

# Rancangan Dokumen Disaster Recovery Plan Pada Infrastruktur Teknologi Informasi Di Dinas Lingkungan Hidup Kabupaten Banyumas

1<sup>st</sup> Ainy Rahmatia Karepesina, 2<sup>nd</sup> Anis Alfiah, 3<sup>rd</sup> Dwi Hari Mahardika, 4<sup>th</sup> Melvira Dwi Ajiati,  
5<sup>th</sup> Ridwan Wahyu Pratama, 6<sup>th</sup> Rosita Maulida

Program Studi Sistem Informasi  
Universitas Amikom Purwokerto  
Purwokerto, Indonesia

1<sup>st</sup> akarepesina17@gmail.com, 2<sup>nd</sup> anisalfi@gmail.com, 3<sup>rd</sup> dwiharimardika01@gmail.com, 4<sup>th</sup> Mellvira90@gmail.com,  
5<sup>th</sup> ridwan33@gmail.com, 6<sup>th</sup> rositaamikom39@gmail.com

**Abstrak—** Disaster recovery plan (DRP) adalah rencana yang disiapkan organisasi untuk membantu organisasi pulih setelah terjadi musibah atau bencana. Penyebab musibah bervariasi, mulai dari fenomena alam hingga akibat perbuatan manusia, baik yang disengaja maupun tidak disengaja. Pada bidang teknologi informasi, penyebab dapat lebih spesifik misalnya kegagalan infrastruktur, kekeliruan operator, hingga serangan virus. Tingginya kebergantungan organisasi pada infrastruktur teknologi informasi menyebabkan perlunya dipertimbangkan DRP di bidang infrastruktur teknologi informasi. DRP perlu dibuat dengan tepat dan optimal, sesuai dengan kebutuhan dan kemampuan organisasi. Untuk itu, diperlukan studi awal untuk melihat kelayakan organisasi atas kebutuhan adanya DRP. Pada penelitian ini dilakukan studi kelayakan pada sistem informasi pada Dinas Lingkungan Hidup Kabupaten Banyumas. Untuk mengetahui tingkat keberhasilan perancangan dokumen pemulihan akibat bencana kami melakukan pengujian dokumen tersebut dengan standar NIST SP 800-34. Berdasarkan hasil pengujian yang telah dilakukan, tindakan pemulihan terhadap masalah yang terjadi bisa dilakukan dengan yang lebih cepat.

**Kata Kunci :** Disaster Recovery Plan, NIST SP 800-34, Sistem Informasi, Infrastruktur Teknologi Informasi

## I. PENDAHULUAN

Seperti umum diketahui, teknologi informasi merupakan salah satu kebutuhan mendasar hampir di semua sector bisnis, seperti halnya kebutuhan akan listrik dan telepon. Teknologi informasi, dalam konteks teknis, dapat diartikan sebagai sekumpulan infrastruktur untuk mendukung pengelolaan informasi yang meliputi proses collect, store, retrieve, disseminate dan reusable of information. Disadari atau tidak, dewasa ini, hampir semua sektor bisnis mempercayakan informasi penting perusahaannya pada sederetan peralatan teknologi informasi atau lazim kita sebut dengan infrastruktur. Tetapi, tingginya tingkat kebergantungan ini jarang sekali disertai dengan kesadaran akan adanya ancaman kerusakan infrastruktur, yang umumnya terjadi secara tidak terduga, baik akibat pengaruh dari lingkungan internal maupun eksternal, baik yang disengaja maupun tidak.

Dalam skala teknologi informasi, *Disaster Recovery Plan* menjadi sebuah wacana penting ketika sebuah organisasi sangat menggantungkan dukungan operasionalnya pada layanan teknologi informasi. Bidang penanggulangan bencana di sektor teknologi informasi melibatkan berbagai aspek dan disiplin ilmu, dimulai dari aspek teknologi seperti komponen *hardware*, *software*, infrastruktur seperti jaringan komputer, komunikasi data, hingga aspek non teknis seperti manusia, prosedur, standar, biaya, dan kebijakan. Kebutuhan data yang semakin meningkat menjadikan data sebagai aset yang bernilai tinggi, maka resiko terjadinya kerusakan pada data yang mengakibatkan data tidak dapat diakses yang dapat terjadi setiap saat. Tidak dapat dibayangkan apabila data-data penting bagi organisasi hilang karena suatu bencana (*disaster*).

