TEMPLATE RENCANA TANGGAP INSIDEN SIBER

CYBER INCIDENT RESPONSE PLAN TEMPLATE

Restia Moegiono, S.ST {CEH|CHFI|ECSA|QRMO}

TLP : CLEAR
Dokumen ini bisa disebarluaskan secara bebas

[Tambahkan informasi klasifikasi dokumen]

DAFTAR ISI

1. Pendahuluan

1.1 Latar Belakang

Keamanan siber berkaitan dengan kerahasiaan (*confidentiality*), ketersediaan (*availability*), dan integritas (*integrity*) informasi yang diproses, disimpan, dan dikomunikasikan dengan cara digital, serta upaya untuk melindungi informasi dan sistem elektronik dari ancaman eksternal atau internal. Keamanan siber melibatkan perlindungan informasi penting dan infrastruktur TIK melalui penyelarasan antara *people*, *process*, dan *technology*.

Karena teknologi yang menopang infrastruktur TIK dan sistem elektronik terus berkembang, penjahat siber juga meningkatkan keterampilannya dan memanfaatkan teknologi untuk melakukan serangan siber dengan tujuan menipu uang, mengganggu operasional bisnis, atau melakukan spionase. Selain itu, teknologi canggih juga kompleks, yang mengarah pada kesalahan manusia (*human error*) dan kesalahan alur kerja seperti kesalahan konfigurasi dan perilaku keamanan siber yang tidak memenuhi praktik terbaik.

Dokumen Rencana Tanggap Insiden Siber ini mendukung <organisasi> dalam mengelola insiden siber. Diharapkan dengan adanya penerapan dokumen ini akan mendukung <organisasi> dalam mengurangi ruang lingkup, dampak, dan keparahan insiden siber.

1.2 Tujuan

Dokumen Rencana Tanggap Insiden Siber ini menjelaskan proses yang diperlukan untuk memastikan pendekatan terorganisir untuk mengelola insiden siber di dalam <organisasi> dan mengoordinasikan upaya tanggap insiden siber untuk mencegah atau membatasi kerusakan yang mungkin ditimbulkan.

1.3 Tanggung Jawab

Rencana Tanggap Insiden Siber ini dikelola oleh <Tim Tanggap Insiden Siber> yang bertanggung jawab untuk memastikan bahwa <organisasi> memiliki lingkungan TIK yang dapat diandalkan dan aman.

1.4 Reviu

Rencana Tanggap Insiden Siber ini akan direviu setiap tahun oleh <Tim Tanggap Insiden Siber> atau sesuai dengan kebutuhan tanggap insiden siber yang dianggap perlu oleh <organisasi>.

[Tambahkan informasi klasifikasi dokumen]

1.5 Definisi

1. Insiden siber adalah kejadian yang mengganggu atau mengancam berjalannya Sistem Elektronik dan/atau pelanggaran kepatuhan terhadap kebijakan keamanan siber. Contoh insiden siber meliputi (namun tidak terbatas pada):
   a. Serangan *Denial of Service* (DoS) yang memengaruhi ketersediaan sistem atau layanan.
   b. Serangan virus atau *malware*.
   c. Kompromi atau pengungkapan informasi sensitif.
   d. Kompromi kredensial jaringan atau akun *email*.
2. Kejadian/peristiwa pada sistem elektronik adalah segala aktivitas yang terjadi pada sistem elektronik. Kejadian/peristiwa memiliki potensi untuk menjadi insiden siber, tetapi tidak selalu bisa dipastikan. Contoh kejadian/peristiwa siber meliputi (namun tidak terbatas):
   a. Beberapa *logon* berurutan yang gagal untuk satu pengguna.
   b. Seorang pengguna telah menonaktifkan aplikasi antivirus di komputernya.
   c. Pengguna telah menghapus atau mengubah *file* sistem.
   d. Pengguna me-*restart* server.
   e. Akses tidak sah ke *server* atau sistem elektronik.

2. Insiden Siber dan Tanggap Insiden Siber Minimum

Tabel berikut menyediakan daftar jenis insiden siber yang umum, bersama dengan aktivitas tanggap insiden siber yang sesuai (tanggap insiden siber minimum).

Tabel 1. Insiden siber dan tanggap insiden siber minimum

No.	Insiden Siber	Tanggap Insiden Siber Minimum
Jelaskan secara singkat tanggap insiden siber awal yang akan dilakukan. Misalnya, beri tahu personel yang relevan, aktifkan Rencana Tanggap Insiden Siber, isolasi perangkat yang terdampak, ikuti prosedur tanggap insiden yang relevan.		
1.	***Ransomware*** yaitu *malware* yang mengenkripsi atau mengunci data korban hingga uang tebusan dibayarkan.	Segera isolasi perangkat yang terinfeksi dari jaringan untuk membatasi penyebaran *ransomware*. Ambil semua *log* yang tersedia yang relevan dengan perangkat untuk melakukan analisis dan pemulihan.
2.	**Infeksi *Malware*** yaitu virus, worm, Trojan horse, atau entitas jahat berbasis kode lainnya yang berhasil menginfeksi *host*.	Segera isolasi perangkat yang terinfeksi dari jaringan untuk membatasi penyebaran *malware*. Ambil semua log yang tersedia yang relevan dengan perangkat untuk melakukan analisis dan pemulihan.
3.	**Serangan *Denial of Service* (DoS) dan *Distributed Denial of Service* (DDoS)** yaitu serangan yang membanjiri jaringan TIK dengan lalu lintas yang tidak dapat diprosesnya sehingga menyebabkan kegagalan jaringan.	Meminta *Internet Service Provider* (ISP) untuk mengidentifikasi sifat DOS/DDOS, vektor serangan, dan mengimplementasikan solusi yang sesuai. Berkoordinasi dengan ISP dan tim jaringan untuk menerapkan *filter* di tepi jaringan (*network edge*) dan/atau meningkatkan kapasitas.
4.	***Phishing* dan *Social Engineering*** yaitu upaya pengelabuhan yang dirancang untuk memperoleh informasi sensitif pengguna.	Meninjau *log* pengguna yang terpengaruh (*log web* dan *email*) untuk menentukan apakah terdapat tautan (*link*) atau lampiran (*attachment*) berbahaya yang telah diakses. Berkonsultasilah dengan pengguna untuk mengonfirmasi tindakan yang sudah dilakukan, dan apakah ada informasi pribadi/sensitif yang diberikan sebagai tanggapan atas upaya *phishing*/*social engineering*. Pertimbangkan untuk mengatur ulang *password* pengguna dan memantau akun untuk setiap akses yang tidak sah.
5.	**Pelanggaran data (*data breach*)** yaitu akses tidak sah ke informasi sensitif atau informasi pribadi.	Memeriksa jejak eksfiltrasi data ke luar jaringan sesegera mungkin untuk menyelidiki penyebab kebocoran data. Tim tanggap insiden siber, tim hukum, dan tim komunikasi publik harus siaga.

