KEMENTERIAN PENDIDIKAN, KEBUDAYAAN, RISET DAN TEKNOLOGI

UNIVERSITAS HASANUDDIN

PROSEDUR
MANAJEMEN INSIDEN KEAMANAN INFORMASI

No. PT/UH/DSITD-14

Status Dokumen	:	☐ Master	☐ Salinan, No.
Nomor Revisi	: 00		
Tanggal Terbit	: 23 Agustus 2024		

Dibuat oleh	Diperiksa oleh	Disahkan oleh
Kasubdit Teknologi Informasi dan Komunikasi	Direktur Sistem Informasi dan Transformasi Digital	Wakil Rektor Bidang SDM,Alumni dan Sistem Informasi
Muh. Yusni Ismail, S.T., M.T.	Dr. Eng. Ady Wahyudi Paundu, S.T., M.T.	Prof. Dr. Farida Patittingi, S.H., M.Hum.

DAFTAR REVISI

No. Revisi	Tanggal	Penjelasan Revisi

DAFTAR ISI

TUJUAN	Prosedur ini bertujuan untuk memberikan pedoman dalam hal Penanganan Insiden agar dapat dilaksanakan secara jelas, efektif, efisien dan terukur untuk menghindari kerugian yang lebih besar
RUANG LINGKUP	Prosedur ini mencakup beberapa rangkaian kerja yaitu identifikasi, pelaporan insiden, dan penanganan insiden
DEFINISI	1. Insiden keamanan informasi adalah satu atau serangkaian kejadian keamanan informasi yang memiliki peluang signifikan bagi pelemahan operasi bisnis dan peningkatan ancaman keamanan informasi 2. Keamanan Informasi adalah terjaganya kerahasiaan (confidentiality), keutuhan (integrity) dan ketersediaan (availability) informasi
KETENTUAN UMUM	1. Insiden terdeteksi sesegera mungkin dan dilaporkan dengan benar. 2. Yang termasuk dalam insiden keamanan informasi adalah : keamanan cyber, *server down,* dll 3. Insiden ditangani oleh personel berwenang yang tepat dengan cadangan 'terampil' sesuai kebutuhan. 4. Insiden dicatat dan didokumentasikan dengan baik. 5. Insiden ditangani tepat waktu dan layanan dipulihkan sesegera mungkin. 6. Semua insiden harus dianalisis dan dilaporkan kepada petugas yang ditunjuk.
REKAMAN /CATATAN	1. FT/UH/DSITD-03-01 Laporan Insiden Keamanan Informasi

UNIVERSITAS HASANUDDIN **DIREKTORAT SISTEM INDORMASI DAN TRANSFORMASI DIGITAL**	Nomor SOP	PT/UH/DSITD-14
	Tanggal Pembuatan/Terbit	23 Agustus 2024
	Tanggal Revisi	-
	Tanggal Efektif	
	Disahkan Oleh	Wakil Rektor Bidang SDM,Alumni dan Sistem Informasi Prof. Dr. Farida Patittingi, S.H., M.Hum
	NAMA SOP	STANDAR PENGAMANAN WEBSITE BERBASIS WORDPRESS PADA CPANEL

