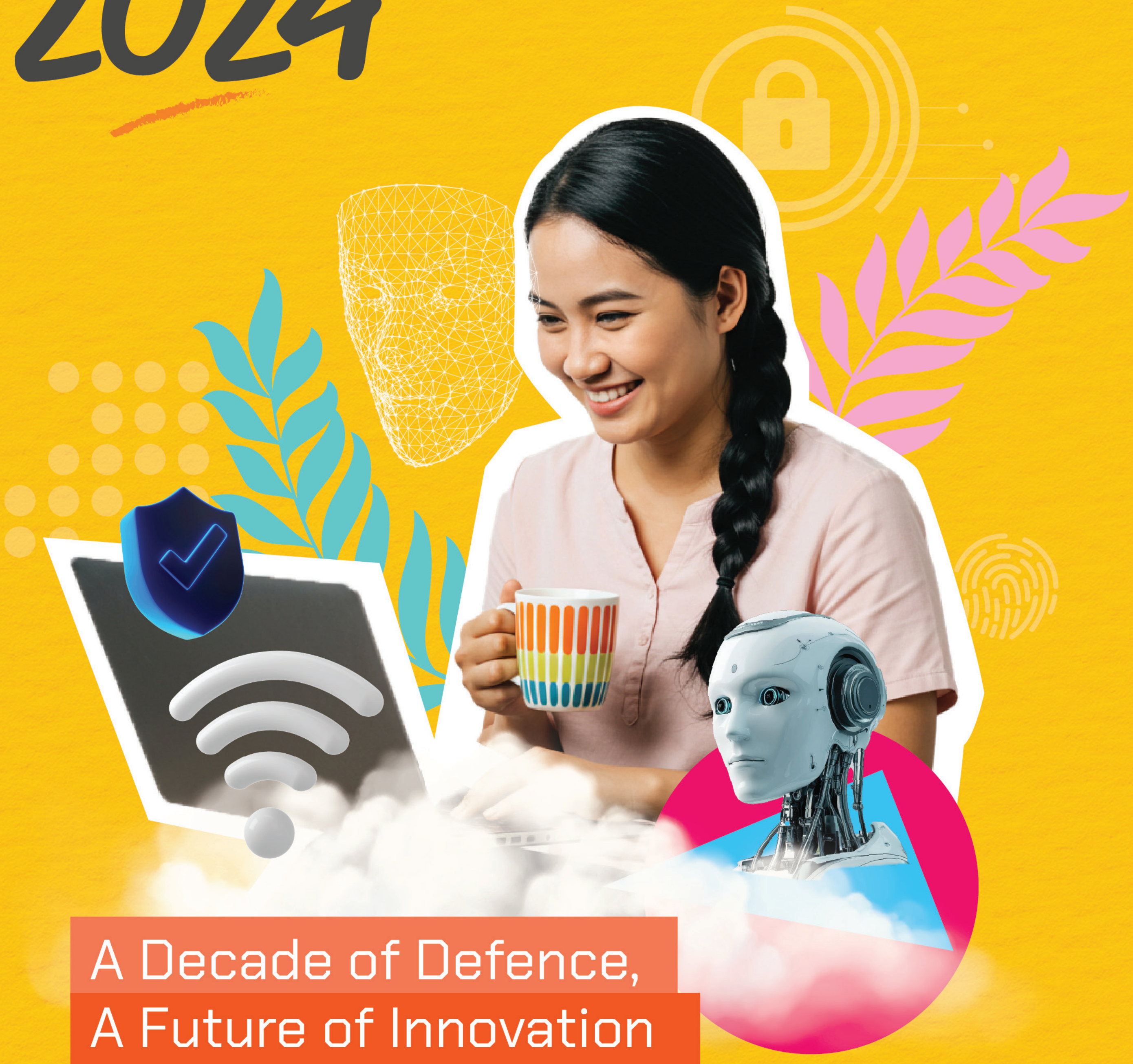
MINISTRY OF DIGITAL

CyberSecurity MALAYSIA

ANNUAL REPORT 2024



A Decade of Defence,
A Future of Innovation

COVER RATIONALE

In line with our commitment to creating a safer digital future, CyberSecurity Malaysia's annual report this year embraces a **youthful, fun, and energetic** concept, reflecting the dynamic spirit of our team and the vibrant, tech-savvy generation we aim to engage. By infusing bold visuals, fresh storytelling, and an approachable tone, we highlight that cybersecurity is not just a technical necessity, but also an exciting frontier of innovation, empowerment, and opportunity.

