Iqra: Jurnal Perpustakaan Dan Informasi
Volume 19 Nomor 2 Oktober 2025
ISSN: 1979-7737 E-ISSN: 2442-8175

Rancangan Keamanan Informasi Dan Perancangan Disaster Recovery Satker ZYX

Ariq Rizky Attariqh, Benedicta Ursula Nelvina, Cahyo Nugraha Purnomo, Farrel Rio Lucky Rachmadi, Izma Shabry Pratama, Muhammad Fazli Mawla
Universitas Pembangunan Nasional Veteran Jakarta

Email: 2310414027@mahasiswa.upnvj.ac.id,

ABSTRAK

Di era digital yang berkembang pesat, keamanan informasi menjadi aspek yang penting dan tidak dapat diabaikan. meskipun kemajuan teknologi memberikan kemudahan dalam penyimpanan, pengolahan dan distribusi data. hal ini juga membuka celah terhadap berbagai ancaman, seperti peretasan dan kebocoran informasi. Selain itu, faktor non-teknis seperti bencana alam yang waktu kejadiannya sulit diperkirakan dapat menjadi risiko yang harus diperhitungkan, karena dapat menyebabkan kerusakan infrastruktur dan hilangnya data penting jika tidak diantisipasi dengan baik. oleh karena itu penelitian ini bertujuan untuk merancang disaster recovery plan (DRP) serta mengidentifikasi potensi ancaman baik dari faktor internal maupun eksternal, dan merumuskan strategi pemulihan yang efektif dan terstruktur dalam menghadapi insiden. Pendekatan yang digunakan adalah kualitatif, dengan teknik pengumpulan data melalui wawancara dan studi dokumen. Penelitian ini menghasilkan dokumen Disaster Recovery Plan (DRP) untuk Satker ZYX sebagai pedoman pemulihan sistem informasi pasca-insiden. Disaster Recovery Plan (DRP) disusun melalui tahapan seperti identifikasi aset, risk assessment, BIA, hingga pengujian dan pemeliharaan rencana. Strategi pemulihan disesuaikan dengan prioritas sistem, mencakup penggunaan hot, warm, dan cold site, serta penerapan backup bertingkat dan peran tim yang terstruktur. Penerapan keamanan informasi masih memerlukan peningkatan, khususnya pada sistem informasi.

Kata Kunci: *Disaster Recovery Plan*, Keamanan Informasi, Sistem Infomasi.

ABSTRACT

In the rapidly growing digital era, information security is an important aspect that cannot be ignored. although technological advances provide convenience in data storage, processing and distribution. this also opens gaps to various threats, such as hacking and information leaks. In addition, non-technical factors such as natural disasters whose timing of occurrence is difficult to

predict can be a risk that must be taken into account, because it can cause infrastructure damage and loss of important data if not properly anticipated. therefore this study aims to design a disaster recovery plan (DRP) and identify potential threats from both internal and external factors, and formulate an effective and structured recovery strategy in the face of incidents. The approach used is qualitative, with data collection techniques through interviews and document studies. This research produced a Disaster Recovery Plan (DRP) document for ZYX work unit as a guideline for post-incident information system recovery. Disaster Recovery Plan (DRP) is prepared through stages such as asset identification, risk assessment, BIA, to plan testing and maintenance. Recovery strategies are tailored to system priorities, including the use of hot, warm, and cold sites, as well as the implementation of multilevel backups and structured team roles. Information security implementation still needs improvement, especially on information systems.

***Keywords**: Disaster Recovery Plan, Information Security, Information System.*

PENDAHULUAN

Pemerintahan Indonesia haruslah memiliki sistem informasi yang andal dan aman. Di dunia yang semakin terhubung, instansi pemerintah dan sektor pertahanan menghadapi tantangan besar dalam melindungi data-data sensitif mereka. Menurut Admass et al. (2024), meningkatnya ancaman terhadap sistem informasi yang mengelola data penting merupakan masalah utama. Keamanan siber menjadi sangat penting karena potensi serangan yang dapat merusak integritas dan kerahasiaan data strategis (Li & Liu, 2021). Digitalisasi dalam sektor pemerintahan, khususnya bidang pertahanan, menciptakan celah terhadap ancaman yang lebih kompleks sehingga memerlukan langkah-langkah keamanan yang tangguh (Tóth, 2023). Satker ZYX, sebagai lembaga yang mengelola data strategis, harus memastikan bahwa sistem informasinya tidak hanya dapat diandalkan, tetapi juga mampu mengatasi berbagai gangguan yang mungkin muncul, baik dari ancaman internal maupun eksternal (Ajayi et al., 2025).

Keamanan informasi dalam sistem layanan menjadi perhatian utama karena melibatkan data pribadi pengguna serta koleksi digital yang bernilai

penting bagi institusi. Data pengguna seperti identitas, riwayat peminjaman, dan informasi akun perlu dilindungi agar tidak disalahgunakan oleh pihak yang tidak bertanggung jawab. Satker ZYX dapat mengidentifikasi ancaman dari sumber eksternal (seperti serangan hacker atau virus) maupun internal (seperti kelalaian pengguna atau karyawan). Menurut McIlwraith (2021), ancaman internal seringkali lebih berbahaya karena terkait langsung dengan kebijakan organisasi dan bagaimana setiap anggota staf mengikuti peraturan keamanan. Sementara itu, penelitian Sengan et al. (2021) menekankan pentingnya kesadaran keamanan informasi di seluruh pihak yang terlibat untuk mengurangi kerentanan terhadap ancaman eksternal dan internal. Sejalan dengan itu, Wangen & Ulven (2021) menyatakan bahwa pengelolaan ancaman yang efektif memerlukan partisipasi semua pihak dalam menerapkan kebijakan keamanan informasi dan mitigasi risiko. Oleh karena itu, keamanan informasi harus dipandang sebagai tanggung jawab kolektif, dan peran serta seluruh elemen organisasi sangat penting untuk meminimalkan kerentanan terhadap serangan yang dapat mengancam keberlangsungan sistem informasi.