3. Potensi Vektor Ancaman

Ada beberapa vektor di mana insiden siber dapat muncul. Mempertahankan kesadaran akan vektor ancaman ini akan mendukung <organisasi> dalam mengidentifikasi potensi 'titik lemah' atau aspek yang umumnya menjadi sasaran jaringan dan sistem Anda. Beberapa vektor yang lebih umum termasuk:

Tabel 2. Potensi vektor ancaman.

No.	Vektor Ancaman	Deskripsi
1.	Media penyimpanan portabel/eksternal	Serangan dilakukan dari USB yang mengandung *malware*
2.	Jaringan	Serangan DDoS pada jaringan atau sistem kritis
3.	*Web*	Pengalihan lalu lintas *web* ke URL berbahaya yang dapat menginstal *malware* di perangkat korban
4.	*Email*	Serangan *phishing* yang berupaya mencuri informasi dan/atau menyebarkan *malware* ke perangkat korban
5.	Upaya peniruan (*impersonation*)	Misalnya, domain yang dibuat untuk meniru sistem elektronik milik organisasi dalam upaya menipu korban (biasanya terkait dengan serangan *phishing*)
6.	Penggunaan TIK yang tidak benar	Kesalahan manusia (*human error*) yang mengakibatkan pelanggaran kebijakan keamanan informasi atau serangan dari orang dalam yang bermaksud jahat (*insider threat*) sehingga mengakibatkan insiden siber.

4. Peran dan Tanggung Jawab

Bagian berikut merinci komposisi dan fungsi pada Tim Tanggap Insiden Siber dan Komite Pengarah Keamanan Informasi pada <organisasi>.

4.1 Tim Tanggap Insiden Siber

Anggota Tim Tanggap Insiden Siber <organisasi> antara lain:

Nama	Kontak	Jabatan	Peran pada Tim	Tanggung Jawab
			Ketua Tim Tanggap Insiden Siber	▪ Perencanaan tanggap insiden siber ▪ Operasional Tim Tanggap Insiden Siber
			Wakil Ketua Tim Tanggap Insiden Siber	▪ Analisis situasi ▪ Intelijen ancaman (*threat intelligence*) ▪ Saran teknis
			Koordinator teknis	▪ Investigasi (jika dicurigai adanya ancaman orang dalam) ▪ Penghubung untuk upaya penegakan hukum
			Staf Penanggap Insiden (*incident responder*)	▪ Investigasi teknis (pengumpulan dan pemrosesan data jaringan dan *host*) ▪ Upaya penahanan, perbaikan dan pemulihan ▪ Laporan investigasi
			Staf Komunikasi dan Media	▪ Informasi dan peringatan ▪ Komunikasi internal ▪ Penghubung/juru bicara media dan masyarakat

Untuk insiden siber yang lebih signifikan, Tim Tanggap Insiden Siber dapat diperluas untuk mencakup:

Nama	Kontak	Jabatan	Peran pada Tim	Tanggung Jawab
			Penasihat kelangsungan bisnis	▪ Dukungan fasilitas ▪ Analisis/manajemen bisnis dan masyarakat
			Penasihat hukum	Layanan penasihat hukum (termasuk kepatuhan terhadap peraturan)
			Penasihat keuangan dan pengadaan	Fasilitas dan dukungan keuangan
			Administrasi dan pencatatan	Dukungan administrasi, termasuk *log* Insiden dan laporan

4.2 Komite Pengarah Keamanan Informasi

Insiden siber yang lebih serius mungkin memerlukan pembentukan Komite Pengarah Keamanan Informasi <organisasi>. Komite Pengarah Keamanan Informasi harus memberikan pengawasan strategis, arahan dan dukungan kepada Tim Tanggap Insiden Siber dengan berfokus pada:

- Identifikasi dan pengelolaan isu-isu strategis pada keamanan informasi.
- Pelibatan dan komunikasi dengan berbagai pihak, seperti regulator dan pemangku kepentingan (*stakeholder*).
- Pemantauan sumber daya dan kapabilitas Tim Tanggap Insiden Siber, termasuk kebutuhan logistik atau keuangan yang mendesak, dan pertimbangan sumber daya manusia selama upaya tanggap insiden siber.

Jika Komite Pengarah Keamanan Informasi tidak dapat dibentuk, maka pastikan ada pihak manajemen dalam organisasi yang memiliki kewenangan untuk membuat keputusan penting.

Nama	Kontak	Jabatan	Peran/Tanggung Jawab
		Pimpinan tertinggi organisasi	Ketua Komite Pengarah Keamanan Informasi
		Kepala unit kerja yang membawahi fungsi TI	Wakil Komite Pengarah Keamanan Informasi
		Kepala Bagian yang membawahi fungsi keamanan siber	Sekretaris Komite Pengarah Keamanan Informasi
		Kepala unit kerja yang membawahi fungsi keuangan/pengadaan	Pengadaan darurat dan pengawasan pengeluaran
		Kepala unit kerja yang membawahi fungsi hukum	Kepatuhan terhadap peraturan; asuransi siber
		Kepala unit kerja yang membawahi fungsi komunikasi publik	Hubungan masyarakat dan keterlibatan pemangku kepentingan
		Kepala unit kerja yang membawahi fungsi SDM	Manajemen kesejahteraan staf

4.3 Bantuan Tanggap Insiden Siber

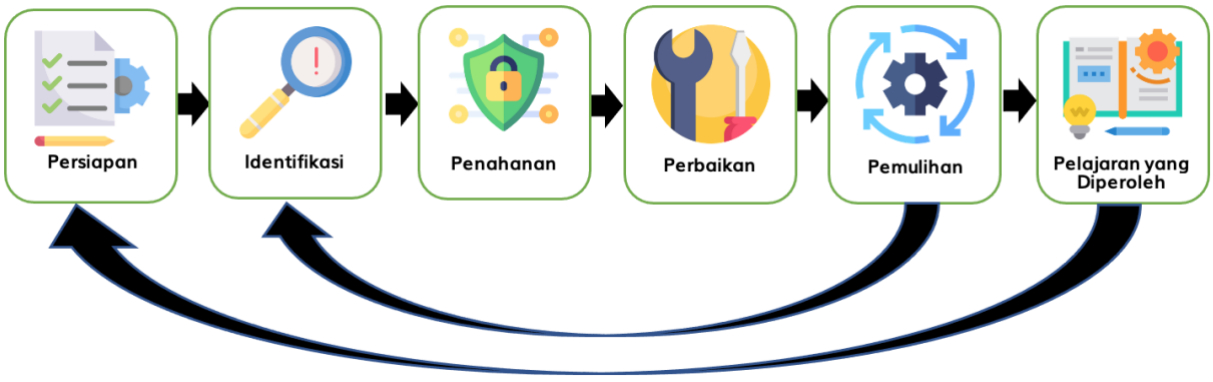
Untuk mendapatkan bantuan dalam melakukan tanggap insiden siber, dapat menghubungi Badan Siber dan Sandi Negara (BSSN) melalui layanan aduan siber pada nomor telepon (021) 78833610 atau *email* pada bantuan70@bssn.go.id.