This concept mirrors our mission to foster awareness and participation among youth, start-ups, and digital natives, while reinforcing the message that staying secure online can be both smart and inspiring.

TABLE OF CONTENT

INTRODUCTION

Design & Cover Rationale........ 02
About CyberSecurity Malaysia........ 05
History........ 07
Our Products & Services........ 08

CORPORATE GOVERNANCE

The Board of Directors........ 19
Corporate Governance........ 20
Notice of Annual General Meeting........ 25
Form of Proxy........ 27

OPERATIONAL REVIEW

Forward from the CEO........ 30
The Management Committee........ 32
Review of Corporate Performance........ 34
2024 Calendar of Activities........ 36
Achievements and Awards 2024........ 40
Professional Certifications........ 41
Editorial Committee........ 46
Social Media........ 47

INTRODUCTION

ABOUT CYBERSECURITY MALAYSIA

CYBERSECURITY MALAYSIA IS THE NATIONAL CYBERSECURITY SPECIALIST AGENCY UNDER THE PURVIEW OF THE MINISTRY OF DIGITAL

With effect from 10 January 2024, CyberSecurity Malaysia is placed under the Ministry of Digital.

CyberSecurity Malaysia is committed to provide a broad range of cybersecurity innovation-led services, programmes, and initiatives to reduce vulnerability of digital systems, and at the same time strengthen Malaysia's self-reliance in cyberspace.

The agency provides the following specialised cybersecurity services:

- Cyber Security Responsive Services
- Cyber Security Proactive Services
- Pre-emptive Technology & Services
- Outreach and Capacity Building
- Strategic Study and Engagement
- Industry and Research Development

HISTORY

AN UNQUENCHABLE FAITH TO ACHIEVE MORE THAN THE MIRACLES OF TECHNOLOGY AND THE PROMISE OF FUTURE ACCOMPLISHMENTS

1997

13 Jan 1997

The journey started with formation of the Malaysia Computer Emergency Response Team or MyCERT (www.mycert.my) as a unit under MIMOS Berhad (www.mimos.my)

2001

10 April 2001

The National ICT Security & Emergency Response Centre (NISER) was established as a Department in MIMOS Berhad, and Malaysia Computer Emergency Response Team (MyCERT) was placed under NISER

2005

28 September 2005

The Cabinet decided for NISER to spun-off from MIMOS Berhad as a company Limited-by-Guarantee under the Ministry of Science, Technology and Innovation (MOSTI)

Our journey started with formation of the Malaysia Computer Emergency Response Team or MyCERT (www.mycert.org.my) on 13 January 1997 as a unit under MIMOS Berhad (www.mimos.my). On 24 January 1998, the National Information Technology Council (NITC) chaired by the Prime Minister of Malaysia proposed for the establishment of an agency to address emerging ICT security issues in Malaysia. As a result, the National ICT Security and Emergency Reponse Center (NISER) was formed in 2001 as a Department in MIMOS Berhad, and MyCERT was placed under NISER.

The Cabinet Meeting on 28 September 2005 through the Joint Cabinet Notes by the Ministry of Finance (MoF) and Ministry of Science, Technology and Innovation (MOSTI) No. H609/2005 agreed to establish NISER (now known as CyberSecurity Malaysia) as a national body to monitor the National e-Security aspect, spun-off from MIMOS Berhad to become a separate agency and incorporated as a Company Limited-by-Guarantee. On 30 March 2007, NISER was registered as a not-for-profit, Company Limited-by-Guarantee under supervision of MOSTI.

The NITC Meeting No. 1/2006 decided to implement the National Cyber Security Policy (NSCP) led by MOSTI. NISER was mandated to provide technical support for NCSP implementation and was rebranded to CyberSecurity Malaysia reflecting its wider mandate and larger role. On 20 August 2007, the Prime Minister of Malaysia officiated CyberSecurity Malaysia and launched its new logo.