Fakultas Teknik, Universitas Amikom sebagai salah satu organisasi yang menyelenggarakan pendidikan berbasis teknologi informasi tentu saja tidak terlepas dari kewajiban memelihara informasi terhadap berbagai ancaman disaster atau bencana contohnya mati listrik yang mengakibatkan kerusakan pada perangkat sehingga sistem berjalan secara manual, server terbakar, data yang tidak dapat terbaca karena terkena virus, tidak melakukan pemeliharaan rutin sehingga mengakibatkan data yang rusak. Kerugian yang terjadi dari rusaknya data secara tiba-tiba akan sangat besar. Dengan demikian, pentingnya menjaga data agar tetap aman kapan saja dan dimana saja dibutuhkan merupakan suatu keharusan bagi sebuah organisasi untuk merencanakan suatu tindakan pengamanan terhadap arsip-arsip dalam rangka mengantisipasi bencana.

Oleh karena itu membutuhkan rancangan *disaster recovery plan* yang berfungsi untuk mengatur proses pemulihan terhadap bencana (*disaster*) dalam kegiatan organisasi tersebut agar tetap berjalan dan dapat menjaga data tetap konsisten walaupun data mengalami gangguan bahkan kerusakan. Perencanaan disaster recovery mengacu pada persiapan untuk menghadapi bencana dan respon yang harus diberikan ketika bencana terjadi. Tujuan DRP adalah keberlangsungan (*continuity*) atau kemampuan organisasi untuk bertahan (*survival*) dalam menghadapi bencana (Proses

penyusunan DRP meliputi analisis, perencanaan, pembuatan DRP, pengujian dan revisi periodik berdasarkan kondisi bisnis terkini.

## II. METODE PENELITIAN

### A. Observasi

Observasi adalah suatu cara pengumpulan data dengan pengamatan langsung dan pencatatan secara sistematis terhadap obyek yang akan diteliti. Observasi dilakukan oleh peneliti dengan cara pengamatan secara langsung terhadap kondisi IS/IT di Dinas Lingkungan Hidup Kabupaten Banyumas. Di dalam pembuatan disaster recovery plan diperlukan data-data untuk mendukung prosedur disaster recovery plan tersebut. Adapun data yang di dapat dari hasil observasi adalah data bencana yang pernah terjadi terhadap IS/IT, data perangkat baik perangkat keras maupun perangkat lunak. Dari data hasil observasi tersebut di gunakan sebagai pembobotan untuk mendapatkan nilai yang digunakan sebagai atribut didalam penentuan potensi yang ditimbulkan dari suatu bencana

### B. Wawancara

Wawancara merupakan alat re-checking atau pembuktian terhadap informasi atau keterangan yang diperoleh sebelumnya. Tehnik wawancara yang digunakan dalam penelitian kualitatif adalah wawancara mendalam. Wawancara mendalam (in-depth interview) adalah proses memperoleh keterangan untuk tujuan penelitian dengan cara tanya jawab sambil bertatap muka antara pewawancara dengan informan atau orang yang diwawancarai, dengan atau tanpa menggunakan pedoman (guide) wawancara, di mana pewawancara dan informan terlibat dalam kehidupan sosial yang relatif lama.

### C. Framework & metode analisa data

Dalam membuat rancangan dokumen perancangan disaster recovery plan ini, kerangka kerja yang digunakan adalah *national intitute form standards and technology (NIST) special publication (SP) 800-34* adalah sebuah panduan yang berisi intruksi, rekomendasi, keputusan dalam pembuatan perancangan tentang pemulihan system informasi setelah terjadinya bencana atau gangguan.

## III. HASIL DAN PEMBAHASAN

### A. Sistem Informasi Dinas Lingkungan Hidup Kabupaten Banyumas

Dalam menjalankan kegiatan operasionalnya sehari-hari, dinas DLH kabupaten banyumas menggunakan beberapa sistem informasi antara lain:

- 1) *Sistem Informasi Manajemen Absensi Pegawai*
- 2) *Sistem Informasi Manajemen Keuangan*

### B. Risk Assesment

Risk Assesment berfokus pada ancaman yang dapat memengaruhi aset-aset instansi yang ada hubungannya dengan pelaksanaan pelayanan public oleh dinas lingkungan hidup kabupaten banyumas . Risk Assesment diperlukan untuk dapat menentukan klasifikasi dampak dan penyebab terjadinya gangguan dan bencana yang mungkin terjadi dan berguna dalam penentuan langkah-langkah yang optimal untuk memitigasi resiko yang terjadi .