5. Proses Tanggap Insiden Siber

5.1 Daftar Referensi Cepat Tanggap Insiden Siber

Tabel 3. Daftar referensi cepat tanggap insiden siber.

No.	Aktivitas
1.	Melakukan analisis untuk menentukan apakah suatu insiden telah terjadi atau sedang terjadi.
2.	Menentukan ruang lingkup, dampak, tingkat keparahan insiden, dan mengkategorikan insiden siber tersebut.
3.	Jika perlu, hubungi Komite Pengarah Keamanan Informasi untuk melaporkan insiden siber yang terjadi.
4.	Mengembangkan dan menerapkan Rencana Tanggap Insiden Siber yang merinci kegiatan tanggap insiden siber.
5.	Mengidentifikasi pemangku kepentingan yang terdampak insiden siber tersebut.
6.	Menerapkan strategi dalam memberitahukan pemangku kepentingan yang terdampak insiden siber tersebut.
7.	Mengkonfirmasi ancaman telah dihapus dan mengembalikan sistem/layanan yang terdampak ke fungsi normal (uji sistem/layanan untuk mengkonfirmasi fungsionalitas yang diharapkan)
8.	Menyatakan tanggap insiden siber telah selesai dilakukan dan memastikan pemenuhan persyaratan yang diperlukan sebelum melakukan komunikasi dengan pemangku kepentingan.
9.	Lakukan reviu pasca insiden untuk mengidentifikasi hal-hal yang berjalan dengan baik dan setiap peluang untuk perbaikan, serta mendokumentasikan pembelajaran yang didapatkan dari insiden siber.
10.	Perbarui Rencana Tanggap Insiden Siber untuk menyertakan pembelajaran insiden siber.



Gambar 1. Siklus tanggap insiden siber.

5.2 Tahap 1: Persiapan

Persiapan pada siklus tanggap insiden sangat penting karena tidak hanya menetapkan kemampuan tanggap insiden, tetapi juga mencegah insiden dengan memastikan bahwa sistem, jaringan, dan aplikasi dalam keadaan yang cukup aman. Tahap ini berisikan persiapan untuk menangani insiden dan pencegahan insiden yang bertujuan untuk membangun kontak, menentukan prosedur, dan mengumpulkan informasi untuk menghemat waktu selama insiden. Langkah-langkah pada tahap persiapan, antara lain:

1. Pastikan sudah memiliki skema terkini yang menggambarkan sistem, jaringan, dan aplikasi.
2. Menyiapkan sistem, jaringan, dan aplikasi cadangan yang siap pakai jika sumber daya utama mengalami kegagalan operasional.
3. Menetapkan prosedur untuk mengalihkan pengguna ke sistem, jaringan, dan aplikasi cadangan untuk memastikan keberlangsungan proses bisnis.
4. Menerapkan alat pemantauan dan pencegahan intrusi untuk mendeteksi dan mencegah aktivitas abnormal yang menargetkan sistem, jaringan, dan aplikasi yang penting.
5. Melakukan manajemen log terpusat dan memastikan jam sudah disinkronkan.
6. Menerapkan aturan deteksi serangan dan eksploitasi kerentanan berdasarkan manajemen log terpusat dan memantaunya.
7. Mengaudit aplikasi sebelum dirilis dan melakukan pemantauan secara berkala.
8. Mendata kontak operasional pihak penyedia jasa TI.
9. Memastikan pihak penyedia jasa TI menerapkan kebijakan keamanan informasi dan memverifikasi kepatuhan kontraktual.
10. Menyiapkan *template* komunikasi jika insiden siber terlihat oleh pengguna dan perlu dijelaskan.

5.3 Tahap 2: Identifikasi

Tahap ini bertujuan untuk mendeteksi insiden siber, menentukan ruang lingkupnya, dan melibatkan pihak yang tepat.

5.3.1 Deteksi Insiden

Tidak ada proses tunggal untuk mendeteksi insiden siber. Deteksi sering melibatkan:

1. Prekursor, yaitu mendeteksi bahwa serangan siber mungkin terjadi di masa mendatang, seperti penerimaan *email phishing* atau berita tentang serangan *malware/ransomware* global (catatan: bentuk deteksi ini jarang terjadi).

2. Indikator, yaitu deteksi bahwa suatu insiden mungkin telah terjadi. Misalnya, peringatan deteksi intrusi, nama *file* dengan karakter aneh, perubahan konfigurasi.
3. Pemantauan keamanan (*security monitoring*), yaitu rujukan dari *Managed Security Service Provider* (MSSP) atau organisasi/pemangku kepentingan lain, mengingatkan adanya insiden siber.

Tabel di bawah memberikan beberapa indikator umum yang menunjukkan bahwa organisasi mungkin mengalami insiden siber.

Tabel 4. Indikator insiden siber.

Indikator	Contoh
Laporan aktivitas yang tidak biasa atau mencurigakan oleh staf atau pemangku kepentingan eksternal.	Seorang personel menerima *email* yang menyampaikan permintaan untuk mengonfirmasi kredensial jaringan atau memberikan informasi pribadi atau sensitif lainnya.
	Beberapa personel melaporkan akun jaringannya terkunci.
	Laporan pemangku kepentingan menerima *email* berupa *spam* atau *phishing* dari organisasi.
	Anggota masyarakat melaporkan temuan kerentanan atau eksploitasi keamanan.
Sistem/layanan tidak beroperasi atau berfungsi seperti yang diharapkan	Satu atau lebih sistem atau layanan TI mungkin berhenti berfungsi, atau tidak berfungsi seperti yang diharapkan, dan tidak ada penyebab yang dapat diidentifikasi dengan mudah.
	Sertifikat SSL rusak, sehingga pelanggan mengeluh bahwa situs web organisasi memiliki tautan yang rusak.
Aktivitas yang tidak biasa	Administrator jaringan mengamati sejumlah besar *email* tidak bisa masuk karena berisi konten yang mencurigakan (*suspicious*); atau ada perubahan substansial dalam arus lalu lintas jaringan tanpa penyebab yang dapat diidentifikasi dengan mudah.
	Log jaringan atau aplikasi menunjukkan beberapa upaya *login* yang gagal dari sistem jarak jauh yang tidak dikenal, seperti lokasi di luar negeri.
	Pemberitahuan dari aplikasi anti-virus tau penyedia layanan terkelola yang telah mendeteksi aktivitas atau *file* yang mencurigakan di jaringan organisasi, sehingga memerlukan analisis dan perbaikan.
	Izin pengubahan izin akun layanan atau admin, akun admin menambahkan pengguna standar ke grup, atau akun layanan masuk ke *workstation*.
	Administrator sistem mengamati nama *file* dengan karakter yang tidak biasa, atau *file* yang diharapkan tidak lagi terlihat di jaringan.