2007

30 March 2007

NISER was officially registered as CyberSecurity Malaysia

20 August 2007

CyberSecurity Malaysia was officially launched by the Prime Minister of Malaysia

2018

19 October 2018

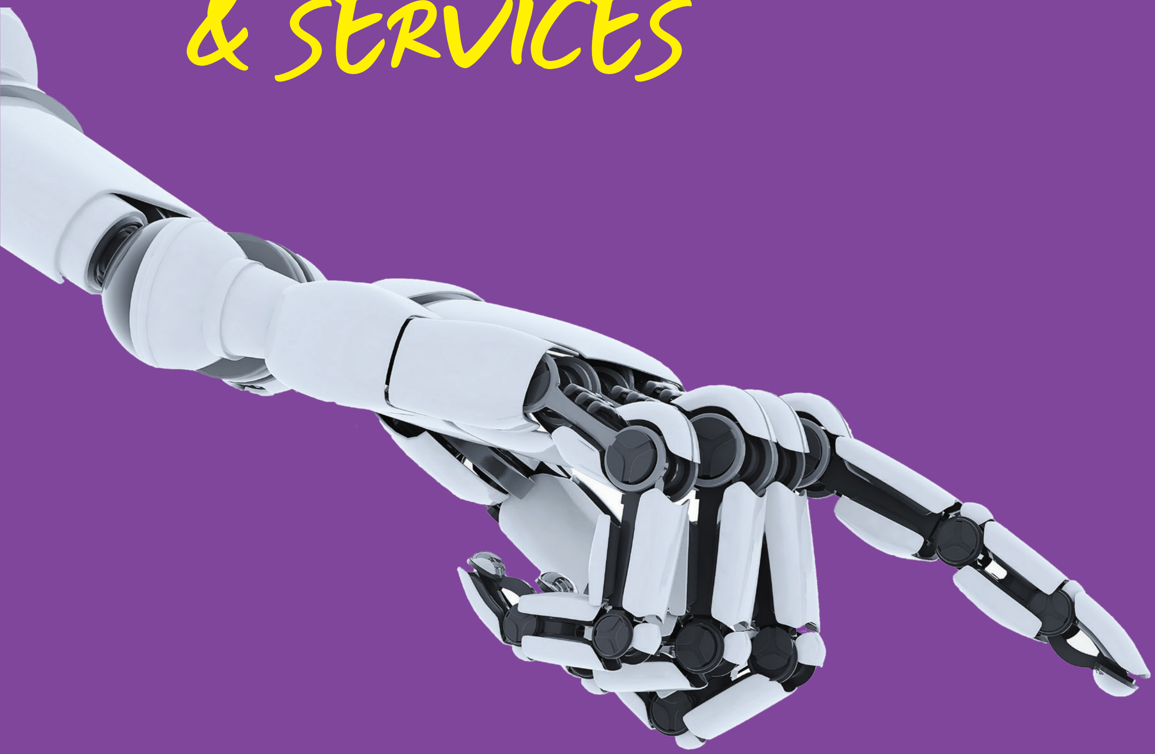
The Cabinet Meeting chaired by the Prime Minister of Malaysia decided CyberSecurity Malaysia to be placed under the Ministry of Communication and Multimedia Malaysia (KKMM)

2024

10 January 2024

The Cabinet Meeting chaired by the Prime Minister of Malaysia decided that CyberSecurity Malaysia to be placed under the Ministry of Digital

OUR PRODUCTS & SERVICES



With the vision to become a world-class cybersecurity specialist agency, our mission is to lead the development of a safer and more resilient cyber ecosystem to enhance national security, economic prosperity, and social harmony through:

- Provision of quality and impactful services
- Frontier-expanding cyber knowledge and technical supremacy
- Continuous nurturing of talent and expertise

CyberSecurity Malaysia pursues this mission through SiberKASA, a comprehensive framework that develops cybersecurity solutions by virtue of the three elements of People, Process, and Technology.

The SiberKASA framework is developed based on our six core services:

- Cybersecurity Responsive Services
- Cybersecurity Proactive Services
- Pre-emptive Technology & Services
- Outreach and Capacity Building
- Strategic Study and Engagement
- Industry and Research Development

The following is a distilled overview of our six core services and some examples of the services and products that are offered.

