

JUNE 2026



HKIT SECURITY SOLUTIONS

NEWSLETTER

WELCOME TO THE JUNE 2026 EDITION

June 2026 was a milestone month for HKIT Security Solutions, marked by innovation, customer success, and continued excellence in cybersecurity and compliance. This edition highlights the launch of our new platforms—BHISH – The Cyber Mentor and RADHE CRM, the successful completion of external ISO certification audits for our valued clients, and expert insights into AI security and emerging cyber threats.

INSIDE THIS EDITION

- 🚀 Product Launches
- 🎓 BHISH – The Cyber Mentor
- 📊 RADHE CRM
- 🏆 ISO Certification Audit Success
- 🤖 AI Security Spotlight
- 🛡️ AI Security Best Practices

New Product Launch

BHISH - The Cyber Mentor

As cyber threats continue to evolve and regulatory requirements become more stringent, organizations need more than occasional training—they need continuous, engaging, and measurable learning. BHISH – The Cyber Mentor was developed to bridge the gap between compliance and practical cybersecurity awareness by providing a centralized, interactive Learning Management System (LMS) for individuals and organizations.

Key Features

- ✓ Cyber Security Awareness
- ✓ ISO 27001 Training
- ✓ DPDP Act Training
- ✓ GDPR Awareness
- ✓ Interactive Learning
- ✓ Online Assessments
- ✓ Progress Tracking
- ✓ Completion Certificates
- ✓ Organization-wide Training
- ✓ Role-based Learning



Organizations are increasingly targeted through human error. Continuous awareness training helps reduce cyber risks and strengthens an organization's overall security posture.

BHISH is more than a training platform—it is HKIT's commitment to creating a cyber-aware workforce and helping organizations build a culture of security, compliance, and continuous learning.

New Product Launch

RADHE CRM

Streamlining Business Operations Through Intelligent Workflow Management

As organizations grow, managing customer interactions, proposals, work orders, and invoicing efficiently becomes essential for maintaining productivity and delivering exceptional customer service. Traditional manual processes often result in delays, inconsistencies, and limited visibility into business operations. To address these challenges, HKIT Security Solutions developed RADHE CRM, an internal Customer Relationship Management platform designed to simplify and automate day-to-day business processes.

Key Features

- ✓ Proposal Management
- ✓ Work Order Management
- ✓ Invoice Generationn
- ✓ Customer Database Management
- ✓ Centralized Document Repository
- ✓ Workflow Automation
- ✓ Activity & Status Tracking
- ✓ Business Reporting & Dashboard
- ✓ Secure Role-Based Access
- ✓ Role-based Learning



More than just a CRM, RADHE is HKIT's integrated business management platform that empowers teams to collaborate efficiently, automate routine tasks, maintain complete document traceability, and support informed decision-making through streamlined processes and centralized information management.

ISO/IEC 27001:2022 Certification Successfully Completed

42 Card Solutions Pvt. Ltd.

HKIT Security Solutions successfully completed the ISO/IEC 27001:2022 External Certification Audit for 42 Card Solutions Pvt. Ltd. The audit involved a comprehensive assessment of the organization's Information Security Management System (ISMS), including risk management practices, security controls, documentation, and regulatory compliance. Through effective implementation of ISO 27001:2022 requirements, the organization demonstrated its commitment to protecting information assets and continually improving its security posture. We congratulate the team at 42 Card Solutions Pvt. Ltd. on this significant achievement.

Airport Information Systems

HKIT Security Solutions also successfully completed the ISO/IEC 27001:2022 External Certification Audit for Airport Information Systems. The audit evaluated the organization's information security framework, operational controls, risk treatment processes, asset management, and compliance with ISO 27001:2022 requirements. The successful certification reflects the organization's dedication to maintaining a robust Information Security Management System and safeguarding critical business information. We appreciate the excellent cooperation and commitment demonstrated by the Airport Information Systems team throughout the certification process.

AI Security: Securing the Future in the Age of Artificial Intelligence

Artificial Intelligence (AI) has rapidly transformed the way businesses operate, enabling automation, intelligent decision-making, predictive analytics, and enhanced customer experiences. Organizations across industries are increasingly integrating AI into their daily operations to improve efficiency and drive innovation. While AI offers tremendous opportunities, it also introduces new cybersecurity challenges that organizations must proactively address.

Cybercriminals are now leveraging AI to launch more sophisticated, targeted, and scalable attacks than ever before. AI-powered phishing campaigns, deepfake videos, automated malware generation, prompt injection attacks, and data poisoning are becoming increasingly common.

AI Security Best Practices

- Establish a Clear AI Governance Policy
- Classify Data Before Using AI Tools
- Never Upload Confidential or Sensitive Information to Public AI Platforms
- Implement Role-Based Access Control (RBAC) and Multi-Factor Authentication (MFA)
- Verify AI-Generated Content Before Use
- Monitor and Audit AI Usage Continuously
- Secure AI APIs with Strong Authentication and Encryption
- Conduct Regular AI Risk and Vulnerability Assessments
- Train Employees on Secure and Responsible AI Usage
- Keep AI Models, Libraries, and Dependencies Updated



Deepfake Awareness: Think Before You Trust

Deepfake technology has made it increasingly difficult to distinguish genuine digital content from manipulated media. Organizations should encourage employees to verify unexpected video calls, voice messages, payment requests, and executive communications through independent channels before taking action.

Protect Yourself from Deepfakes

- ✓ Verify unusual requests through a secondary communication channel.
- ✓ Be cautious of urgent financial or confidential requests.
- ✓ Examine videos and audio carefully for inconsistencies.
- ✓ Use multi-factor authentication for sensitive transactions.
- ✓ Educate employees about emerging AI-enabled fraud techniques.
- ✓ Report suspicious content immediately to the security team.



As technology evolves, HKIT Security Solutions remains committed to protecting businesses through excellence, innovation, and cyber resilience.