Peningkatan security awareness terbukti memperbaiki perilaku kepatuhan staf secara signifikan dan mempertegas pentingnya budaya keamanan kolektif (Kavak, 2024). Penting untuk membangun budaya keamanan informasi di lingkungan kerja agar setiap individu menyadari perannya masing-masing. Dengan demikian, setiap risiko dapat diminimalisir dan dampak kerugiannya dapat ditekan. Gangguan teknis seperti kerusakan server atau bencana alam juga menjadi ancaman signifikan. Oleh karena itu, merancang *Disaster Recovery Plan* (DRP) berbasis standar seperti NIST SP 800-34 Rev.1 sangat penting untuk mempercepat pemulihan sistem dan meminimalkan dampak kerusakan (Akbar, Sucahyo, & Gandhi, 2022).

Disaster Recovery Plan (DRP) merupakan dokumen penting yang berfungsi sebagai panduan bagi organisasi dalam menghadapi bencana

atau insiden yang dapat mengganggu operasional sistem informasi. Satker ZYX yang sangat bergantung pada infrastruktur digital, perlu menerapkan DRP untuk mengurangi efek gangguan operasional. DRP dirancang untuk menjamin kelangsungan layanan penting dan pemulihan sistem yang efisien pasca-bencana (Phillips & Mincin, 2023). DRP yang tidak terstruktur akan menyulitkan institusi menangani masalah secara tepat waktu, mengakibatkan waktu pemulihan lebih lama dan kerugian yang lebih besar (McEntire, 2021). Hal ini semakin penting mengingat kompleksitas dan ketergantungan tinggi terhadap teknologi informasi dalam sistem layanan pemerintahan berbasis digital (Linardos, Drakaki, & Tzionas, 2022).

Penerapan DRP yang efektif juga membantu pengelolaan infrastruktur kritis, yang memerlukan pemulihan terencana setelah bencana (Stamenkov, 2025). Oleh karena itu, DRP sangat penting untuk menjaga kelangsungan operasional dan ketahanan sistem, khususnya bagi lembaga seperti Satker ZYX yang mengelola data strategis. Selain itu, prosedur penanganan insiden juga harus disusun secara rinci, mulai dari tahap persiapan, pencegahan, respons, pemulihan, hingga evaluasi pasca-insiden. Perspektif layanan publik pun relevan di sini. Survei nasional di Amerika Serikat menemukan bahwa 51% perpustakaan sudah memiliki rencana tanggap darurat, tetapi hanya 13% yang memuat continuity-of-operations plan secara eksplisit. Ini menegaskan pentingnya budaya pemulihan layanan di sektor informasi untuk diperkuat (Antonelli et al., 2025). Satker ZYX dapat memanfaatkan hasil evaluasi keamanan informasi untuk menyusun DRP yang sesuai dengan kondisi sistem layanan yang ada. Phillips & Mincin (2023) menyarankan bahwa DRP efektif harus dibangun berdasarkan hasil evaluasi ancaman terbaru dan kondisi sistem keamanan saat ini. DRP yang disesuaikan membantu institusi menghadapi ancaman lebih tepat. Hal ini sesuai dengan Li & Liu (2021), yang menekankan bahwa DRP yang baik dapat mempercepat pemulihan sistem sekaligus meningkatkan kepercayaan pengguna terhadap keamanan layanan. Seperti yang diungkapkan McEntire (2021), keberadaan DRP menunjukkan komitmen organisasi untuk menjaga

keamanan dan ketersediaan akses informasi pengguna. Oleh sebab itu, penelitian ini sangat penting untuk memperkuat sistem keamanan informasi Satker ZYX dan memastikan layanan tetap berjalan meskipun terjadi insiden yang mengganggu.

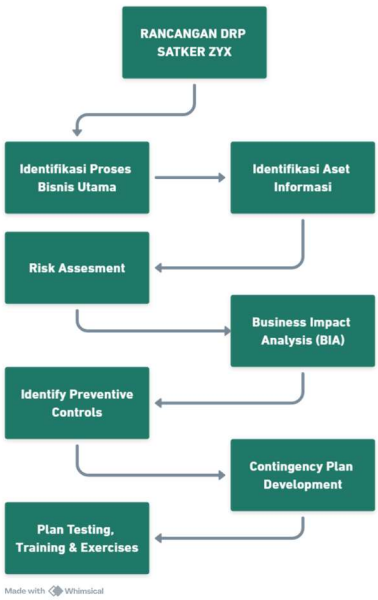
Penelitian ini bertujuan untuk merancang Disaster Recovery Plan (DRP) yang sesuai dengan kebutuhan dan kondisi institusi, sebagai upaya untuk memastikan keberlangsungan operasional serta perlindungan terhadap data dan sistem informasi dari gangguan yang bersifat merusak atau mengganggu layanan. Penelitian ini juga bertujuan untuk mengevaluasi sejauh mana sistem keamanan informasi saat ini telah diterapkan, mengidentifikasi potensi ancaman baik dari faktor internal maupun eksternal, dan merumuskan strategi pemulihan yang efektif dan terstruktur dalam menghadapi insiden. Dengan demikian, hasil penelitian diharapkan dapat menjadi acuan dalam penyusunan DRP yang komprehensif dan adaptif terhadap risiko yang mungkin terjadi. Dengan adanya penelitian ini, diharapkan dapat memberikan gambaran menyeluruh mengenai kondisi aktual sistem keamanan informasi pada layanan digital di Satker ZYX. Dengan demikian, penelitian ini diharapkan dapat menjadi acuan dalam perancangan DRP dan kebijakan keamanan informasi yang adaptif terhadap ancaman siber serta mendukung keberlanjutan layanan digital Satker ZYX secara aman dan andal.