5.3.2 Analisis Insiden

Setelah mempertimbangkan indikator potensi insiden siber, penting untuk memastikan apakah insiden telah atau terus terjadi. Tabel berikut mengidentifikasi langkah-langkah yang berguna untuk memastikan adanya insiden siber.

Tabel 5. Analisis insiden.

Tindakan	Deskripsi
Melakukan pembaruan pada sumber daya	Pastikan Anda memiliki akses ke yang terbaru: ▪ Diagram jaringan. ▪ Skema IP *address*. ▪ Daftar *port*. ▪ Dokumentasi yang mungkin mencakup desain/arsitektur sistem, rencana keamanan, konfigurasi GPO, dan lain-lain.
Meninjau entri *log* dan peringatan keamanan	Apakah ada entri yang tidak biasa atau tanda-tanda perilaku mencurigakan di jaringan atau aplikasi?
Memiliki *Standard Operating Procedure* (SOP) untuk sistem operasi yang berbeda	Untuk *workstation* Windows, ikuti SOP tentang apa yang harus dicari atau ditinjau (yaitu sumber *event log* tertentu, jenis *event* yang akan dicari, dan lain-lain). Hal yang sama berlaku untuk sistem operasi Linux dan Unix.
Konsultasikan dengan pakar jaringan dan aplikasi	Apakah ada penjelasan yang sah untuk aktivitas yang tidak biasa atau mencurigakan yang diamati?
Melakukan riset	Teliti dan tinjau semua materi *open source* (termasuk melalui *search engine* internet) yang berkaitan dengan aktivitas yang tidak biasa atau mencurigakan yang diamati (misalnya, pertimbangkan untuk melakukan pencarian pada nama *file* yang tidak biasa yang diamati di jaringan).
Daftar pantau	Mambuat daftar akun atau IP *address* yang dicurigai dapat ditambahkan untuk memantau aktivitas yang sedang berlangsung.
Penting	Jangan melakukan 'ping' atau mencoba berkomunikasi dengan IP *address* atau URL yang dicurigai dari jaringan sendiri, karena tindakan demikian dapat memberi tahu penyerang bahwa aktivitas mereka telah dideteksi. Ini harus dilakukan oleh pihak ketiga yang dapat melakukan aktivitas ini dengan aman dan *anonymous*.

Penting untuk mempertimbangkan ketepatan waktu analisis insiden siber. Analisis yang panjang berguna untuk mengembangkan pemahaman yang komprehensif tentang suatu insiden tetapi juga dapat menghambat proses tanggap insiden siber secara keseluruhan. Umumnya, disarankan untuk menghabiskan waktu hingga 1 (satu) jam pada fase analisis insiden awal sebelum mencari bantuan dari luar.

5.3.3 Klasifikasi Insiden Siber

Tabel berikut memberikan panduan untuk mengklasifikasikan kategori insiden siber dan juga memberikan indikator untuk dipertimbangkan saat menentukan apakah insiden siber meningkat atau menurun dalam dampak dan tingkat keparahannya.

Tabel 6.Klasifikasi insiden.

Klasifikasi Insiden	Dampak
Kritikal	▪ Lebih dari 80% personel tidak dapat bekerja ▪ Sistem kritis berhenti beroperasional ▪ Terjadi/risiko tinggi terhadap kebocoran data berskala besar yang meliputi data sensitif organisasi atau data pribadi pelanggan ▪ Dampak finansial lebih besar dari 100 miliar rupiah ▪ Kerusakan reputasi yang parah dan kemungkinan berdampak pada bisnis dalam jangka panjang
Tinggi	▪ Sekitar 50% personel tidak dapat bekerja ▪ Sistem yang tidak kritis terdampak ▪ Terdapat risiko kebocoran data berskala kecil yang meliputi data sensitif organisasi atau data pribadi pelanggan ▪ Dampak keuangan 1-99 miliar rupiah ▪ Potensi kerusakan reputasi yang serius
Sedang	▪ Sekitar 20% personel tidak dapat bekerja ▪ Terdapat beberapa sistem non-kritis terdampak ▪ Terdapat risiko kebocoran sejumlah kecil data organisasi non-sensitif ▪ Dampak keuangan 100-999 juta ▪ Terdapat risiko rendah terhadap reputasi
Rendah	▪ Sekitar <10% personel terkena dampak sementara (jangka pendek) ▪ Terdapat sistem yang dampak minimal, jika ada ▪ Terdapat satu atau dua sistem non-sensitif/non-kritis yang terdampak ▪ Tidak ada kebocoran data ▪ Risiko reputasi yang dapat diabaikan

5.3.4 Koordinasi Tim Tanggap Insiden Siber

Jika insiden siber telah terkonfirmasi, maka perlu dilakukan koordinasi dengan Tim Tanggap Insiden Siber untuk mengelola upaya tanggap insiden siber tersebut. Tim Tanggap Insiden Siber berada di <detail ruangan> atau hubungi <detail kontak berupa telepon dan alamat email> pada waktu operasionalnya yaitu pada hari <hari operasional> dan waktu <waktu operasional>.

5.3.5 Pemberitahuan Insiden Siber

Penting untuk memberi tahu pemangku kepentingan terkait bahwa insiden siber telah terjadi atau sedang terjadi. Cakupan, dampak, dan tingkat keparahan insiden siber harus menentukan sejauh mana pemberitahuan kepada pemangku kepentingan. Insiden siber yang lebih serius kemungkinan akan membutuhkan keterlibatan dengan pemangku kepentingan yang lebih luas.

Pemangku kepentingan yang harus diberitahukan meliputi:

1. Layanan aduan insiden siber BSSN (24/7), dimana pemberitahuan segera diperlukan untuk insiden siber dan keadaan darurat yang signifikan.
2. Komite Pengarah Keamanan Informasi, namun jika tidak ada maka dapat menghubungi pihak manajemen dalam organisasi yang memiliki kewenangan untuk membuat keputusan penting.
3. Instansi pemerintah dan regulator terkait organisasi.
4. Penyedia asuransi siber organisasi, jika ada.