Cybersecurity Responsive Services

Compromise Assessment - Host Assessment

A focused security evaluation conducted on individual computing systems (hosts) within a network. These hosts can include servers, workstations, laptops, or any other network-connected devices with an operating system. The assessment aims to identify security vulnerabilities and misconfigurations specific to each machine.

Compromise Assessment: Cyber Health Assessment (Network Compromise Assessment)

Cyber Health Assessment (CHA) is conducted using CMERP Insight (INSIGHT), a Breach Detection System (BDS) designed to detect malicious and suspicious activities within a network following a security breach. INSIGHT serves as a monitoring solution that alerts organisations to potential threats, enabling timely responses to harmful activities.

CSIRT Consultancy

Computer Security Incident Response Team (CSIRT) Consultancy offers specialised expert services to organisations in the areas of people, processes, and technology. This consultancy creates tailored implementation plans to help develop and establish a CSIRT within organisations. Additionally, the service provides Incident Handling and Network Security training, job attachments, and professional memberships with the Forum of Incident Response and Security Teams (FIRST), Asia Pacific Computer Emergency Response Team (APCERT), and the Organisation of The Islamic Cooperation – Computer Emergency Response Teams (OICCERT) OIC-CERT.

Cyber Incident Response Plan Consultancy

Consultancy service to help organisations build or enhance their cyber incident response plan and strategy.

2nd and 3rd Level Incident Response Support

Deep-dive technical support for complex or escalated incidents.

System and Network Log Analysis

Analysis of system/network logs to detect anomalies and the root cause of incidents.

CyberDEF (Defense, Eradication & Forensics)

To assist organisation by providing solution, proactive and responsive steps to eradicate and remediate security threats and vulnerabilities (Root Cause Analysis).

Expert Development & Consultation

Digital Forensics Quality Management System Expert Consultation

CyberDISCOVERY **is a specialised cyber forensics service** offered to both individuals and private organisations. It is designed to address concerns related to Electronically Stored Information (ESI) as digital evidence, particularly within the context of civil litigation. The service focuses on uncovering critical information and provide clear, defensible answers to support legal proceedings.

CyberDiscovery offers the following services:

1. **Onsite Evidence Collection and Preservation** Secure acquisition and safeguarding of digital evidence from electronic devices and storage media, ensuring chain-of-custody compliance.

2. **Evidence Examination and Analysis** In-depth forensic analysis of collected data to identify, interpret, and reconstruct relevant digital activities.

3. **Expert Witness Testimony** Provision of qualified forensic experts to present findings and opinions in court, supporting legal arguments with professional credibility.

CyberDiscovery upholds the highest standards of integrity, confidentiality, and forensic best practices, delivering reliable and court-admissible results.

Cybersecurity Proactive Services

ISMS Guidance Series **Information Security Management Consulting** provides expert guidance to organisations in protecting and preserving the confidentiality, integrity, and availability of their information and information systems through the implementation of an Information Security Management System (ISMS) in accordance with the ISO/IEC 27001 standard.

Customised Information Security Management Services

Tailored Information Security Management related services designed to address ISO/IEC 27001 requirements e.g., determination of ISMS scope, risk assessment, implementation of controls and general information security assessment.

DPMA – Data Privacy Management Assessment

A web-based assessment tool that helps organisations assess their data privacy governance, readiness, and compliance, and identify implementation gaps, based on the ISO/IEC 27701 Privacy Information Management System (PIMS).

DPGP - Data Privacy Guard Pro **is an evaluation and testing for ICT / IoT product** or application, based on data protection requirements outlined in Malaysia's Personal Data Protection Act (PDPA) and international best practices. It also aligned with relevant ISO data privacy standards. DPGP evaluates how a product manages personally identifiable information (PII) throughout its lifecycle, including the functional roles involved, to guarantee strong privacy protection for the product.

DPIA- Data -Protection Impact Assessment **assists organisations access the potential impacts on privacy** of processes, information systems, programmes, software modules, devices, or other initiatives that handle Personally Identifiable Information (PII). It also identifies necessary actions in order to treat privacy risk. The DPIA is developed based on ISO/IEC 29134 Guidelines for Privacy Impact Assessment.