METODE

Adapun metode penelitian yang digunakan dalam penelitian ini adalah metode kualitatif. Teknik pengumpulan data dilakukan melalui wawancara dan studi dokumen. Wawancara bersifat semi-terstruktur kepada para pimpinan dan staf Satker ZYX. Wawancara dilakukan secara langsung untuk menggali informasi mengenai kondisi keamanan informasi, potensi ancaman, serta kebijakan penanganan insiden yang diterapkan saat ini. Penulis juga mengobservasi terhadap kondisi fisik infrastruktur sistem yang dikelola oleh Satker ZYX dan sistem pengelolaan data yang digunakan. Data yang diperoleh kemudian dianalisis dengan menggunakan teknik

reduksi data, penyajian data, dan penarikan kesimpulan. Melalui metode ini, diharapkan dapat diperoleh gambaran yang komprehensif mengenai kondisi keamanan informasi di sistem kearsipan Satker ZYX. Metode kualitatif dipilih karena mampu memberikan pemahaman mendalam terhadap permasalahan yang diteliti melalui interaksi langsung dengan informan.

Gambar 1.



Analisis data dari hasil wawancara dan studi dokumen menggunakan acuan dari standar NIST SP 800-34 untuk menyusun Disaster Recovery Plan yang terdiri dari:

1. Mengembangkan kebijakan perencanaan kontinjensi
2. Melakukan analisis dampak bisnis
3. Mengidentifikasi kontrol pencegahan
4. Membuat strategi kontinjensi
5. Mengembangkan rencana kontinjensi
6. Merencanakan pengujian, simulasi, dan latihan
7. Merencanakan pemeliharaan sistem

Hasil penelitian diharapkan dapat memberikan rekomendasi yang aplikatif bagi institusi dalam meningkatkan keamanan informasi dan menyusun DRP yang sesuai. Selain itu, penelitian ini juga diharapkan dapat menambah literatur mengenai keamanan informasi di setiap lembaga pemerintahan, khususnya di Indonesia. Oleh karena itu penelitian ini diharapkan dapat memperkuat sistem keamanan informasi dan memiliki DRP yang dapat diandalkan dalam menghadapi situasi darurat di Satker ZYX. Selain itu, hasil penelitian ini juga dapat menjadi referensi bagi institusi sejenis dalam menerapkan kebijakan keamanan informasi yang baik.

HASIL DAN PEMBAHASAN

A. Skema Sistem Satker ZYX

Satker ZYX adalah unsur pendukung tugas dan fungsi Kementerian yang berada di bawah dan bertanggung jawab kepada Menteri. Satker ZYX bertugas untuk melaksanakan penelitian dan pengembangan di bidang pertahanan.

B. Sistem Informasi Satker ZYX

Sistem informasi yang terdapat dalam Satker ZYX terdiri dari :

1. Sistem Arsip Surat Menyurat berhubungan dengan pengelolaan surat dinas, nota, disposisi
2. Arsip Digital Lokal Satker ZYX berhubungan dengan penyimpanan hasil riset, dokumentasi visual
3. Database Kegiatan Penelitian berhubungan dengan data proyek penelitian strategis

C. Risk Assessment

Penilaian risiko memberikan gambaran mengenai berbagai ancaman yang mungkin dihadapi, relevansi, kemungkinan terjadinya, dampak yang dapat ditimbulkan, serta level risiko yang terkait yang menggunakan

kerangka NIST SP 800-34 Rev. 1 sebagai acuan. Penilaian risiko pada Satker ZYX ditandai dengan keterangan *Confirmed* (C), *Anticipated* (A), *Possible* (P), Sangat Tinggi (ST), Tinggi (T), Sedang (S), Rendah (R), dan Sangat Rendah (SR). beberapa penilaian risiko memiliki tingkat resiko sangat tinggi yang mampu memberikan dampak besar pada data Satker ZYX. Hasil penilaian risiko dapat dilihat dari tabel berikut:

Tabel 1. *Risk Assessment*

No.	Ancaman	Relevansi	Kemungkinan	Impact	Risiko
1	Kebocoran data/informasi sensitif	C	T	ST	ST
2	Hacking	A	ST	ST	ST
3	Phishing	C	S	ST	T
4	Infeksi Virus/Malware	P	S	ST	T
5	Kesalahan Administrasi	C	R	R	R
6	Kesalahan Prosedur	P	S	T	S
7	Perangkat Rusak	C	R	ST	P
8	Perangkat Dicuri	A	R	ST	S
9	Instalasi Gagal	C	S	ST	S
10	Kegagalan Backup	C	ST	T	T
11	Data Hilang	C	T	ST	T
12	Data Rusak	C	R	T	T
13	Sumber Daya Menipis	P	T	T	T
14	Internet Terganggu	C	T	T	T
15	Blackout/Mati Lampu	C	T	S	R
16	Kebakaran	P	R	ST	R
17	Gempa Bumi	P	T	ST	T
18	Petir	A	ST	ST	ST
19	Banjir	A	S	T	S

