terhadap hukum serta menjamin transparansi dalam proses investigasi yang dilakukan, proses tanggap insiden juga perlu mempertimbangkan untuk mengusut tuntas pelaku pembocoran data yang terjadi.

Selain itu, institusi juga dapat mengambil pilihan untuk membeli asuransi siber. Asuransi siber memberikan perlindungan finansial atas kerugian yang disebabkan oleh kebocoran data. Seiring dengan hal tersebut, kebijakan asuransi siber menawarkan beberapa sumber daya berharga lainnya, seperti: akses ke pengacara terkemuka, penyelidik forensik, penyedia solusi kebocoran data, serta perusahaan komunikasi yang dapat membantu anda untuk mengontrol insiden yang kompleks.

Penting bagi anda untuk memastikan bahwa komunikasi dimasukkan ke dalam proses aksi cepat tanggap yang lebih luas dan mengatur bagaimana organisasi akan membuat keputusan komunikasi utama, saluran yang digunakan, serta apa yang harus dikatakan dalam pernyataan mengenai insiden. Berikut adalah hal-hal penting yang perlu diperhatikan dalam strategi komunikasi:

1. Menunjuk perwakilan

   Pastikan perwakilan sebagai juru bicara adalah bagian dari *incident response team* dan mengikuti seluruh proses hukum dan forensik.

2. Memetakan Seluruh Proses

   Mendokumentasikan dengan baik seluruh proses penanganan insiden secara terperinci.

3. Menyiapkan kanal komunikasi khusus untuk berdiskusi dan berkomunikasi dengan karyawan, pelanggan, regulator, maupun mitra bisnis.

4. Menyiapkan bahan *template* untuk berkomunikasi dengan pihak-pihak tertentu. Misalnya: infomasi yang disampaian dengan pihak mitra kerja tentu berbeda dengan informasi yang disampaikan kepada pelanggan. Untuk itu perlu disusun draf *template* seperti FAQ, *script* untuk *call center,* dan lainnya.

5. Menguji komunikasi dengan simulasi dan bagaimana menghadapi tantangan untuk hadapi kebocoran media, keluhan pelanggan, pertanyaan dari karyawan, ataupun pertanyaan dari jaksa saat proses pengadilan.

Tindakan Persiapan

Pastikan setiap anggota tim memahami tanggung jawab masing-masing dalam menyiapkan dan merespon suatu pelanggaran. Setiap anggota tim bertanggung jawab untuk mengimplementasikan tindakan pencegahan dan mempersiapkan praktik terbaik untuk departemennya. Berikut adalah kegiatan atau tindakan yang harus dilakukan:

- Mengintegrasikan *smart data security* ke budaya kerja sehari-hari.
- Mengembangkan keamanan data dan kebijakan perangkat seluler, melakukan *update* secara rutin dan memberitahu ke pihak-pihak terkait.
- Menginvestasikan perangkat lunak keamanan siber, perangkat enkripsi dan *firewall.*
- Memperbaharui regulasi keamanan data secara rutin.
- Menerapkan hak akses untuk setiap tingkatan karyawan.
- Menerapkan mekanisme pelaporan bagi karyawan yang tidak mengikuti langkah-langkah keamanan yang telah dibuat.
- Memberikan pelatihan tentang keamanan data kepada karyawan paling sedikit sekali dalam setahun.

BAGIAN 3:

Pelaksanaan Aksi Tanggap Kebocoran Data

Menerapkan Simulasi Latihan

Seiring dengan meningkatnya kesadaran keamanan dan beberapa perusahaan atau Lembaga sudah memiliki rencana tanggapan (*response plan*). Namun berdasarkan data sekitar 1/3 perusahaan atau Lembaga belum mempraktikkan rencana tersebut. Oleh karena itu, untuk mengefektifkan setiap rencana harus dipraktikkan sesuai dengan langkah-langkah berikut:

1. Mengundang Fasilitator Eksternal

Mengundang ahli dari eksternal sebagai moderator dan narasumber latihan sehingga tim lebih fokus terhadap apa yang sedang dikerjakan.