Ketua Tim Tanggap Insiden Siber bertanggung jawab untuk mengelola pemberitahuan ini atas nama <organisasi>.

Catatan: pertimbangkan untuk mengembangkan daftar pemangku kepentingan yang relevan dengan setiap kategori insiden siber.

5.3.6 Dokumentasi Tim Tanggap Insiden Siber

Tim Tanggap Insiden Siber harus segera mendokumentasikan informasi tentang insiden siber yang mencakup pembaruan situasi (Lampiran A) dan catatan insiden siber (Lampiran B).

Pembaruan situasi harus berisi informasi berikut:

1. Tanggal dan waktu insiden siber, biasanya tanggal dan waktu insiden siber terkonfirmasi.
2. Status insiden siber, misalnya, baru/sedang berlangsung/terselesaikan.
3. Jenis dan klasifikasi insiden siber, misalnya, *malware*/*website hacking*/DDoS.
4. Cakupan insiden siber (*scope*), misalnya detail jaringan, sistem, dan/atau aplikasi yang terdampak.
5. Dampak insiden siber (*impact*), yaitu rincian entitas yang terkena dampak insiden, dan bagaimana dampak insiden siber yang terjadi.
6. Keparahan (*severity*), yaitu tingkat keparahan dampak insiden terhadap organisasi berupa kritikal, tinggi, sedang, atau rendah.

7. Perincian kontak untuk Ketua Tim Tanggap Insiden Siber dan personel yang bertugas.

Pembaruan situasi harus disiapkan dan disebarluaskan kepada pemangku kepentingan internal <organisasi> secara berkala. Penting untuk bersikap proaktif dengan pengembangan dan penyebaran informasi pembaruan situasi, guna mengurangi kebutuhan pemangku kepentingan untuk mendekati Tim Tanggap Insiden Siber dengan berbagai pertanyaan tentang insiden siber tersebut.

Catatan insidensiber harus dipelihara oleh anggota Tim Tanggap Insiden Siber yang berisi risalah dari setiap rapat Tim Tanggap Insiden Siber, perincian semua keputusan penting (termasuk alasan keputusan), tindakan operasional yang diambil, dan rencana rapat di selanjutnya. Setiap entri ke catatan insiden siber harus menyertakan detail tanggal, waktu, dan nama penulis.

5.4 Tahap 3: Penahanan (*Containment*)

Tahap ini bertujuan untuk mengurangi efek serangan terhadap lingkungan yang ditargetkan.

5.4.1 Rencana Aksi

Tim Tanggap Insiden Siber harus mengembangkan rencana aksi (Lampiran C) untuk menyelesaikan insiden siber. Rencana aksi ini harus mempertimbangkan langkah-langkah yang dilakukan segera yang diperlukan untuk mengatasi insiden siber dan menghapus setiap ancaman yang mungkin ada, serta langkah-langkah yang diperlukan untuk memulihkan sistem dan layanan. Rencana aksi ini harus ditinjau selama proses karena dapat berubah tergantung pada bukti apa yang diperoleh selama langkah deteksi dan analisis.

Elemen kunci dari rencana aksi ini adalah:

1. Tindakan penahanan, yaitu apa yang dilakukan sekarang untuk mengendalikan insiden siber dan mencegah penyebaran dampak insiden siber?
2. Tindakan perbaikan, yaitu apa yang dilakukan untuk menghilangkan ancaman dan menghindari terjadinya insiden siber di masa depan.
3. Persyaratan kemampuan dan kapasitas, yaitu sumber daya apa yang diperlukan agar rencana aksi berhasil.
4. Tindakan komunikasi, yaitu pesan apa yang harus dikomunikasikan, kepada siapa, kapan dan bagaimana.

Catatan: detail rencana aksi akan bervariasi tergantung pada jenis insiden siber yang dialami. Tidak ada pendekatan rencana aksi yang cocok untuk semua.

Saat mengembangkan rencana aksi, penting untuk mempertimbangkan:

1. Berapa lama waktu yang dibutuhkan untuk menyelesaikan insiden siber?
2. Sumber daya apa yang diperlukan untuk menyelesaikan insiden siber (jika belum termasuk dalam Tim Tanggap Insiden Siber)?
3. Sistem/layanan apa yang akan terpengaruh selama proses penahanan, perbaikan, dan pemulihan?

5.4.2 Tindakan Penahanan (*Containment*)

Tindakan penahanan bervariasi berdasarkan jenis insiden siber. Organisasi harus membuat tindakan penahanan terpisah untuk setiap jenis insiden besa, dengan kriteria yang didokumentasikan dengan jelas untuk memfasilitasi pengambilan keputusan. Kriteria penentuan tindakan penahanan yang tepat mempertimbangkan hal-hal berikut:

1. Potensi kerusakan dan pencurian sumber daya.
2. Kebutuhan untuk menyimpan bukti (*evidence*).
3. Ketersediaan layanan.
4. Waktu dan sumber daya yang dibutuhkan untuk menerapkan tindakan penahanan.
5. Keefektifan strategi, misalnya penahanan sebagian, penahanan penuh.
6. Durasi solusi yang diterapkan, misalnya solusi darurat akan dihapus dalam 4 (empat) jam, solusi sementara akan dihapus dalam 2 (dua) minggu, dan solusi permanen.

Tabel 7. Penahanan insiden siber.

Tindakan	Deskripsi
Putuskan sambungan area yang terinfeksi dari internet	▪ Isolasi area yang terinfeksi *malware*, putuskan sambungannya dari jaringan apa pun. ▪ Jika lalu lintas bisnis penting tidak dapat diputuskan, sambungkan kembali setelah memastikan bahwa sambungan tersebut tidak dapat menjadi vektor infeksi *malware* atau temukan teknik pengelakan (*circumventions*) yang tervalidasi. ▪ Menetralkan vektor propagasi, dapat berupa apa saja mulai dari lalu lintas jaringan hingga kerentanan perangkat lunak. Tindakan yang relevan harus diterapkan, misalnya tambalan (*patch*), pemblokiran lalu lintas, penonaktifan perangkat.