Resiko yang terjadi pada gedung baik secara menyeluruh atau hanya sebagian dapat merusak dan menghancurkan aset-aset tersebut, misalnya pemadaman listrik , gempa bumi , kebakaran, kerusakan server, serangan virus, dan lain-lain. Menurut data yang diperoleh dari wawancara dengan kepala IT dinas lingkungan hidup kabupaten banyumas pernah terjadi sambaran petir pada mikrotik dinas lingkungan hidup kabupaten banyumas.

Tahap **Risk Assesment** ini merupakan tahap pertama dari prosedur disaster recovery plan. Berikut penjabaran mengenai ancaman yang dapat menimbulkan resiko dari ancaman yang terjadi :

Tabel 1. Risk Assesment

No	Kejadian	Penyebab	Dampak	Mitigasi	Unit yang Bertanggung Jawab
	Migrasi data	Migrasi Data	Tidak bisa mengakses sistem.		Kominfo
	Terkena Petir	Terkena Petir	Mikrotik rusak		kominfo

### A. Strategi Recovery

Strategi Recovery merupakan proses untuk pemulihan ketika terjadi suatu kegagalan pada system . Dari hasil risk assesment dapat diambil jenis-jenis ancaman yang mampu menjadi acuan untuk melakukan proses recovery . Berikut ini table proses proses pemulihan terhadap system informasi pada dinas lingkungan hidup kabupaten banyumas .

Tabel 2. Proses pemulihan system informasi

No.	Gangguan	Kendala	Proses Recovery
1.	Migrasi data	Tidak dapat mengakses system informasi	Melapor ke kominfo agar diperbaiki
2.	Listrik mati	Kehilangan daya menyebabkan beberapa perangkat tidak bisa diakses	Mengganti listrik menggunakan jenset
3.	Server down	Tidak dapat mengakses	Melapor ke kominfo agar diperbaiki

**B. Dokumentasi**

Dokumentasi disaster recovery plan merupakan tahap mendokumentasikan prosedur disaster recovery plan (DRP).

**C. Assembly point**

Ketika terjadi suatu bencana, sangat penting bagi perusahaan untuk melakukan evakuasi pegawai dan pelanggannya dengan cara mengumpulkan mereka pada titik kumpul untuk memudahkan dalam proses evakuasi. Titik kumpul tersebut harus memiliki jarak aman dari gedung atau lokasi yang dilanda bencana tersebut.

Titik kumpul tersebut berada pada :

- 1) *Primary* : Parkiran
- 2) *Secondary* : Parkiran
- 3) *Alternate* : Parkiran

**D. Staff Cadangan**

Setiap perusahaan perlu membentuk staff cadangan sebagai bentuk antisipasi jika terjadi bencana dan staff inti dari perusahaan mengalami cedera dan tidak dapat bekerja. Hal ini perlu dilakukan terutama dalam sisi manajerial. Staff cadangan memiliki jabatan yang sama dengan jabatan yang digantikannya.

Berikut ini adalah daftar staff pengganti serta jabatannya :

No	Nama	Jabatan Awal	Jabatan Pengganti
1	Huda	Staff TU	Wakil Ketua IT
2	Tidak Disebutkan Nama	Waka	KAURTU UT
3			

**E. Relokasi Data Center**

Informasi merupakan bagian yang sangat penting untuk operasional perusahaan. Seiring dengan meningkatnya ketergantungan bisnis terhadap teknologi informasi maka meningkat juga resiko ancaman akibat bencana terhadap keberlangsungan bisnis. Sehingga perusahaan perlu memiliki tempat penyimpanan data cadangan yang digunakan ketika keadaan darurat. Data center cadangan tersebut harus jauh dari lokasi utama perusahaan guna menghindari kejadian yang terjadi bersamaan di lokasi utama. Selain itu data center cadangan harus mampu diakses kapan saja jika perusahaan membutuhkannya.