2. Menjadwalkan Waktu yang Tepat

Menyediakan waktu kurang lebih 4 (empat) jam untuk melakukan latihan dan berdiskusi terhadap permasalahan yang dialami.

3. Memberlakukan ke Seluruh Karyawan

Menerapkan ke seluruh karyawan baik internal maupun eksternal karyawan yang bertanggungj awab terhadap kebocoran data termasuk (CEO, Tim IT, Tim Legal, Humas, Tim SDM, *Customer Service*, dan partner eksternal).

4. Menguji Banyak Skenario

Melakukan latihan di berbagai jenis situasi yang dapat terjadi sebelum, saat, dan setelah pelanggaran data terjadi.

5. Membuat Pertanyaan Setelah Latihan

Melakukan review dan mendiskusikan materi dari sesi latihan.

6. Melaksanakan Pelatihan Setiap 6 (Enam) Bulan

Melakukan pelatihan secara rutin untuk mengetahui perubahan dan perkembangan yang terjadi.

Mengembangkan Simulasi

Skenario simulasi harus sesuai dengan jenis industri, jenis data dan kesiapan infrastruktur TI perusahaan / Lembaga.

Skenario Sederhana :

- Pihiak BSSN menghubungi perusahaan dan memberitahukan bahwa data pelanggan dan passwordnya telah dijual di *Dark web*. BSSN merekomendasikan untuk dilakukan investigasi sebelum media mengetahui permasalahan ini.
- *Hacker* mengirimkan data konsumen perusahaan/Lembaga yang berisikan nama, alamat, password, dll. Kemudian, mereka mengancam akan menjual atau menyebarluaskan data tersebut kecuali perusahaan memenuhi permintaan *hacker* tersebut.
- Vendor perusahaan yang menangani data konsumen mencurigai pencurian data termasuk kedalam data *compromised.*
- Karyawan mengeluhkan bahwa mereka menerima email 5071-C dari IRS yang meminta informasi pribadi mereka. Hal ini bisa terjadi karena penyerang telah berhasil melakukan *phising* terhadap *email* korbannya.
- Organisasi telah menjadi target serangan *Ransomware.*

Kembangkan "Injects"

Dasar untuk setiap simulasi adalah menggunakan "injects" untuk memberikan informasi kejadian kepada peserta dan mengharuskan peserta bereaksi terhadap suatu perkembangan baru yang terjadi selama latihan. "Injects" ini membuat peserta mengambil keputusan untuk mengambil tindakan.

Kemungkinan Injeksi meliputi :

- Penyelidikan media dari reporter yang mengklaim memiliki informasi tentang kejadian dan berencana untuk menuliskannya.
- Surat dari Jaksa Agung yang mengancam penyelidikan atas suatu kejadian jika dia tidak menerima bukti secara rinci.
- Tim Forensik memberikan informasi terbaru ke tim IT tentang sistem yang terkena dampak.
- Email dari konsumen yang merasa dirugikan atas kejadian tersebut.

BAGIAN 4:

Proses Tanggap Insiden

Merespon insiden kebocoran data dapat membantu mengembalikan keamanan, menyimpan bukti dan melindungi reputasi. Pastikan untuk selalu megumpulkan, mendokumentasikan, dan mencatat informasi kebocoran data, berkoordinasi dengan penegak hukum, dan penasihat hukum.