Tindakan	Deskripsi
Menarapkan *tools* untuk memperketat kontrol keamanan	Memperketat kontrol keamanan menggunakan: ▪ EDR. ▪ *Tools* penerapan *patch*, seperti *Windows Server Update Services* (WSUS). ▪ Windows Group Policy *Object* (GPO). ▪ Aturan *firewall*. ▪ Prosedur operasional.
Instruksi kepada pengguna *end user*	Meminta pengguna *end user* untuk mengikuti arahan dengan tepat.
Mematikan perangkat dengan cara yang kasar (*hard way*)	Jika aset informasi tidak dianggap kritis untuk organisasi dan dapat diputuskan dari jaringan, maka matikan aset informasi dengan cara yang kasar (*hard way*), yaitu: ▪ Cabut steker listriknya. ▪ Jika aset informasi berupa laptop dengan baterai, maka tekan saja tombol *power* selama beberapa detik hingga laptop mati.

5.4.3 Pelestarian Bukti

Tim Tanggap Insiden Siber akan mengumpulkan dan merekam bukti tentang insiden siber untuk mendukung penyelidikan forensik terperinci, termasuk upaya penegakan hukum untuk mengidentifikasi dan mengadili penjahat siber yang bersalah. Tim Tanggap Insiden Siber harus mengumpulkan dan mencatat bukti-bukti berikut:

1. *Image* dari *hard drive* dan *raw image.*
2. *Image* RAM.
3. IP *address.*
4. *Capture* dan *flow* dari lalu lintas jaringan.
5. Diagram jaringan.
6. *File log* dan konfigurasi.
7. *Database*.
8. Catatan insiden siber.
9. Tangkapan layar (*screenshot*).
10. *Posting* di media sosial.
11. Rekaman CCTV, video dan audio.
12. Dokumen yang merinci biaya finansial untuk perbaikan atau kerugian aktivitas bisnis.

Saat mengumpulkan bukti, penting untuk mempertimbangkan langkah-langkah berikut:

1. Menunjuk seorang anggota Tim Tanggap Insiden Siber untuk bertanggung jawab mengumpulkan, mencatat dan menyimpan semua bukti yang dikumpulkan.
2. Tim Tanggap Insiden Siber akan membuat dan memelihara daftar dari semua bukti yang dikumpulkan, merinci tanggal dan waktu bukti dikumpulkan, oleh siapa dikumpulkan, dan rincian setiap barang yang dikumpulkan. Lihat Lampiran D untuk *template* yang akan digunakan untuk tugas ini.
3. Memastikan bahwa semua bukti disimpan dengan aman dan ditangani hanya oleh anggota Tim Tanggap Insiden Siber yang ditunjuk, dengan akses terbatas yang diberikan kepada personel yang lain.
4. Setiap akses ke bukti harus dicatat dengan jelas di daftar bukti, termasuk alasan akses. Hal ini penting dalam menjaga lacak balak (*chain of custody*) untuk mengumpulkan bukti.
5. Minimalkan berapa kali bukti ditransfer antar personel. Catat detail transfer bukti antar personel.

5.4.4 Komunikasi Internal

Di luar pembaruan situasi, mungkin perlu memberi pengarahan kepada personel organisasi tentang insiden siber. Hal ini penting jika jaringan, sistem, atau aplikasi TI organisasi tidak lagi beroperasi seperti yang diharapkan, atau jika situasi berpotensi menimbulkan kepentingan ke media atau publik. Pesan yang perlu dipertimbangkan saat berkomunikasi dengan personel organisasi meliputi:

1. Apa yang terjadi dan mengapa itu terjadi?
2. Apa yang akan terjadi dalam waktu dekat?
3. Apa yang diharapkan dari personel?
4. Siapa yang dapat dihubungi personel organisasi jika memiliki pertanyaan?

Semua komunikasi internal harus ditinjau dan disetujui oleh <Ketua Tim Tanggap Insiden Siber> sebelum dirilis.

5.4.5 Komunikasi Eksternal

Bergantung pada dampak dan tingkat keparahan siber, komunikasi dengan pemangku kepentingan eksternal (termasuk menteri, media, dan publik) mungkin diperlukan. Hal ini sangat penting jika insiden siber tersebut memengaruhi jaringan, sistem, atau aplikasi TI yang diandalkan oleh pihak ketiga, seperti situs *web* atau

layanan publik. Pesan utama yang perlu dipertimbangkan saat berkomunikasi dengan pemangku kepentingan eksternal meliputi:

1. Apa yang terjadi dan mengapa itu terjadi?
2. Sistem/layanan apa yang terpengaruh?
3. Langkah apa yang diambil untuk mengatasi situasi tersebut?
4. Apakah mungkin untuk mengatakan kapan situasi tersebut akan diselesaikan?
5. Apa yang diharapkan dilakukan oleh pemangku kepentingan eksternal?
6. Siapa yang dapat dihubungi oleh pemangku kepentingan eksternal jika terdapat memiliki pertanyaan/masalah?

Semua komunikasi eksternal harus ditinjau dan disetujui oleh <Kepala unit kerja yang membawahi fungsi komunikasi publik dan Ketua Tim Tanggap Insiden Siber> sebelum dirilis. Jika terdapat Komite Pengarah Keamanan Informasi, maka Komite Pengarah Keamanan Informasi harus menyetujui semua komunikasi eksternal sebelum dikeluarkan.

5.5 Tahap 4: Perbaikan (*Remediation*)

Tahap ini bertujuan untuk mengambil tindakan untuk menghilangkan ancaman dan menghindari insiden di masa depan.

1. Penghapusan ancaman

   Tim Tanggap Insiden Siber harus menghapus persistensi peretas, memblokir hak akses peretas, dan menutup semua vektor/sumber serangan.

2. Perbaikan kontrol keamanan

   Kontrol keamanan diperbarui dengan menghapus kerentanan untuk mencegah insiden serupa di masa mendatang. Perbaikan ini dilakukan dengan melakukan *update*, memasang *patch*, atau penggantian *password* untuk memastikan lingkungan aman. Proses dan *tools* baru dapat diterapkan untuk memperketat perimeter keamanan di jaringan internal, *host* internal, aplikasi, dan data. *Level logging* pada sistem atau pemantauan jaringan juga perlu dibuat yang lebih tinggi/detail. Hal ini penting untuk diperhatikan karena setelah sumber daya berhasil diserang, sering kali diserang lagi, atau sumber daya lain dalam organisasi diserang dengan cara yang sama. Pada tahap ini pastikan setiap tindakan didokumentasikan, seperti apa yang terjadi dan tindakan perbaikannya.

Tabel 8. Perbaikan insiden siber.

