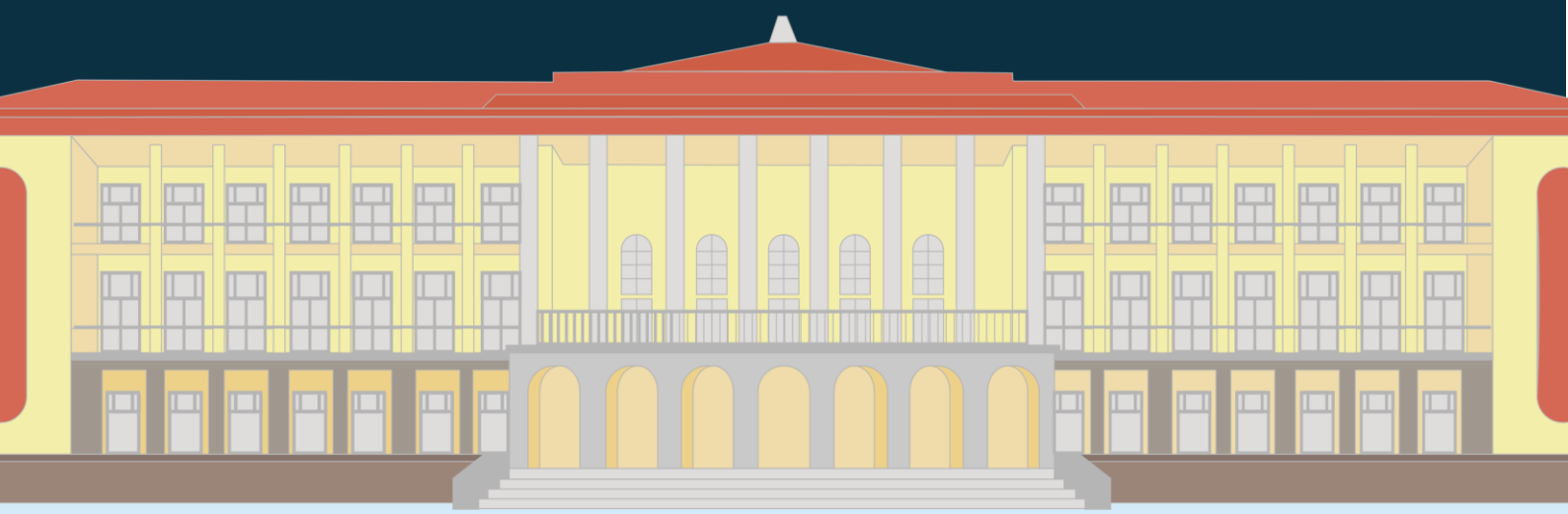
UNIVERSITAS
GADJAH MADA

Kebijakan Penguatan Manajemen Keamanan Teknologi Informasi di Universitas Gadjah Mada

Policy for Strengthening Information Technology Security Management at Gadjah Mada University



Daftar Isi

UNIVERSITAS
GADJAH MADA

Kebijakan Penguatan Manajemen Keamanan Teknologi Informasi di Universitas Gadjah Mada

Policy for Strengthening Information Technology Security Management at Gadjah Mada University

1. Ringkasan Eksekutif

Universitas Gadjah Mada (UGM) tengah melakukan percepatan transformasi digital dan pengembangan smart campus melalui pemanfaatan *Internet of Things (IoT)*, *big data analytics*, kecerdasan buatan (AI), serta sistem layanan akademik dan administrasi berbasis digital. Transformasi ini membawa peluang besar bagi peningkatan kualitas pendidikan, riset, dan tata kelola kampus. Namun, di sisi lain, peningkatan kompleksitas teknologi menimbulkan tantangan serius dalam aspek keamanan informasi, perlindungan data, dan pengaturan ruang udara kampus.

Ancaman seperti kebocoran data pribadi sivitas akademika, serangan siber terhadap infrastruktur digital, dan penggunaan drone tanpa izin dapat memengaruhi reputasi serta keselamatan kampus. Dengan volume data yang semakin besar ─ mulai dari data mahasiswa, hasil riset, dokumen kerjasama, hingga informasi kelembagaan strategis ─ risiko penyalahgunaan informasi menjadi semakin signifikan.

Policy brief ini mengusulkan kebijakan terpadu untuk penguatan keamanan informasi dan pengaturan penggunaan ruang udara berbasis drone di lingkungan UGM. Kebijakan disusun berlandaskan ISO/IEC 27001:2022 tentang sistem manajemen keamanan informasi dan regulasi nasional terkait penerbangan drone. Dengan pendekatan preventif, detektif, dan responsif, kebijakan ini diharapkan menjadikan UGM sebagai model smart campus yang aman, inovatif, dan berdaya saing global.

