

## ABSTRAK

### **Firqohtunnajiyah Salim, Nur Khaerah, Nursaleh Hartaman. 2026 Strategi Cybersecurity Dinas Komunikasi Dan Informatika Dalam Mendukung Transformasi Digital Pemerintah Kota Makassar**

Transformasi digital Pemerintah Kota Makassar melalui Sistem Pemerintahan Berbasis Elektronik (SPBE) memperluas ketergantungan pada layanan daring sekaligus meningkatkan risiko *phishing/vishing*, *defacement*, *DDoS*, *malware*, hingga potensi *ransomware*. Penelitian ini bertujuan menganalisis strategi *cybersecurity* Dinas Komunikasi dan Informatika (Diskominfo) Kota Makassar dalam menjaga keberlanjutan layanan dan perlindungan data pemerintah daerah. Metode penelitian adalah deskriptif kualitatif dengan pengumpulan data melalui wawancara mendalam, observasi, dan dokumentasi menggunakan *purposive sampling*. Analisis data dilakukan dengan model Miles, Huberman, dan Saldaña, serta keabsahan data diuji melalui triangulasi sumber dan teknik. Hasil penelitian menunjukkan strategi *cybersecurity* dioperasionalkan melalui tiga indikator. Pertama, pencegahan: penerapan SMKI, evaluasi kebijakan, SOP operasional (pengelolaan akses, penggunaan email dinas, *patching*, *backup*, dan pelaporan awal), sosialisasi SDM, penguatan infrastruktur, serta kontrol akses dan hardening termasuk *firewall*. Kedua, deteksi: monitoring sistem dan jaringan, analisis anomali oleh tim, pelaporan via helpdesk, klasifikasi serta eskalasi insiden, dan koordinasi dengan PIC OPD serta BSSN pada kasus tertentu. Ketiga, pemulihan: verifikasi dampak, penanganan teknis, aktivasi *backup*/DRC bila diperlukan, dokumentasi rekomendasi, dan pembelajaran pasca-insiden. Temuan ini menegaskan perlunya penguatan prosedur dan koordinasi lintas OPD untuk meningkatkan ketahanan SPBE.

**Kata kunci:** *cybersecurity*, SPBE, Diskominfo, pencegahan, deteksi, pemulihan.

## ABSTRACT

***Firgohtunnajiyah Salim, Nur Khaerah, Nursaleh Hartaman. 2026 Cybersecurity Strategy of the Communication and Information Agency in Supporting the Digital Transformation of the Makassar City Government***

*The digital transformation of the Makassar City Government through the Electronic-Based Government System (SPBE) has increased dependence on online services while also increasing the risk of phishing/vishing, defacement, DDoS, malware, and even ransomware. This study aims to analyze the cybersecurity strategies of the Makassar City Communication and Information Agency (Diskominfo) in maintaining the sustainability of services and protecting local government data. The research method is descriptive qualitative with data collection through in-depth interviews, observation, and documentation using purposive sampling. Data analysis was conducted using the Miles, Huberman, and Saldaña model, and data validity was tested through source and technique triangulation. The results of the study show that cybersecurity strategies are operationalized through three indicators. First, prevention: implementation of SMKI, policy evaluation, operational SOPs (access management, use of official email, patching, backup, and initial reporting), human resource socialization, infrastructure strengthening, and access control and hardening, including firewalls. Second, detection: system and network monitoring, anomaly analysis by the team, reporting via the helpdesk, incident classification and escalation, and coordination with the OPD PIC and BSSN in certain cases. Third, recovery: impact verification, technical handling, activation of backup/DRC if necessary, documentation of recommendations, and post-incident learning. These findings emphasize the need to strengthen procedures and coordination across OPDs to improve SPBE resilience.*

**Keyword:** *Cybersecurity, SPBE, Department of Communication and Information Technology, prevention, detection, recovery.*