Tindakan	Deskripsi
Perbaikan pada sistem yang disusupi	▪ Cara paling mudah untuk menghilangkan *malware* adalah dengan menginstal ulang aset informasi. ▪ Menghapus sementara semua hak akses ke akun yang terlibat dalam insiden tersebut. ▪ Menghapus semua *file* berbahaya yang diinstal dan mekanisme persistensi yang diterapkan oleh peretas. ▪ Terapkan *prevention mode* pada EDR untuk semua IoC yang teridentifikasi.
Blokir sumber ancaman	▪ Dengan menggunakan hasil analisis dari langkah-langkah identifikasi dan penahanan sebelumnya, temukan semua saluran komunikasi yang digunakan oleh penyerang dan lakukan pemblokiran di semua *network boundaries*. ▪ Jika sumber telah diidentifikasi sebagai orang dalam (*insider threat*), ambil tindakan yang tepat dan libatkan pihak manajemen, unit kerja SDM, atau unit kerja hukum. ▪ Jika sumber telah diidentifikasi sebagai pelaku eksternal, pertimbangkan untuk melibatkan unit kerja hukum dan lembaga penegakan hukum jika diperlukan.
Menghubungi ISP dan/atau penyedia anti-DDoS	Mengkoordinasikan perbaikan berupa: ▪ *Filtering* (jika memungkinkan pada level Tier 1 atau 2). ▪ *Traffic-scrubbing/sinkhole/clean-pipe*. ▪ IP *public balancing/splitting/switching*. ▪ *Blackhole routing*.

5.6 Tahap 5: Pemulihan (*Recovery*)

Tim Tanggap Insiden Siber harus mengembangkan rencana pemulihan dari insiden siber. Rencana pemulihan harus merinci pendekatan untuk memulihkan jaringan, sistem, dan aplikasi TI setelah penahanan dan perbaikan selesai. Bergantung pada jenis dan tingkat keparahan insiden, Tim Tanggap Insiden Siber mungkin perlu mengembangkan rencana ini bersama dengan penasihat layanan TI dan kesinambungan bisnis. Rencana pemulihan harus mencakup unsur-unsur berikut:

1. Rencana untuk mengembalikan sistem ke operasi normal.
2. Proses pemantauan berkelanjutan untuk memastikan bahwa sistem yang terkena dampak berfungsi normal.
3. Rencana untuk memulihkan kerentanan guna mencegah insiden siber serupa di masa mendatang.

Penting untuk mempertimbangkan bahwa, dalam keadaan tertentu, rencana pemulihan dapat mencakup finalisasi investigasi kriminal terkait (termasuk pengumpulan bukti forensik) yang mungkin perlu dilakukan sebelum tahap pemulihan.

Tabel 9. Pemulihan insiden siber.

Tindakan	Deskripsi
Persetujuan dari pihak manajemen (Komite Pengarah Keamanan Informasi, jika ada)	Verifikasi semua langkah sebelumnya telah dilakukan dengan benar dan dapatkan persetujuan pihak manajemen sebelum mengikuti langkah selanjutnya.
Menyambungkan perangkat terdampak ke jaringan	▪ Buka kembali lalu lintas jaringan yang digunakan sebagai metode propagasi oleh *malware*. ▪ Sambungkan kembali beberapa area secara bersamaan. ▪ Sambungkan kembali laptop dan perangkat *mobile* ke area tersebut. ▪ Sambungkan kembali area ke jaringan lokal. ▪ Sambungkan kembali area ke internet.
Menginstall ulang sistem	Tidak peduli seberapa jauh peretas telah masuk ke dalam sistem dan pengetahuan yang diperoleh tentang penyusupan tersebut selama sistem telah dikompromikan, maka praktik terbaiknya adalah menginstal ulang sistem dari media yang asli dan menerapkan semua pembaruan keamanan ke sistem yang baru diinstal.
Melakukan perbaikan pada sistem terdampak	▪ Ubah semua *password* akun sistem dan meminta pengguna untuk melakukannya dengan cara yang aman. ▪ Mengembalikan semua *file* yang mungkin telah diubah oleh peretas, misalnya svchost.exe.

5.7 Tahap 6: Pelajaran yang Diperoleh (*Lesson Learned*)

Salah satu bagian terpenting dari tanggap insiden juga yang paling sering diabaikan, yaitu mendapatkan pembelajaran dan melakukan peningkatan. Setiap Tim Tanggap Insiden Siber harus melakukan perubahan berdasarkan adanya ancaman baru, peningkatan teknologi, dan pembelajaran yang diperoleh. Tujuan dari tahap ini adalah untuk mendokumentasikan detail insiden, membahas pelajaran yang diperoleh, dan menyesuaikan Rencana Tanggap Insiden Siber dan pertahanan.

5.7.1 Reviu Pasca Insiden Siber

Tim Tanggap Insiden Siber dan pihak manajemen (Komite Pengarah Keamanan Informasi, jika ada) harus berkumpul untuk melakukan reviu pasca insiden untuk membahas:

1. Tepatnya apa yang terjadi, dan kapan?
2. Seberapa baik kinerja Tim Tanggap Insiden Siber dan pihak manajemen (Komite Pengarah Keamanan Informasi, jika ada) dalam menangani insiden siber tersebut? Apakah prosedur terdokumentasi diikuti? Apakah sudah memadai?
3. Informasi apa yang dibutuhkan lebih cepat?

4. Apakah ada langkah atau tindakan yang diambil yang mungkin menghambat pemulihan?
5. Apa yang akan dilakukan oleh Tim Tanggap Insiden Siber dan pihak manajemen (Komite Pengarah Keamanan Informasi, jika ada)secara berbeda saat insiden serupa terjadi lagi?
6. Bagaimana berbagi informasi dengan organisasi lain dapat ditingkatkan?
7. Tindakan korektif apa yang dapat mencegah kejadian serupa di masa mendatang?
8. Prekursor atau indikator apa yang harus diperhatikan di masa mendatang untuk mendeteksi kejadian serupa?
9. *Tools* atau sumber daya tambahan apa yang diperlukan untuk mendeteksi, menganalisis, dan memitigasi insiden di masa mendatang?

Diskusi harus didokumentasikan dan semua wawasan/pelajaran utama dibagikan dengan semua pihak yang terlibat. Setiap rekomendasi yang muncul dari diskusi harus didokumentasikan dalam rencana kapan.

5.7.2 Laporan Insiden Siber

Laporan insiden harus ditulis dan tersedia untuk semua pelaku yang berlaku. Hal-hal berikut harus dibahas:

1. Deteksi awal.
2. Tindakan dan timeline dari setiap peristiwa penting.
3. Apa yang sudah dilakukan dengan benar.
4. Apa yang masih dilakukan dengan salah.
5. Dampak dari insiden tersebut.
6. *Indicators of compromise* (IoC).

5.7.3 Perbarui Rencana Tanggap Insiden Siber

Rencana Tanggap Insiden Siber ini akan terus diperbarui untuk mencerminkan praktik yang lebih baik dalam aktivitas respons insiden siber, termasuk mengikuti hasil reviu pasca insiden yang relevan.