Aksi Cepat Tanggap pada 24 Jam Pertama

Selalu mengumpulkan, mendokumentasikan, dan mencatat sebanyak mungkin informasi kebocoran data. Berikut adalah aksi yang perlu dilakukan pada 24 jam pertama insiden terjadi:

- Dokumentasikan hasil temuan kebocoran data (membentuk tim insiden respon ketika terjadi kebocoran data).
- Memberikan imbauan dan membentuk satgas (ikut sertakan semua orang dalam satgas termasuk pihak eksternal).
- Mengamankan area kebocoran data.
- Menghentikan kebocoran data selanjutnya (biarkan perangkat *offline* tetap dalam kondisi *offline*, hindari menghidupkan perangkat hingga tim forensik tiba).
- Dokumentasikan apapun (mencatat siapa yang menemukan kebocoran data, siapa yang melaporkan kebocoran data, siapa yang mengetahui kebocoran data, dan kebocoran data seperti apa yang terjadi).
- Wawancarai pihak-pihak terkait (pihak-pihak yang terlibat dan dokumentasikan hasil wawancara tersebut).
- *Review* protokol pemberitahuan (*review* orang yang terlibat dalam mempublikasikan informasi kebocoran data).
- Membuat skala prioritas dan risiko (membawa mitra forensik untuk menyelidiki lebih dalam).
- Laporkan kepada penegak hukum.

Langkah Selanjutnya

1. Identifikasi akar masalah.
2. Memberi imbauan kepada mitra eksternal.
3. Melanjutkan bekerja bersama forensik.
4. Mengidentifikasi kewajiban hukum.
5. Melaporkan pada pimpinan.
6. Mengidentifikasi inisiatif yang bertentangan.

Komunikasi dan Lindungi Reputasi

Untuk menghindari hilangnya reputasi, sebaiknya perusahaan menyiapkan strategi komunikasi sebelum terjadi insiden. Perusahaan harus memahami tentang investigasi kebocoran data dan komunikasikan fakta dengan tepat.

Berikut ini langkah-langkah komunikasi dengan konsumen :

- Asumsikan berita kebocoran data muncul sebelum perusahaan memiliki semua rincian dan rencanakan jawaban pertanyaan sebelum memiliki rincian tersebut.
- Menolak berspekulasi secara rinci sebelum dilakukan forensik.
- Jika perusahaan berkomitmen memberikan perlindungan data pribadi, maka pertimbangkan untuk menyebutkan komitmen tersebut dalam memberikan pernyataan.
- Lakukan pemantauan media tradisional dan sosial untuk mendeteksi kebocoran data yang dilakukan oleh pihak eksternal.
- Membuat situs web yang berfokus pada konsumen yang menjelaskan tentang apa yang terjadi dan langkah-langkah untuk melindungi diri.
- Berkomunikasi dengan regulator sejak awal.
- Memastikan karyawan yang berhubungan langsung dengan konsumen memiliki informasi dibutuhkan.

Layanan Konsumen

Pemberitahuan kebocoran data wajib diberikan kepada konsumen, biasanya dibutuhkan waktu 60 hari dari penemuan hingga pemberitahuan.

1. Pemberitahuan

Menjadi tanggung jawab perusahaan menentukan waktu pemberitahuan yang disesuaikan dengan peraturan yang berlaku. Tentukan waktu pemberitahuan sebelum terjadinya pelanggaran untuk meminimalisir terjadinya hal-hal yang tidak diinginkan.

2. Perlindungan Data Pribadi

Konsumen mengharapkan pemulihan kebocoran data. Banyak penyedia yang memberikan layanan perlindungan data pribadi, sebelum memilih layanan perlindungan data pribadi sebaiknya pahami dan mampu mengelola fitur produk. Adapun data yang harus dilindungi sebagai berikut :

- Laporan kredit konsumen.
- Pemantauan kredit.
- Pemantauan *Social Security Number* (SSN).
- *Dark web* dan peringatan *scanning* internet.
- Layanan penipuan.
- Asuransi pencurian data.

BAGIAN 5:

Melaksanakan Audit Data

Setelah membuat perencanaan, perusahaan seharusnya melakukan audit dan menguji perencanaan yang telah dibuat. Apakah perencanaan tersebut membantu mengatasi permasalahan masing-masing, termasuk pelanggaran internal, serangan eksternal, berbagi data tanpa sengaja dan kehilangan/pencurian perangkat fisik. Selalu perbaharui rencana perusahaan untuk menghindari ancaman baru yang tidak terduga yang muncul bulan atau tahun yang akan datang.