D. *Business Impact Analysis (BIA)*

Business Impact Analysis (BIA) merupakan salah satu tahap penting dalam perancangan *Disaster Recovery Plan (DRP)* yang bertujuan untuk mengidentifikasi dan mengevaluasi dampak dari gangguan terhadap sistem informasi yang ada di Satker ZYX. BIA membantu dalam menentukan prioritas pemulihan sistem berdasarkan tingkat kritikalitasnya terhadap kelangsungan operasional dan fungsi organisasi. Dalam analisis ini, setiap sistem informasi akan dianalisis dampaknya jika terjadi gangguan, serta ditentukan *Recovery Time Objective (RTO)* dan *Recovery Point Objective (RPO)* yang sesuai. RTO dan RPO digunakan untuk menetapkan waktu maksimal yang dapat diterima untuk pemulihan sistem dan pemulihan data agar operasional tetap berjalan dengan minimal gangguan. Berikut ini adalah hasil BIA untuk beberapa sistem informasi yang ada di Satker ZYX.

Tabel 2. *Business Impact Analysis*

No	Sistem Informasi	Fungsi	Dampak	RTO	RPO
1	Sistem Arsip Surat Menyurat	Pengelolaan surat dinas, nota, disposisi	Tinggi	1 Jam	1 Jam
2	Arsip Digital Lokal	Penyimpanan hasil riset, dokumentasi visual	Sedang	2 Jam	1 Jam
3	Database Kegiatan Penelitian	Data proyek penelitian strategis	Tinggi	1 Jam	30 Menit

E. Identifikasi Kontrol Pencegahan

Tahap penting dalam pembuatan *Rencana Pengurangan Bencana (DRP)* adalah identifikasi kontrol pencegahan. Pada tahap ini dilakukan identifikasi pengendalian terhadap kerentanan sistem yang bertujuan untuk mengidentifikasi ancaman dan kekurangan yang dapat memengaruhi sistem informasi. Adapun kondisi ruangan yang menjadi tempat sumber informasi: terdapat ruangan server kecil yang hanya diisi 1 rak berisi server, terdapat UPS *(Uninterruptible Power Supply)* sebagai pasokan listrik khusus di ruang server, dan perlindungan ruang server yang dikelilingi kaca tebal

tetapi tidak tahan api. Sehingga dapat diidentifikasi empat ancaman sebagai kendali pencegahan.

Tabel 3. *Identify Preventive Controls*

Ancaman	Tingkat Dampak	Kerentanan	Rekomendasi
Kebocoran data-data penting	Tinggi	Belum ada klasifikasi yang pasti terkait data-data yang penting untuk mendapat keamanan penuh	Membuat klasifikasi terhadap informasi/data yang penting untuk mendapat keamanan ekstra, memastikan hanya orang tertentu yang dapat mengakses data/informasi sensitif
Bencana alam	Tinggi	Banjir, kebakaran, tetapi belum ada pelatihan evakuasi seperti kebakaran dan perlindungan fisik perangkat belum terverifikasi	Mengadakan pelatihan evakuasi bencana secara rutin, menggunakan material tahan guncangan, dan tahan api di ruang server atau pusat data
Kerusakan perangkat keras	Sedang	Backup masih dilakukan manual, belum otomatis	Mengatur sistem backup menjadi otomatis dan membuat jadwal maintenance perangkat
Kegagalan sistem jaringan	Tinggi	Adanya gangguan koneksi dan router	Menggunakan sistem pemantauan jaringan dan penggunaan dua jalur internet yang berbeda

F. Pengembangan Rencana Kontingensi

Mengacu pada pedoman NIST SP 800-34 Revision 1, setelah diketahui risiko dan dampak yang ditimbulkan berikut ini adalah strategi kontingensi untuk Satker ZYX, yang bertujuan untuk memastikan pemulihan sistem dan layanan setelah terjadinya gangguan. Strategi ini dirancang untuk meminimalkan risiko dan mengembalikan operasional dengan efektif dalam menghadapi berbagai jenis gangguan.

1. **Backup dan Pemulihan**

Strategi Backup

- **Sistem Mission-Critical**: Data dan aplikasi yang sangat penting untuk kegiatan penelitian Satker ZYX harus memiliki backup real-time dan backup penuh harian. Backup ini harus disimpan baik secara lokal maupun di lokasi cadangan (misalnya, penyimpanan cloud atau situs pemulihan bencana).
- **Sistem Penting**: Backup incremental harian dan backup penuh mingguan untuk sistem administratif dan pendukung. Backup ini juga harus disimpan di fasilitas luar lokasi untuk keamanan tambahan.
- **Sistem Prioritas Rendah**: Data harus dicadangkan mingguan. Sistem ini dapat menoleransi waktu pemulihan yang lebih lama, tetapi backup tetap penting untuk integritas data dan dampak pemulihan minimal.

Metode Pemulihan

- Cold Site: Untuk sistem prioritas rendah, Satker ZYX harus mempertahankan cold site yang dapat diaktifkan jika terjadi downtime yang lama. Situs ini akan memerlukan waktu pengaturan substansial untuk mengembalikan fungsionalitas sistem.

- Warm Site: Untuk sistem penting, warm site akan menyediakan situs pemulihan dengan perangkat keras dan perangkat lunak yang sudah dikonfigurasi untuk pemulihan cepat saat dibutuhkan.
- Hot Site: Untuk sistem mission-critical, hot site harus siap dengan replikasi data real-time dan sistem untuk memastikan tidak ada downtime untuk operasi penting.