DASAR HUKUM / REFERENSI	KUALIFIKASI PELAKSANA
1. Undang-Undang Nomor 20 Tahun 2003 tentang Sistem Pendidikan Nasional 2. Undang-Undang Nomor 12 Tahun 2012 tentang Pendidikan Tinggi 3. Undang Undang No.11 Tahun 2008 tentang Informasi & Transaksi Elektronik (ITE) 4. Peraturan Pemerintah RI No. 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE) 5. SNI ISO 21001:2018 tentang Sistem Manajemen Organisasi Pendidikan-Persyaratan Klausul 8.5 Penyediaan Produk dan Layanan Pendidikan 6. SNI ISO 27001:2016 Sistem Manajemen Keamanan Informasi - Persyaratan, klausul 8.1 Perencanaan & pengendalian Operasional, Annex A.5.24 Manajemen perencanaan dan persiapan insiden keamanan informasi	1. Memiliki pemahaman tentang manajemen insiden 2. Memiliki kemampuan komunikasi yang baik 3. Memiliki kemampuan bekerja sama dan berkoordinasi dengan pihak lain
KETERKAITAN	**PERALATAN/PERLENGKAPAN**
- Tabel Manajemen Risiko - SOP akses ruang server	1. Laptop 2. Akses Internet
PERINGATAN	**PENCATATAN/PENDATAAN**
Jika SOP ini tidak dijalankan, dapat menyebabkan penanganan insiden tidak efektif yang menyebabkan kerugian lebih besar	Disimpan sebagai data elektronik dan manual

PROSEDUR :

A. Pelapor (Pimpinan, Staf)
   Melaporkan permasalahan insiden keamanan informasi melalui group media sosial (group WhatsApp DSITD)

B. Staf Admin Server, melakukan hal-hal sebagai berikut.
   1. Mencatat permasalahan insiden keamanan informasi yang terjadi pada form laporan insiden keamanan informasi (identitas pelapor, waktu, dampak, dll).
   2. Melaporkan kepada Kepala Seksi Teknologi Informasi dan Komunikasi mengenai kondisi insiden tersebut.

C. Kepala Seksi Teknologi Informasi dan Komunikasi, melakukan hal-hal sebagai berikut.
   1. Melakukan koordinasi dengan bawahannya untuk menangani kondisi insiden yang terjadi.
   2. Melakukan penanganan insiden tersebut
   3. Jika kondisi tidak normal tidak dapat ditangani sendiri maka melaporkan hal tersebut kepada Kepala Sub Direktorat DSITD.

D. Kepala Sub Direktorat melakukan hal-hal sebagai berikut.
   1. Melakukan koordinasi, baik internal maupun eksternal, dan mengambil keputusan untuk penanganan kondisi insiden tersebut.
   2. Melaporkan hasil penanganan insiden tersebut kepada Direktur
   3. Selesai.

PROSEDUR :

A. Pelapor (Pimpinan, Staf)
   Melaporkan permasalahan insiden keamanan informasi melalui group media sosial (group WhatsApp DSITD)

B. Admin Server, melakukan hal-hal sebagai berikut.
   1. Mencatat permasalahan insiden keamanan informasi yang terjadi pada form laporan insiden keamanan informasi (identitas pelapor, waktu, dampak, dll).
   2. Melakukan penilaian awal untuk menentukan tingkat keparahan insiden
   3. Melakukan investigasi menyeluruh dengan mengumpulkan bukti dan menganalisis data terkait insiden
   4. Melaporkan kepada Kepala Seksi Teknologi Informasi dan Komunikasi mengenai kondisi insiden tersebut.

C. Kepala Seksi Teknologi Informasi dan Komunikasi, melakukan hal-hal sebagai berikut.
   1. Melakukan koordinasi dengan bawahannya untuk menangani kondisi insiden yang terjadi.
   2. Melakukan penanganan insiden tersebut dengan merekomendasikan langkah mitigasi atau perbaikan
   3. Jika kondisi tidak normal tidak dapat ditangani sendiri maka melaporkan hal tersebut kepada Kepala Sub Direktorat DSITD.

D. Kepala Sub Direktorat melakukan hal-hal sebagai berikut.
   1. Melakukan koordinasi, baik internal maupun eksternal, dan mengambil keputusan untuk penanganan kondisi insiden tersebut.
   2. Implementasi rekomendasi dan pemantauan keberhasilan tindakan korektif
   3. Melakukan evaluasi akhir untuk memastikan insiden tidak terulang
   4. Melaporkan hasil penanganan insiden tersebut kepada Direktur
   5. Selesai.