Standar Operasional Prosedur

Penanganan Insiden Keamanan Informasi

2024

Kementerian Pendidikan dan Kebudayaan

Universitas Brawijaya

Jalan Veteran

0341 575878

Malang

KEMENTERIAN PENDIDIKAN DAN KEBUDAYAAN
UNIVERSITAS BRAWIJAYA
DIREKTORAT TEKNOLOGI INFORMASI

Nomor SOP	UN10.D20/HK.01.02.a/29
Tanggal Pembuatan	12 Juni 2023
Tanggal Revisi	1 Februari 2024
Tanggal Efektif	15 Februari 2024
Disahkan Oleh	Direktur DTI Dr. R. Arief Setyawan, S.T., M.T. NIP. 197508191999031001
Nama SOP	Penanganan Insiden Keamanan Informasi

DASAR HUKUM	KUALIFIKASI PELAKSANA
1. Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik 2. Peraturan Pemerintah No. 82 Tahun 2012 tentang Penyelenggara Sistem dan Transaksi Elektronik 3. Peraturan Rektor Nomor 73 Tahun 2020 tentang Perubahan Atas Peraturan Rektor Nomor 25 Tahun 2020 tentang Susunan Organisasi dan Tata Kerja 4. Peraturan Rektor Nomor 55 Tahun 2020 tentang Rencana Strategis Universitas Brawijaya Tahun 2020—2024 5. Panduan Pelaksanaan Manajemen Keamanan Informasi	1. Direktur DTI 2. Kasubdit 3. Administrator Sistem
PENJELASAN SINGKAT	**TUJUAN**
SOP Penanganan Keamanan Informasi ini menjelaskan langkah-langkah yang harus dilakukan ketika terjadi insiden pada keamanan informasi. Ruang lingkup insiden kemanan informasi terdiri dari 2 bagian yaitu yang disebabkan oleh program jahat (Worm, Virus, Backdoor, dan sejenisnya) dan aktivitas peretas. Aktivitas peretas yang harus ditangani adalah percobaan pemaksaan akses pada sistem dan akses oleh pengguna yang tidak punya otorisasi.	SOP Penanganan Keamanan Informasi ini disusun dengan tujuan untuk mencegah atau meminimalkan kerugian yang ditimbulkan dari insiden ini dan jika sudah mengganggu maka SOP ini juga bertujuan megembalikan operasi layanan normal kembali dan meminimalkan dampak negatif operasional layanan/aplikasi, sehingga memastikan tingkat kualitas dan ketersediaan layanan/aplikasi dapat dipertahankan.
KETERKAITAN	**PERALATAN/PERLENGKAPAN**
1. Sistem Informasi yang sudah dibangun sebelumnya 2. Authentikasi di UB	1. Sistem monitoring 2. Sistem Log 3. Laporan Insiden 4. Laporan Identifikasi dan Penanganan Insiden 5. Peralatan identifikasi dan proteksi keamanan informasi
PERINGATAN	**PENCATATAN DAN PENDATAAN**
1. Pelaksana bertanggung jawab atas pelaksanaan aktivitas yang telah dibakukan dan ditetapkan.	Disimpan sebagai data elektronik dan manual

No	Aktifitas	Pelaksana			Mutu Baku			Keterangan
		Helpdesk	Administrator Sistem	Kasubdit	Persyaratan/Perlengkapan	Waktu (menit)	Output	
Prosedur Penanganan Insiden Keamanan Informasi Karena Program Jahat								
1	Pengguna melaporkan insiden kepada Helpdesk DTI	mulai			https://helpdesk-tik.ub.ac.id/	Ticket		
2	Administrator Sistem Melakukan isolasi layanan/sistem melalui pemutusan koneksi keluar					10	Layanan/Sistem Disconnect	
3	Administrator Sistem mencatat kejadian dalam Logbook Insiden Keamanan Informasi				Laporan Insiden	10	Laporan Insiden	
4	Administrator Sistem memberitahukan kejadian ini kepada Kasubdit dan menunggu arahan kebijakan prosedur yang harus dilakukan					60		
5	Kasubdit meminta kepada Helpdesk untuk menginformasikan penghentian sementara Sistem untuk memberikan kesempatan perbaikan					60		
6	Administrator Sistem Menangani insiden keamanan informasi dan melakukan identifikasi insiden dan melakukan backup log sistem dan status sistem informasi				Laporan identifikasi insiden dan backup log	60	Laporan identifikasi insiden dan backup log	
7	Administrator menangani insiden keamanan informasi melakukan pembersihan sistem dari program jahat dengan menghentikan sementara sistem yang berjalan					60		
8	Jika pembersihan sistem selesai dilakukan, dilanjutkan dengan melakukan patch yang diperlukan					60		
9	jika sudah selesai tahapan tersebut, maka Administrator Sistem melakukan tindak lanjut mengembalikan sistem berjalan seperti biasa					60		
10	Menangani insiden Keamanan Informasi mendokumentasikan penanganan Insiden tersebut untuk keperluan pelaporan atau referensi		selesai		Laporan Insiden	60	Laporan Insiden	

No	Aktifitas	Pelaksana				Mutu Baku			Keterangan
		Helpdesk	Administrator Sistem	Kasubdit	ID SIRTII	Persyaratan/Perlengkapan	Waktu (menit)	Output	
Prosedur Penanganan Insiden Keamanan Informasi Karena Aktivitas Peretas yang Memaksa Akses pada Sistem									
1	Administrator Sistem melakukan isolasi layanan/sistem melalui pemutusan koneksi keluar		mulai				10	Layanan/Sistem Disconnect	
2	Administrator Sistem melakukan identifikasi masalah dengan cara mencari sumber serangan berdasarkan file, sistem log dan koneksi jaringan aktif					sistem log	180	capture file, aktivitas log	
3	Administrator Sistem melakukan pemberitahuan kepada Kasubdit untuk mendapatkan otoritas langkah selanjutnya						60		
4	Apakah sumber serangan diketahui		tidak ya						
5	Jika sumber serangan diketahui maka dilakukan patch yang diperlukan dan penutupan akses masuk yang dilakukan peretas pada layanan/sistem yang diakses						60		
6	Jika sumber serangan tidak diketahui maka sistem yang diretas dinonaktifkan terlebih dahulu untuk sementara dan menghubungi Support ID SIRTII untuk mendapatkan dukungan/bantuan informasi tentang serangan ini					https://idsirtii.or.id/halaman/tentang/kontak-kami.html	120		
7	Setelah penyelidikan dilakukan maka buat laporan pendek berkenan dengan insiden dan langkah yang harus diambil dan sebarkan informasi kepada pihak yang berkemptingan lainnya		selesai			Laporan insiden	60	Laporan Insiden	