2. Latar Belakang

UGM sedang melakukan digitalisasi berbagai layanan kampus, termasuk integrasi *smart campus*, aplikasi berbasis IoT, analitik Big Data, dan kecerdasan buatan. Namun, meningkatnya konektivitas teknologi diikuti pula oleh risiko:

- Belum adanya sistem manajemen keamanan informasi yang menyeluruh dan berstandar di seluruh unit.
- Aset informasi UGM (data mahasiswa, dosen, riset, keuangan, dll.) memiliki risiko tinggi terhadap kebocoran, manipulasi, atau *ransomware*.
- Keamanan sistem masih sangat bergantung pada kebijakan unit masing-masing tanpa koordinasi strategis.
- Tidak adanya mekanisme standar pelaporan, audit, dan respons terkait insiden keamanan siber
- Peraturan Badan Siber dan Sandi negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis Dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik

3. Tujuan Kebijakan

- Membangun *Information Security Management System* (ISMS) universitas yang mengacu pada standar internasional (misalnya ISO/IEC: 27001).
- Menjamin keamanan sistem informasi dan data universitas dalam kerangka *confidentiality*, *integrity*, dan *availability*.
- Mengembangkan budaya kesadaran keamanan digital pada seluruh sivitas akademika UGM.
- Mengatur peran dan tanggung jawab keamanan informasi secara institusional dan berkelanjutan.

4. Elemen Strategis Manajemen Keamanan Teknologi Informasi (TI)

a. Kebijakan dan Tata Kelola Keamanan Informasi

- Penetapan dokumen kebijakan keamanan TI tingkat universitas.
- Penunjukan *Chief Information Security Officer (CISO)* atau pejabat setara.
- Pembentukan tim keamanan informasi di lintas unit.

b. Manajemen Risiko Keamanan Siber

- Identifikasi aset digital dan penilaian risiko.
- Rencana mitigasi dan proteksi aset utama seperti server pusat, data mahasiswa, dan sistem keuangan.

c. Pengamanan Infrastruktur dan Aplikasi

- Enkripsi, firewall, sistem deteksi intrusi, VPN institusi.
- Penguatan autentikasi pengguna (MFA, SSO, sertifikat digital).
- Pengamanan aplikasi dan layanan *cloud* yang digunakan oleh UGM.

d. Manajemen Akses dan Privasi Data

- Pengaturan hak akses berbasis peran (RBAC).
- Kebijakan proteksi data pribadi dan kerahasiaan hasil penelitian.

e. Audit, Monitoring, dan Penanggulangan Insiden

- Sistem pemantauan terpusat terhadap aktivitas digital yang abnormal.
- Prosedur respon terkait insiden dan *disaster recovery plan*.

f. Pendidikan dan Budaya Keamanan Digital

- Kampanye literasi keamanan siber bagi dosen, mahasiswa, dan tenaga kependidikan.
- Pelatihan berkala dan simulasi respon jika terjadi serangan siber.

5. Rekomendasi Kebijakan

1. **Mengesahkan Kebijakan Keamanan TI UGM sebagai Peraturan Rektor**

   Dokumen formal sebagai dasar pelaksanaan, evaluasi, dan penguatan kontrol terkait keamanan informasi.

2. **Mendirikan Unit Keamanan Informasi UGM (*UGM-CSIRT* atau *SOC*)**

   Bertanggung jawab terhadap pengawasan, penanggulangan, dan pengembangan keamanan digital kampus.

3. **Melakukan Sertifikasi dan Audit Keamanan Berkala**

   Sertifikasi ISO/IEC: 27001 untuk sistem kritis dan audit keamanan sistem utama secara berkala (setiap tahun).

4. **Mewajibkan Prosedur Keamanan Minimal pada Pengembangan Sistem**

   Mengimplementasikan keamanan ada pengembangan sistem. Termasuk kode aman, audit kerentanan, dan pengujian penetrasi sebelum peluncuran sistem.

5. **Integrasi dengan Kebijakan Nasional dan Global**

   Mengimplementasikan dan menerapkan kebijakan sesuai dengan UU PDP, Permendikbudristek, NIST *Cybersecurity Framework*, dan The General Data Protection Regulation (GDPR) serta peraturan yang berlau.

6. Manfaat Implementasi

- Meningkatkan kepercayaan pengguna dan mitra terhadap layanan digital di UGM.
- Mencegah kerugian finansial, reputasi, dan operasional akibat insiden siber.

- Memastikan keberlangsungan layanan akademik dan administratif tanpa gangguan digital.
- Mendukung transformasi digital yang aman dan berkelanjutan di lingkungan UGM.

7. Penutup dan Tindak Lanjut

Keamanan teknologi informasi adalah tanggung jawab kolektif dan bagian tak terpisahkan dari tata kelola universitas modern. Universitas Gadjah Mada perlu mengambil langkah tegas dan terstruktur dalam membangun sistem keamanan digital yang handal sebagai bagian dari misi transformasi digital UGM untuk masa mendatang.

UNIVERSITAS
GADJAH MADA

Kebijakan Penguatan Manajemen Keamanan Teknologi Informasi di Universitas Gadjah Mada

Bulaksumur, Caturtunggal, Kec. Depok, Kabupaten Sleman,
Daerah Istimewa Yogyakarta 55281