Lampiran A. *Template* Pembaruan Situasi

TANGGAL MULAI:	**WAKTU MULAI:**	**PENULIS:**
TANGGAL DAN WAKTU INSIDEN SIBER TERDETEKSI		
STATUS SAAT INI	Baru / sedang berlangsung / terselesaikan	
JENIS INSIDEN SIBER		
KLASIFIKASI INSIDEN SIBER	Insiden siber / krisis siber	
CAKUPAN Berisi daftar jaringan, sistem, dan/atau aplikasi yang terkena dampak dan catat semua perubahan dari entri awal		
DAMPAK Berisi daftar pemangku kepentingan yang terkena dampak dan catat semua perubahan dari entri awal		
KEPARAHAN Berisi dampak insiden terhadap pemangku kepentingan dan catat semua perubahan dari entri awal		
PEMBERITAHUAN TINDAKAN/TERTUNDA		
CATATAN TAMBAHAN		
DETAIL KONTAK UNTUK KETUA TIM TANGGAP INSIDEN SIBER		
TANGGAL DAN WAKTU PEMBARUAN BERIKUTNYA		

Lampiran B. *Template* Catatan Insiden Siber

TANGGAL/WAKTU	CATATAN (*log*, rekaman/bukti, keputusan dan alasan)

Lampiran C. *Template* Rencana Aksi

TANGGAL DAN WAKTU	KATEGORI (Penahanan / Perbaikan / Pemulihan / Komunikasi)	AKSI	PENANGGUNG JAWAB AKSI	STATUS (Belum dialokasikan / Sedang Berlangsung / Ditutup)

Lampiran D. *Template* Daftar Bukti

TANGGAL, WAKTU DAN LOKASI PENGUMPULAN	DIKUMPULKAN OLEH (nama, jabatan, kontak dan nomor telepon)	DETAIL ITEM (kuantitas, nomor seri, nomor model, nama *host*, MAC *address*, dan IP *address*)	LOKASI PENYIMPANAN DAN NOMOR LABEL	AKSES (tanggal, waktu, personel dan alasan akses setelah pengumpulan)

Lampiran E. *Template* Aset dan Kontak

SITE INFORMATION

IP SUBNET	
DHCP SCOPE	
CORE ROUTER IP	
DNS SERVERS (INTERNAL) / LOGS & LOCATIONS	
DNS NAME / LOGS & LOCATION	
SECONDARY DNS NAME (EXTERNAL)	

INTERNET CONNECTION / COMMUNICATIONS

INTERNET SERVICE PROVIDERS IP & CONNECTION DETAILS	
NETWORK PROVIDER IP & CONNECTION DETAILS	
VOIP / PABX PHONE SYSTEM DETAILS IPs & NUMBER RANGE	
FIXED LINE SERVICES & HARDWARE	
3G/4G MOBILE DATA SERVICES & HARDWARE	
SATELLITE PHONE SERVICES & HARDWARE	
SINGLE POINT OF FAILURE ANALYSIS – COMMUNICATIONS INFRASTRUCTURE	

FIREWALL & SECURITY

FIREWALL SOFTWARE / HARDWARE	
WIRED NETWORK	
WIRELESS NETWORK	
SINGLE POINT OF FAILURE – FIREWALL INFRASTRUCTURE	

SITE REMOTE ACCESS

REMOTE ACCESS METHODS / LOGS & LOCATIONS	
SINGLE POINT OF FAILURE ANALYSIS – REMOTE ACCESS INFRASTRUCTURE	

WIRED NETWORK SWITCH INFRASTRUCTURE

HARDWARE / FIRMWARE / LOGS & LOCATIONS	
SINGLE POINT OF FAILURE ANALYSIS	

WIRELESS NETWORK SWITCH INFRASTRUCTURE

HARDWARE / FIRMWARE / LOGS & LOCATIONS	
SINGLE POINT OF FAILURE ANALYSIS	

INDUSTRIAL CONTROL SYSTEMS / SCADA INFRASTRUCTURE

SCADA PLC RTU HARDWARE / FIRMWARE / LOGS & LOCATIONS	
AUTHENTICATION METHODS & CONTROLS	
FUNCTIONAL ANALYSIS	
PROCESS FLOW DIAGRAM	
CONFIGURATION BACKUP SCHEDULE / LOCATIONS	
ALERT / ALARM SYSTEMS & THRESHOLDS	
SINGLE POINT OF FAILURE ANALYSIS	

DATA BACKUP

BACKUP SOFTWARE	
BACKUP LOCATION & RESTORATION TIMEFRAMES	
DATA RETENTION REQUIREMENTS	

DISASTER RECOVERY PLAN

IDENTIFIED HIGH AVAILABILITY? (YES / NO)	
REQUIRED UP TIME (%)	
REQUIRED RETURN TO OPERATION (Hrs)	

REDUNDANT POWER SUPPLY / UPS INFRASTRUCTURE

UPS HARDWARE / LOCATION	
BATTERY CAPACITY / RUN TIME	
CONNECTED DEVICES	

REDUNDANT POWER SUPPLY / GENERATOR INFRASTRUCTURE

GENERATOR HARDWARE / LOCATION	
FIXED OR PORTABLE	
CAPACITY (KVA)	
FUEL TYPE / CAPACITY (L)	
FUEL CONSUMPTION (L/Hr)	
ON SITE FUEL STORAGE (L) & LOCATIONS	
FUEL SUPPLY ARRANGEMENTS / AGREEMENTS	
DOCUMENTED FAIL OVER / RESTORATION OF SERVICES.	

ADMINISTRATION SYSTEMS (Supporting ICT systems)

WEB PROXY SERVER DETAILS / LOGS & LOCATIONS	
DOMAIN CONTROLLER DETAILS / LOGS & LOCATIONS	
WEB SERVER DETAILS / LOGS & LOCATIONS	
SERVER ENVIRONMENT OPERATING SYSTEM DETAILS / LOGS & LOCATIONS	
VIRTUAL SERVER HOST ENVIRONMENT DETAILS / LOGS & LOCATIONS	

EMAIL SYSTEMS

EMAIL SERVER DETAILS / LOGS & LOCATIONS	

DATABASE SYSTEMS

SERVER DETAILS / LOGS & LOCATIONS	
PRODUCTION DATABASE DETAILS / LOGS & LOCATIONS	
TEST DATABASE DETAILS / LOGS & LOCATIONS	

CLOUD SERVICE PROVIDERS

HOSTED SERVICE PROVIDERS & SLAs	

STAFF DESKTOP / LAPTOP / TABLET SYSTEMS

CLIENT ENVIRONMENT OS / LOGS & LOCATIONS	
CLIENT HARDWARE MANUFACTURER / MODEL	