2. Penyimpanan Data di Luar Lokasi (Offsite Storage)

Penyimpanan Data di Luar Lokasi

- Satker ZYX harus menggunakan fasilitas penyimpanan data komersial untuk backup data di luar lokasi. Fasilitas ini menyediakan standar keamanan yang lebih tinggi dan perlindungan bencana.
- Transportasi dan Penyimpanan: Data yang dibackup harus diberi label, diketik, dan diangkut dengan aman ke fasilitas luar lokasi. Jika data diperlukan untuk pemulihan, fasilitas akan mengirimkan data ke lokasi yang dibutuhkan (baik kembali ke Satker ZYX atau situs alternatif).
- **Kriteria Pemilihan Fasilitas Penyimpanan di Luar Lokasi**:

  a. Area Geografis: Pastikan bahwa fasilitas penyimpanan di luar lokasi tidak berada di zona risiko yang sama dengan pusat data utama untuk menghindari bencana yang mempengaruhi kedua lokasi.
  b. Keamanan: Pastikan fasilitas memenuhi standar keamanan yang diperlukan untuk melindungi data sensitif.
  c. Biaya: Evaluasi biaya penyimpanan dan transportasi untuk mengoptimalkan anggaran.

3. Situs Alternatif

Satker ZYX harus memastikan bahwa ia memiliki jenis situs alternatif berikut untuk pemulihan:

- Cold site, sudah cukup untuk sistem prioritas rendah. Ini menyediakan infrastruktur dasar tetapi memerlukan waktu untuk mengonfigurasi dan memasang perangkat setelah kejadian.
- Warm site, untuk sistem penting, warm site adalah pilihan yang ideal. Situs ini berisi perangkat keras dan perangkat lunak penting yang telah dikonfigurasi untuk pemulihan cepat, memungkinkan pemulihan operasional yang lebih cepat dibandingkan dengan cold site.
- Hot site, untuk sistem mission-critical seperti database penelitian dan dokumentasi strategis, hot site diperlukan. Hot site ini akan sepenuhnya operasional dan mampu langsung mengambil alih sistem dari situs utama jika terjadi kegagalan.

Tabel 4. Lokasi Alternatif

Prioritas Pemulihan	Keterangan	Strategi Backup dan Recovery	Frekuensi Backup	Lokasi Alternatif
Tinggi (Mission-Critical)	Dampak besar pada proses bisnis dan layanan	Menggunakan perangkat storage, metode yang digunakan adalah data replication dan virtual machine backup	Real-time dan harian	Hot Site
Sedang (Important)	Dampak cukup besar pada proses bisnis dan layanan	Menggunakan perangkat storage, metode yang digunakan adalah data replication dan virtual machine backup	Harian dan mingguan	Warm Site

Rendah (Low)	Dampak kecil pada proses bisnis dan layanan	Menggunakan perangkat storage, metode yang digunakan adalah data replication dan virtual machine backup	Mingguan	Cold Site

4. Penggantian dan Perbaikan Perangkat

Redundansi Perangkat

- Perangkat redundan harus dipertahankan untuk sistem kritis. Perangkat yang dapat diganti saat berjalan (hot-swappable) seperti pasokan daya, disk, dan antarmuka jaringan harus disimpan di tempat yang mudah dijangkau untuk meminimalkan downtime jika terjadi kegagalan.
- Perjanjian dengan Vendor: Perjanjian harus dibuat dengan vendor untuk penggantian perangkat dengan cepat jika terjadi kegagalan. Perangkat pengganti harus disimpan di fasilitas pemulihan bencana atau diposisikan di tempat lain untuk memfasilitasi pemulihan yang cepat.

5. Peran dan Tanggung Jawab

Aktivasi Rencana Kontingensi

- Koordinator ISCP (Rencana Kontingensi Sistem Informasi) akan bertanggung jawab untuk mengaktifkan rencana kontingensi dan mengawasi pelaksanaannya. Koordinator akan memimpin tim pemulihan dan memastikan sumber daya dialokasikan dengan efektif.
- Tim Manajemen: Manajemen senior, termasuk CIO, akan memiliki kewenangan untuk mengambil keputusan terkait aktivasi rencana, prioritas pemulihan, dan pengeluaran keuangan.

Tim Pemulihan

- Tim Pemulihan Teknis: Termasuk tim pemulihan server, pemulihan jaringan, dan pemulihan database. Tim ini akan menangani upaya pemulihan untuk berbagai komponen sistem.
- Tim Pemulihan Aplikasi: Tim ini akan fokus pada pemulihan aplikasi perangkat lunak, terutama yang sangat penting untuk penelitian.
- Tim Telekomunikasi: Untuk memastikan bahwa komunikasi dipulihkan dengan cepat.
- Tim Urusan Hukum: Bertanggung jawab untuk memastikan bahwa persyaratan hukum dan kepatuhan dipenuhi selama proses pemulihan.

Setiap tim akan memiliki tanggung jawab yang jelas dan dilatih secara teratur untuk merespons berbagai skenario pemulihan.

6. Pengujian dan Pelatihan

Pengujian

- Simulasi Berkala: Simulasi pemulihan bencana harus dilakukan secara berkala untuk menguji efektivitas strategi kontingensi dan waktu respons. Skenario yang diuji dapat mencakup serangan siber, kerusakan perangkat keras, atau bencana alam.

Pelatihan

- Pelatihan: Semua staf yang terlibat dalam pemulihan harus mengikuti pelatihan berkala untuk membiasakan mereka dengan peran dan tanggung jawab mereka dalam pemulihan.

