INDONESIA
FINANCIAL SERVICES
AUTHORITY

SP 86/DKPU/OJK/IV/2026

PRESS RELEASE

OJK ENHANCES NATIONAL DIGITAL FINANCIAL INDUSTRY'S CYBER DEFENSE CAPACITY

Jakarta, 30 April 2026. Indonesia Financial Services Authority (OJK) continues to enhance the national digital financial industry's cyber defence capacity to maintain for the industry's endurance and public's trust.

"Cyber defense goes beyond technical issue, it is a main prerequisite of the digital financial industry's continuation. In the increasingly interconnected ecosystem, one cyber incident will impact not only one institution, but the reputation, credibility, and ecosystem of the overall ecosystem," Chief Executive of Financial Sector Technology Innovation, Digital Assets, and Crypto Assets Supervision of OJK Adi Budiarso during the 2026 Cyber Security Workshop for Financial Sector Technology Innovation (FSTI), Digital Financial Assets (DFA), and Cr ypto Assets Operators in Jakarta, on Monday (27/4).

The workshop was held in collaboration with the National Cyber and Crypto Agency (BSSN) as a part of OJK's commitment in improving digital financial industry's foresight in facing growingly complex, fast cyber threats that widely impacts public confidence.

Adi reiterates that the industry needs to shift to resilience-based security from compliance-based security, underlining that cybersecurity should be a part of business strategy, corporate governance, risk management, and consumer in addition to compliance.

"Trust is the main currency of digital economy. Quick innovations should be measured up with security. Without proper cybersecurity, innovations will become a new vulnerability to the public and the industry," Adi said.

Henceforth, OJK encourages all FSTI, DFA, and Crypto Asset Operators to prioritize strategic investment in cybersecurity. Cybersecurity enhancement will make a significant difference for industry players' credibility establishment, services continuation, and competitiveness amid the digital economy development.

OJK also highlights human capital enhancement in the digital financial sector. Solid security technology shall be supported with competence, operational discipline, prepared procedure, as well as transparent and responsible incident reports.

The workshop was held on 27 to 29 April 2026 in Jakarta, participated by FSTI, DFA and Crypto Asset (IAKD) Operators. The workshop participants are comprised mostly of IAKD Operators Board of Directors. The workshop aims to increase knowledge, alertness, human resources capacity, and industry's capability in cyber incident prevention, detection, response, and recovery.

Human Firewall

By collaborating with BSSN, OJK continues to strengthen institutional synergism in developing national cyber defense, particularly in the digital financial services sector. Cross-institution collaborations are essential as cyber threats are not bound to sectoral, institutional, and even jurisdictional limits.

Deputy of Economic Cyber and and Crypto of BSSN Slamet Aji Pamungkas emphasized the significance of human firewall, a cybersecurity concept that puts the employees in the frontline through training and awareness to detect cyber threats such as phishing and malware.

Meanwhile, OJK will continue to expand cooperation with ministries/institutions, law enforcement apparatus, industry associations, and business players to ensure integrated cyber risk management.

In the report session, Deputy Commissioner of Human Resources of OJK Irnal Fiscallutfi presented the Cyber Security Workshop for FSTI, DFA, and Crypto Assets Operators as a measure to enhance the industry's capacity and resilience.

This event is designed to raise awareness, align comprehension on cyber risk profiles, and improve human capital competency in effective and structure cyber incident detection, prevention, and response.

***

For more information
Head of Integrated Financial Services Sector Surveillance and Policy Department of OJK – Agus Firmansyah
Tel. 021.29600000; Email: humas@ojk.go.id