

New Policy Relative to Computer and Cyber Security

Ankur Soni, Student, Dept. of Management, Janardan Rai Nagar Rajasthan Vidyapeeth University, Udaipur, Rajasthan

Abstract

The rapid growth of digital technologies, cloud computing, artificial intelligence, and interconnected information systems has significantly increased the need for effective policies related to computer and cyber security. This study examines emerging cybersecurity policies and their role in protecting digital infrastructure, sensitive information, organizational networks, and individual privacy. The paper focuses on major policy areas, including data protection, cybercrime prevention, incident reporting, risk management, access control, security awareness, and organizational accountability. Modern cybersecurity policies increasingly emphasize proactive threat detection, continuous monitoring, secure-by-design principles, zero-trust approaches, and coordinated responses to cyber incidents. The study also considers the challenges organizations face in implementing new security policies, including rapidly changing cyber threats, technological complexity, lack of skilled professionals, compliance requirements, and increasing dependence on third-party digital services. Effective policies require cooperation among governments, private organizations, technology providers, and users to establish clear responsibilities and consistent security practices. Furthermore, cybersecurity policies must balance strong protection with privacy, accessibility, innovation, and economic development. The study highlights the importance of regularly reviewing and updating security policies to address emerging threats such as ransomware, phishing, social engineering, artificial intelligence-enabled attacks, and supply-chain vulnerabilities. Overall, the research emphasizes that comprehensive, adaptable, and risk-based cybersecurity policies are essential for strengthening digital resilience and maintaining trust in modern information systems.

Keywords: Cybersecurity Policy, Computer Security, Data Protection, Cybercrime, Risk Management, Data Privacy, Cyber Resilience, Information Security, Digital Infrastructure, Cyber Threats.