- Evaluasi: Setelah setiap sesi pelatihan, umpan balik harus dikumpulkan untuk menilai efektivitas pelatihan dan mengidentifikasi area yang perlu diperbaiki.

7. Pemeliharaan dan Evaluasi Rencana

Perbaikan Berkelanjutan

- Rencana kontinjensi harus diperbarui secara rutin untuk mencakup perubahan dalam infrastruktur sistem, ancaman baru, atau pembaruan lingkungan operasional.
- Evaluasi Pasca-Incident: Setelah setiap insiden atau simulasi, lakukan evaluasi post-mortem untuk mengidentifikasi pelajaran yang dapat dipelajari, menilai efektivitas pemulihan, dan melakukan perbaikan pada rencana.

G. *Plan Testing, Training & Exercises*

1. Pengujian Rencana *(Plan Testing)*

Pengujian rencana *(Plan Testing)* dilakukan untuk memastikan kemampuan pemulihan dari rencana kontingensi dapat divalidasi dan dapat diaktifkan sesuai dengan prosedur secara efektif saat dibutuhkan.

Tabel 5. Pengujian Rencana *(Plan Testing)*

Tujuan	Aktivitas	Frekuensi	Langkah-langkah

Validasi Efektivitas Pemulihan Sistem	Melakukan pengujian DRP untuk memvalidasi prosedur pemulihan sistem di lingkungan Satker ZYX, termasuk pengujian backup dan pemulihan data penting.	Tahunan/Setelah Pembaruan Besar	1. Menyusun skenario uji coba pemulihan data dan sistem di Satker ZYX. 2. Menyusun tim penguji dan menetapkan peran masing-masing. 3. Melakukan uji coba pemulihan data dari server lokal dan Pusdatin. 4. Mengevaluasi hasil pengujian dan memperbaiki prosedur pemulihan bila diperlukan.
Memverifikasi Pemulihan Sistem dari Infrastruktur Alternatif	Menguji pemulihan sistem di platform alternatif, seperti server cadangan atau perangkat keras lain yang ada di lingkungan Satker ZYX.	Tahunan	1. Menentukan sistem yang akan diuji pemulihannya. 2. Melakukan uji coba pemulihan di platform alternatif (server lokal atau cadangan). 3. Memverifikasi bahwa pemulihan berjalan lancar tanpa gangguan. 4. Mencatat masalah yang ditemukan dan melakukan perbaikan yang diperlukan.

Uji Kelangsungan Operasi	Mensimulasikan skenario gangguan yang mempengaruhi kelangsungan operasional Satker ZYX, seperti pemadaman listrik atau gangguan server.	Tahunan	1. Menyusun skenario bencana yang relevan (misalnya, pemadaman listrik atau gangguan sistem). 2. Menentukan tim yang terlibat. 3. Melakukan simulasi untuk menguji kelangsungan operasi dan pemulihan. 4. Menyusun laporan hasil simulasi dan mengevaluasi efektivitas pemulihan.

2. Pelatihan *(Training)*

Pelatihan *(Training)* merupakan komponen kunci untuk memastikan kesiapan seluruh personel yang terlibat dalam proses kontingensi untuk merespons gangguan dengan efektif. Pelatihan ini dilakukan untuk mempersiapkan tim untuk menangani gangguan yang dapat mengganggu operasional dan meningkatkan koordinasi antar unit yang terlibat dalam pemulihan.

Tabel 6. Pelatihan *(Training)*

Tujuan	Aktivitas	Frekuensi	Langkah-langkah

Mempersiapkan Personel untuk Tanggapan Darurat	Menyediakan pelatihan tentang DRP untuk personel, termasuk peran mereka dalam pemulihan data dan sistem setelah bencana.	Setiap Tahun	1. Menyusun materi pelatihan DRP berdasarkan sistem dan prosedur yang berlaku di Satker ZYX. 2. Menyusun jadwal pelatihan dan seminar untuk personel terkait. 3. Melakukan pelatihan dengan simulasi peran dalam pemulihan. 4. Evaluasi hasil pelatihan dan tindak lanjut untuk perbaikan.
Meningkatkan Koordinasi Antar Tim	Melatih tim untuk memahami koordinasi yang efektif antara berbagai unit (IT, manajemen, keamanan informasi, dan operasional) selama pemulihan bencana.	Setiap Tahun	1. Menyusun materi pelatihan untuk koordinasi tim. 2. Mengorganisir pelatihan koordinasi antar tim Satker ZYX. 3. Melakukan evaluasi terhadap hasil pelatihan dan mengidentifikasi celah dalam koordinasi.
Pelatihan Pemulihan Data dan Sistem	Melatih staf untuk merespons skenario pemulihan data dan sistem dengan menggunakan perangkat yang tersedia dan prosedur	Setiap Enam Bulan	1. Menyusun skenario insiden yang melibatkan pemulihan data dan sistem. 2. Mengorganisir pelatihan berbasis simulasi dengan tim pemulihan.

	pemulihan yang telah disusun.		3. Melakukan simulasi pemulihan untuk mengevaluasi kesiapan tim. 4. Memberikan umpan balik dan memperbaiki prosedur.

3. Latihan (Exercises)

Latihan *(Exercises)* merupakan langkah penting dalam memastikan bahwa tim pemulihan siap menghadapi insiden nyata dan dapat merespons dengan cepat serta efisien. Bagian ini termasuk berbagai jenis latihan yang bertujuan untuk menguji kemampuan tim dalam mengelola dan memulihkan sistem informasi Satker ZYX. Fokus latihan adalah untuk meningkatkan koordinasi tim dan meningkatkan waktu respons. Untuk mempelajari fungsi dan tanggung jawab setiap tim dalam situasi darurat, latihan ini melibatkan simulasi insiden besar, pemulihan fungsional, dan latihan berbasis diskusi.