Berikut ini adalah lokasi dari data center cadangan yang digunakan oleh perusahaan :

- 1) *Kominfo*  
 Alamat : *Kominfo Jln.masjid*  
 Tlp : -  
 Email : -

**F. Anggota DRT**

Berikut ini adalah informasi kontak dari anggota DRT yang dapat dihubungi jika terjadi bencana dalam perusahaan :

No	Nama	Divisi/Jabatan	Pilihan Kontak	Nomor Kontak
1	Endah Mawarti	Pemimpin DRT	Handphone 1	082137737028
			Handphone 2	
			Email	
2	Iswandari	Tim Manajemen DRT	Handphone 1	
			Handphone 2	
			Email	
3	Aditya Ginanjar	DRT Jaringan	Handphone 1	
			Handphone 2	
			Email	
4	Aditya Ginanjar dan Koinfo	DRT Infrastruktur	Handphone 1	
			Handphone 2	
			Email	
5	Aditya Ginanjar	DRT Server	Handphone 1	
			Handphone 2	
			Email	
6	Koinfo	DRT Aplikasi	Handphone 1	
			Handphone 2	
			Email	
7	Bagian TU	DRT Komunikasi	Handphone 1	
			Handphone 2	
			Email	
8	Bagian TU	DRT Operasional	Handphone 1	
			Handphone 2	
			Email	

Sedangkan berikut ini adalah informasi kontak dari vendor atau pihak eksternal perusahaan yang dapat dihubungi ketika terjadi bencana :

No	Nama	Pilihan Kontak	Nomor Kontak
1	Listrik PLN	Telepon Kantor	
		Handphone	
		Email	
2	Telekomunikasi TELKOM	Telepon Kantor	
		Handphone	
		Email	
3	Supplier Hardware GTI	Telepon Kantor	
		Handphone	
		Email	
4	Supplier Server Kominfo	Telepon Kantor	
		Handphone	
		Email	
5	Pemilik Property PEMDA	Telepon Kantor	
		Handphone	
		Email	
6	Keamanan Setempat Kominfo	Telepon Kantor	
		Handphone	
		Email	

#### IV. PENUTUP

Berdasarkan penelitian yang telah kami lakukan maka dapat diambil kesimpulan sebagai berikut :

1. Disaster Recovery Plan di bidang teknologi informasi merupakan salah satu aspek penting dalam mendukung keberlangsungan bisnis ataupun perkantoran setelah terjadinya bencana, untuk mempertahankan semua pihak yang terlibat pada

bisnis tersebut termasuk konsumen dan pelaku bisnis itu sendiri.

2. Dengan adanya *Disaster Recovery Planning* yang baik, maka segala kemungkinan ancaman-ancaman yang mungkin muncul dalam pelaksanaan bisnis dan industry dapat diatasi dengan baik. Kontinuitas bisnis dapat dijaga dan segala bentuk kerugian dapat diminimalisir sehingga perusahaan dapat bangkit kembali dari keadaan darurat yang mungkin terjadi. *Disaster Recovery Planning* harus disesuaikan dengan situasi dan kondisi perusahaan agar perencanaan yang dilakukan tidak salah dan dapat menangani masalah tepat.

#### V. SARAN

Berdasarkan penelitian yang telah kami lakukan maka dapat kami beri saran. Dinas Lingkungan Hidup Kabupaten Banyumas belum memiliki server pemulihan sendiri pada perusahaannya. Sebaiknya Dinas Lingkungan Hidup Kabupaten Banyumas memiliki server sendiri agar apabila terjadi gangguan maka tidak harus menunggu konfirmasi dari pusat untuk memprbaikinya

#### UCAPAN TERIMA KASIH

Ucapan terima kasih diucapkan kepada Universitas Amikom Purwokerto, dosen pengampu mata kuliah ITI Bapak Zanuvar Rifa'i dan semua pihak yang telah membantu menyelesaikan penelitian ini.

#### REFERENSI

- [1] *CEES (jurnal of engineering system and science) vol. 3 no. 2 juli 2018. Rancangan dokumen Disaster Recover Plan pada IS/IT DINAS XYZ*
- [2] <https://fitwiethayalisi.wordpress.com/teknologi-pendidikan/penelitian-kualitatif-metode-pengumpulan-data/>
- [3] <https://eprints.uny.ac.id/9804/4/BAB3%20-%2006205244111.pdf>