Fokus Area

Berikut ini beberapa area yang dilaksanakan audit :

1. Call Center

Persiapkan perwakilan *call center* ketika terjadi insiden kebocoran data atau mengumpulkan sumber daya eksternal untuk membantu mengelola meningkatnya volume panggilan. Selalu siap siaga menjawab panggilan konsumen untuk memperkuat reputasi dan komitmen perusahaan terhadap keamanan data konsumen.

2. Negosiasi Penyedia

Banyak perusahaan yang mengalami kebocoran data akibat penyedia. Perusahaan harus waspada memilih penyedia, pilih penyedia yang memiliki langkah-langkah keamanan yang sesuai dalam mengelola data yang mereka proses. Beberapa hal yang harus dipastikan :

- Memiliki program keamanan tertulis yang mencakup data perusahaan
- Hanya menggunakan data konsumen untuk layanan sesuai kontrak
- Mematuhi semua undang-undang keamanan data yang berlaku
- Mengembalikan atau menghancurkan data tepat di akhir kontrak

Audit Checklist

Berikut ini langkah yang disarankan untuk melakukan audit, namun disarankan menyesuaikan ruang lingkup rencana respon perusahaan yang dimiliki:

√ Perbaharui Daftar Kontak Tim

Periksa apakah informasi kontak anggota internal dan eksternal dari tim insiden respon kebocoran data diperbaharui dan hapus yang tidak diperlukan. Berikan daftar kepada pihak-pihak terkait.

√ Verifikasi Rencana Secara Komprehensif

Perbaharui perencanaan untuk mencegah terjadinya perubahan besar seperti bisnis, departemen, atau kebijakan. Verifikasi setiap anggota tim memahami perannya selama kebocoran data.

√ Periksa Kontrak Penyedia

Pastikan memiliki kontrak yang sah dengan forensik, penyedia kobocoran data, dan penyedia lainnya. Verifikasi kontrak dan penyedia masih sesuai ruang lingkup perusahaan.

√ Review Panduan Pemberitahuan

Pastikan bagian pemberitahuan dari rencana respon memperhitungkan peraturan terbaru dan perbaharui surat pemberitahuan jika diperlukan. Pastikan informasi kontak perusahaan untuk pengacara, lembaga pemerintah atau media yang perlu diberi tahu ketika terjadi kebocoran data.

√ Review Orang-Orang yang Dapat Mengakses Data

Mengkaji apakah penyedia memenuhi standar perlindungan dan memastikan menggunakan mengikuti aturan terbaru.

√ Evaluasi Keamanan

Memastikan kontrol akses data yang tepat. Memastikan pembaharuan sistem operasi dan pembaharuan perangkat lunak di seluruh perusahaan terinstal dengan benar dan cadangan kaset disimpan dengan aman.

√ Review Budaya Keamanan

Memastikan semua staff memahami tentang prosedur perlindungan data, termasuk data apa, dokumen, dan email yang harus disimpan dan yang harus dihapus dengan aman. Verifikasi staff secara aktif menjaga keamanan perangkat seluler dan laptop di dalam dan di luar kantor dan mengganti password setiap tiga bulan sekali.

SUMBER

[1] **AllClear ID: "Data Breach Incident Response Workbook"**

https://dpoacademy.gr/_files/200000035-ba715bc634/ACID_Self_Service_Incident_Response_Workbook.pdf

[2] **Experian: "Data Breach Response Guide"**

https://www.experian.com/assets/data-breach/brochures/response-guide.pdf

PUSAT OPERASI KEAMANAN SIBER NASIONAL

Id-SIRTII
INDONESIA SECURITY INCIDENT RESPONSE TEAM ON INTERNET INFRASTRUCTURE

Pusopskamsinas
Badan Siber dan Sandi Negara
Republik Indonesia