Tabel 7. Latihan *(Exercises)*

Tujuan	Aktivitas	Frekuensi	Langkah-langkah
Evaluasi Respons Tim dengan Latihan Tabletop	Melakukan latihan berbasis diskusi untuk mengeksplorasi peran dan tanggung jawab dalam menghadapi insiden bencana Satker ZYX.	Setiap Kuartal	1. Menyusun skenario bencana berbasis diskusi. 2. Mengorganisir latihan tabletop dengan tim yang terlibat. 3. Melakukan diskusi peran dan respons tim.

			4. Mengevaluasi hasil diskusi dan mengidentifikasi perbaikan yang dibutuhkan.
Latihan Pemulihan Fungsional	Mensimulasikan pemulihan data dan sistem secara langsung untuk menguji efektivitas pemulihan Satker ZYX.	Setiap Enam Bulan	1. Menyusun skenario latihan yang melibatkan pemulihan data. 2. Mengkoordinasikan tim untuk melaksanakan pemulihan dalam simulasi. 3. Mengevaluasi hasil latihan dan memperbaiki prosedur jika diperlukan.
Latihan Skala Penuh untuk Menguji Pemulihan Sistem	Mensimulasikan kegagalan sistem besar dan melaksanakan pemulihan penuh di situs pemulihan (hot site atau warm site) untuk memastikan kelangsungan operasional.	Setiap Tahun	1. Menyusun skenario pemulihan skala besar. 2. Melakukan latihan pemulihan dari hot site atau warm site. 3. Mengevaluasi waktu pemulihan dan koordinasi tim selama latihan. 4. Menyusun laporan dan memperbaiki prosedur pemulihan.

H. *Plan Maintenance*

Pemeliharaan rencana ini diperlukan untuk menjaga tiap prosedur dari pemulihan bencana dapat berjalan dengan baik setiap saat. Dengan melakukan tinjauan dan pembaruan secara berkala, Satker ZXY dapat memastikan bahwa setiap prosedur pemulihan

tetap sesuai dengan kebutuhan aktual, peraturan terbaru, dan hasil evaluasi risiko terkini.

Tabel 8. *Plan Maintenance*

Poin Rencana Pemeliharaan	Deskripsi	Langkah-langkah
Pembaruan dan Tinjauan Rencana	Pembaruan dan tinjauan DRP dilakukan secara berkala sesuai dengan interval yang telah direncanakan. Tinjauan ini mencakup hasil audit keamanan, insiden yang terjadi, serta perubahan organisasi, teknologi, ancaman, dan regulasi eksternal. Perubahan dilakukan berdasarkan asesmen risiko terbaru.	1. Menentukan interval tinjauan DRP. 2. Melakukan audit keamanan dan evaluasi insiden yang terjadi. 3. Menganalisis perubahan organisasi, teknologi, ancaman, dan regulasi eksternal. 4. Melakukan perbaikan dan pembaharuan berdasarkan hasil asesmen risiko.
Koordinasi Internal	Koordinasi internal dilakukan oleh Desk Pertahanan Siber Satker ZYX, Pusdatin Satker ZYX, satker pelaksana data dan informasi, serta unit-unit keamanan informasi. Pelibatan lintas fungsi untuk penyusunan, pelatihan, pelaksanaan, dan evaluasi DRP.	1. Menentukan tim koordinasi internal yang terlibat. 2. Mengadakan rapat koordinasi untuk evaluasi dan penyusunan DRP. 3. Melaksanakan pelatihan dan simulasi DRP bagi semua pihak yang terlibat. 4. Mengevaluasi hasil pelaksanaan DRP dan membuat laporan perbaikan.
Koordinasi Eksternal	Koordinasi eksternal melibatkan vendor penyedia layanan TIK, auditor independen, dan lembaga keamanan nasional seperti BSSN atau mitra keamanan luar negeri. Dilakukan sesuai dengan mekanisme resmi	1. Mengidentifikasi pihak eksternal yang perlu dilibatkan. 2. Menyusun mekanisme koordinasi dengan pihak eksternal. 3. Menjalin komunikasi rutin untuk memastikan kesiapan dan

	Satker ZYX dan ketentuan kerahasiaan yang berlaku.	keterlibatan dalam situasi darurat. 4. Melakukan pengecekan terhadap peraturan kerahasiaan dan regulasi keamanan informasi.
Kontrol Distribusi dan Dokumentasi Perubahan	Setiap perubahan DRP didokumentasikan secara sistematis, mencakup informasi siapa yang melakukan perubahan, tanggal perubahan, serta alasan dan substansi perubahan. Setiap versi dilengkapi dengan nomor versi dan tanggal penerbitan. Distribusi dilakukan secara terstruktur dan disertai dengan pelatihan serta sosialisasi rutin.	1. Membuat dokumentasi perubahan DRP secara lengkap (siapa, kapan, alasan, substansi). 2. Mengupdate nomor versi dan tanggal penerbitan DRP. 3. Menyebarkan dokumen DRP terbaru kepada pihak terkait. 4. Menyelenggarakan pelatihan dan sosialisasi mengenai pembaruan DRP kepada seluruh personel.

Ucapan Terima Kasih

Terima kasih penulis sampaikan kepada BALITBANG KEMHAN RI, yang telah mendukung penelitian ini.

