Analisis Informasi Publik Dikecualikan : Source Code Portal Akademik, Kata Sandi (Password), Dan Arsitektur Teknis Keamanan Server/Jaringan Kampus

Dokumen Penjaminan Mutu Internal

METADATA			
Kode Dokumen	DT/UPT-TIPD/2026/025	Unit Kerja	UPT TIPD
Revisi Ke-	0	Penanggung Jawab	Kepala UPT TIPD
Tanggal Penyusunan	1 Desember 2025	Tanggal Efektif	1 Januari 2026

1. Pendahuluan dan Latar Belakang

Dalam pengelolaan sistem informasi dan infrastruktur teknologi di lingkungan perguruan tinggi, prinsip keterbukaan informasi publik harus diselaraskan dengan standar keamanan siber dan perlindungan aset digital. Badan publik diwajibkan melindungi sistem elektronik yang dikelolanya dari berbagai potensi ancaman siber, peretasan, dan sabotase.

Dokumen ini menyajikan analisis komprehensif mengenai alasan hukum, teknis, dan manajerial mengapa kode sumber (source code) portal akademik, kata sandi (password) sistem, serta arsitektur teknis keamanan server/jaringan kampus dikategorikan sebagai Informasi yang Dikecualikan dari publik.

2. Dasar Hukum dan Kerangka Regulasi

Klasifikasi ketiga elemen teknologi informasi tersebut sebagai informasi rahasia/dikecualikan didasarkan pada regulasi nasional yang berlaku:

- Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (UU KIP) :
  - Pasal 17 Huruf a: Informasi publik yang apabila dibuka dapat membahayakan pertahanan dan keamanan negara/institusi.
  - Pasal 17 Huruf b: Informasi publik yang apabila dibuka dapat mengganggu perlindungan hak atas kekayaan intelektual (HKI) dan persaingan usaha tidak sehat.
  - Pasal 17 Huruf i: Informasi publik yang apabila dibuka dapat merusak atau membahayakan sarana dan prasarana vital/infrastruktur publik.
- Undang-Undang Nomor 11 Tahun 2008 jo. UU Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik (UU ITE):
  - Mengatur larangan akses ilegal (unauthorized access), penerobosan, dan perusakan sistem elektronik/infrastruktur informasi vital.
- Peraturan BSSN Nomor 8 Tahun 2020 tentang Sistem Manajemen Keamanan Informasi:
  - Mewajibkan penyelenggara sistem elektronik untuk menjaga kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability) aset data serta kredensial akses.

3. Analisis Per Elemen Data Pribadi

Berikut adalah perincian alasan spesifik mengapa ketiga variabel data tersebut harus dirahasiakan dari akses umum :

Komponen TI / Sistem	Risiko Pembukaan Informasi kepada Publik	Alasan Teknis & Manajerial Pengecualian
Source Code Portal Akademik	• Memudahkan peretas (hacker) menemukan celah keamanan (vulnerability/zero-day exploit). • Risiko manipulasi nilai, manipulasi data kelulusan, dan pemalsuan ijazah. • Pelanggaran Hak Kekayaan Intelektual (HKI) atas ciptaan perangkat lunak kampus.	Source code memuat logika bisnis, struktur basis data, dan metode autentikasi internal. Membuka kode sumber sama dengan memberikan peta jalan (roadmap) bagi pihak tak bertanggung jawab untuk mengeksploitasi celah sistem.
Kata Sandi (Password) Sistem & Kredensial Akses	• Akses ilegal langsung ke dalam server, basis data, dan panel kontrol administratif. • Pencurian, pengubahan, atau penghapusan data masif (data breach/data destruction). • Penyebaran malware, ransomware, atau penguasaan kontrol sistem secara penuh.	Kata sandi merupakan instrumen kunci autentikasi utama. Berdasarkan prinsip kerahasiaan (confidentiality), kredensial akses hanya boleh diketahui oleh personel terotorisasi (prinsip *Need-to-Know*).
Arsitektur Teknis Keamanan Server & Jaringan	• Pemetaan titik lemah jaringan (network mapping) untuk serangan DDoS. • Bypass lapisan pertahanan seperti Firewall, IDS/IPS, dan Web Application Firewall (WAF). • Lumpuhnya seluruh layanan publik dan operasional perkuliahan berbasis digital.	Topologi jaringan dan konfigurasi keamanan merupakan cetak biru (blueprint) pertahanan digital. Mengungkap arsitektur jaringan akan melumpuhkan efektivitas sistem pertahanan berlapis (defense-in-depth).

4. Uji Konsekuensi dan Uji Kepentingan Publik

Sesuai dengan ketentuan Pengujian Konsekuensi oleh Pejabat Pengelola Informasi dan Dokumentasi (PPID) :

- Uji Konsekuensi (Consequence Test)
  Jika source code, password, atau arsitektur jaringan dibuka kepada publik, potensi bahaya yang ditimbulkan meliputi kelumpuhan total sistem informasi kampus, kebocoran data pribadi ribuan mahasiswa/dosen, serta kerugian finansial dan reputasi yang sangat berat. Konsekuensi negatif ini jauh melampaui manfaat keterbukaan informasi biasa.
- Uji Kepentingan Publik (Public Interest Test)
  Kepentingan publik terhadap transparansi perguruan tinggi telah dipenuhi melalui publikasi profil layanan, statistik akreditasi, pedoman akademik, serta laporan kinerja/keuangan.

Publik tidak membutuhkan detail teknis berupa kode sumber atau kata sandi untuk menilai akuntabilitas penyelenggaraan Pendidikan.

5. Kesimpulan dan Rekomendasi

- Kesimpulan:
  Mengkategorikan source code portal akademik, kata sandi, dan arsitektur keamanan jaringan sebagai informasi yang dikecualikan merupakan langkah hukum dan teknis yang wajib dilakukan guna menjamin kelangsungan operasional serta integritas data kampus.
- Saran Pengelolaan :
  - PPID bersama unit Teknologi Informasi (Puskom/LTI) wajib menerbitkan Surat Keputusan Penetapan Informasi yang Dikecualikan secara formal.
  - Menerapkan prinsip least privilege dan enkripsi ketat pada seluruh sistem penyimpanan data dan transmisi jaringan.
  - Melakukan audit keamanan siber (penetration testing) berkala oleh pihak ketiga tepercaya secara tertutup.

Kepala UPT
Teknologi Informasi dan Pangkalan Data

I Dewa Gede Budiastawa