PENUTUP

Simpulan

Berdasarkan hasil penelitian yang sudah dilakukan, hasil akhir dari penelitian ini berupa dokumen *Disaster Recovery Plan* (DRP) yang disusun untuk pedoman strategis persiapan menghadapi insiden serta prosedur pemulihan sistem informasi di Satker ZYX. dokumen ini berisikan langkah langkah yang terstruktur untuk menjaga layanan dan memastikan perlindungan terhadap aset informasi penting. *Disaster Recovery Plan* pada Satker ZYX dirancang melalui tahapan penting, meliputi identifikasi Skema Sistem Satker ZYX, Sistem Informasi Satker ZYX, *risk assessment*, *business impact analysis* (BIA), *Identify Preventive Controls*, Pengembangan Rencana

Kontingensi, *Plan Testing, Training & Exercises* dan *Plan Maintenance.* Penerapan keamanan informasi pada satker ZYX masih memerlukan beberapa peningkatan, terutama dalam bidang sistem informasi

Berdasarkan identifikasi risiko dan strategi kontingensi yang dirancang, ditemukan bahwa pemulihan sistem memerlukan pendekatan bertingkat sesuai dengan tingkat prioritas sistem. Untuk sistem dengan prioritas pemulihan tinggi diperlukan backup real-time dan pemulihan melalui hot site lalu untuk sistem dengan prioritas perlindungan sedang menggunakan backup harian dan pemulihan melalui warm site, sedangkan sistem dengan prioritas perlindungan rendah cukup menggunakan backup mingguan dan pemulihan melalui cold site. Selain itu, strategi cadangan dan pemulihan juga mencakup penggunaan penyimpanan data di luar lokasi, penggantian perangkat dengan sistem redundansi, serta penetapan peran tim pemulihan secara jelas dan terstruktur.

Saran

Berdasarkan hasil penelitian terdapat beberapa saran yang dapat disampaikan untuk meningkatkan efektivitas *Disaster Recovery Plan* (DRP) antara lain ialah peningkatan infrastruktur DRP mengingat pemulihan data yang cepat merupakan hal yang krusial, khususnya data-data sensitif dan bersifat privasi. Peningkatan infrastruktur dapat berupa meningkatkan kapasitas keamanan infrastruktur baik secara lokal maupun di luar lokasi, seperti penggunaan *cloud* dan replikasi data secara *real-time*. Pengembangan sistem backup otomatis juga perlu dipertimbangkan untuk mengurangi risiko kegagalan dalam proses backup manual. Pelatihan dan simulasi bencana juga perlu untuk dilakukan secara rutin untuk meningkatkan efektivitas waktu respons dalam mengidentifikasi kelemahan dalam proses DRP. Evaluasi DRP secara berkala juga sangat diperlukan, terutama setelah terjadi insiden besar atau perubahan dalam infrastruktur.

DAFTAR PUSTAKA

Admass, W.S., Munaye, Y.Y., & Diro, A.A. (2024). Cybersecurity: State of the art, challenges, and future directions. *Cyber Security and Applications*.

Akbar, B. I., Sucahyo, Y. G., & Gandhi, A. (2022). Disaster recovery plan design in energy government agency using NIST SP 800-34 guidelines. *AIP Conference Proceedings, 2499*(1), 050015. https://doi.org/10.1063/5.0105726

Ajayi, O.O., Alozie, C.E., & Abieba, O.A. (2025). Enhancing cybersecurity in energy infrastructure: Strategies for safeguarding critical systems in the digital age. *Trends in Renewable Energy*.

Antonelli, M., Aldrich, R., Tanner, R., & Ho, A. (2025). The storm is here: Public libraries' role in disaster preparedness and community recovery. *Electronic Green Journal, 51*, Article 2. https://doi.org/10.5070/G3.39629

Farid, G., Warraich, N. F., & Iftikhar, S. (2023). Digital information security management policy in academic libraries: A systematic review (2010–2022). *Journal of Information Science, 49*(4), 496–513. https://doi.org/10.1177/01655515231160026

Kavak, A. (2024). Impact of information security awareness on information security compliance of academic library staff in Türkiye. *Journal of Academic Librarianship, 50*(5), 102937. https://doi.org/10.1016/j.acalib.2024.102937

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cybersecurity: Emerging trends and recent developments. *Energy Reports*.

Linardos, V., Drakaki, M., & Tzionas, P. (2022). Machine learning in disaster management: Recent developments in methods and applications. *MDPI*.

McEntire, D.A. (2021). *Disaster response and recovery: Strategies and tactics for resilience*. Springer.

McIlwraith, A. (2021). *Information security and employee behaviour: How to reduce risk through employee education, training, and awareness*. Taylor & Francis.

Phillips, B.D., & Mincin, J. (2023). *Disaster recovery*. Taylor & Francis.

Sengan, S., Subramaniyaswamy, V., & Nair, S. K. (2021). Enhancing cyber–physical systems with hybrid smart city cybersecurity architecture for secure public data-smart network. *Elsevier*. https://doi.org/10.1016/j.future.2020.06.028

Stamenkov, G. (2025). Cloud service models, business continuity and disaster recovery plans, and responsibilities. *MDPI*.

Tóth, A. (2023). Information security threats in the digitalization of governance and their impact on elements of the defense sector. *BİLGESİNA*.

Wangen, G., & Ulven, J. B. (2021). A systematic review of cybersecurity risks in higher education. *Future Internet, 13*(2), 39. https://doi.org/10.1108/ICS-11-2018-013