PJuRA – Privacy Jurisdiction Risk Assessment **helps organisations assess their data protection practices** against both local and international privacy laws. This structured assessment identifies risk exposure across different legal jurisdictions and highlighting potential compliance gaps. By understanding these risks, organizations can strengthen their data protection measures and build greater customer trust by demonstrating their commitment to data security and privacy.

MyKripto Validation

A security validation and analysis service that includes:

- Cryptanalysis of cryptographic algorithms to assess their security strength.
- Conformance testing of cryptographic algorithms against a standard document.
- Evaluation of the randomness characteristics of a random number generator.
- Cryptographic S-Box Testing checks the strength of encryption's core to ensure they resist codebreaking.

Malaysia's National Trusted Cryptographic Algorithm List (MySEAL)

MySEAL establishes requirements and guidelines for trusted cryptography products in Malaysia, aligning with the National Cryptography Policy to achieve cryptographic sovereignty and support cryptographic science; it provides a list categorising algorithms into AKSA (Existing Cryptographic Algorithms) and AKBA (New Cryptographic Algorithms), with comprehensive evaluation criteria overseen by a committee led by CyberSecurity Malaysia, marking a significant milestone since Malaysia's National IT Agenda in pursuing information security fundamentals.

Blockchain Security Verification

A service that validates and verifies the security properties of a blockchain and smart contract applications. With this, businesses gain insight into their overall blockchain and smart contract security posture, as well as the ability to address any potential flaws in their blockchainbased solutions or applications.

FIPS 140-3 Cryptographic Module Validation

CyberSecurity Malaysia operates a Federal Information Processing Standard (FIPS) Publication 140 testing laboratory that provides independent technical services in the field of cryptographic algorithm testing and verification testing of cryptographic module software and hardware.

FIPS 140-3 Cryptographic Training

Gain a competitive edge with our FIPS 140-3 Cryptographic Training, designed to provide in-depth knowledge of cryptographic module validation in alignment with ISO/IEC 19790 and ISO/IEC 24759 standards.

Cybersecurity Evaluation and Testing of ICT products and Protection Profiles (PP) using the Common Criteria Methodology (based on ISO/IEC 15408 and ISO/IEC 18045) for certification under the MyCC scheme.

ICT Product Security Assessment (IPSA) is a security functional testing and/or vulnerability assessment and penetration testing service for ICT products.

Cloud Security Evaluation

Evaluation and testing of products developed and operated on cloud computing platforms, managed by Cloud Service Providers (CSP) for Platform as a Service (PaaS) and Software as a Service (SaaS).

Expert Consultancy

We provide expert consultancy services for the development of ISO/IEC 17025 laboratories to offer Common Criteria evaluation services.

Cloud Security Audit

Cloud security audit services for cloud computing platforms, managed by Cloud Service Providers (CSP) for Platform as a Service (PaaS) and Software as a Service (SaaS), based on the security requirements stated in ISO/IEC 27017 and ISO/IEC 27002.

Facility Rental

Rental of ISO 17025 Accredited testing facilities, equipment and resource to the public and private organisations to conduct cybersecurity evaluations or testing in a controlled environment.

CyberSOC **Provides Manage, Detect & Response (MDR) services** that monitor, analyse, detect, and protect against potential cyberattacks. The service covers endpoints such as servers, workstations and laptops.

Lebahnet

Lebahnet, based on Honeypot technology, provides valuable insights into network trends and malicious activities, supporting MyCERT in incident handling and advisory services. Honeypots are systems designed to simulate legitimate sites, luring malicious software by appearing vulnerable. This approach allows cybersecurity researchers to detect, monitor, and counteract malicious activities by analysing actions during the intrusion phase and examining attack payloads.

Cyber Drill Exercise

CyberDrill is an activity conducted to assess an organisation's cyber capacity by evaluating its ability to detect and respond to security incidents. This follows a defined methodology and is executed using various tools and infrastructure provided by CyberSecurity Malaysia. During the simulated cyber drill exercise, organisation's readiness is tested based on their existing cyber security incident response procedures, allowing for the identification of areas for improvement.

Incident Response Playbook Development

Creation of tailored response procedures for various incident types.

Vulnerability Assessment and Penetration Testing (VAPT)

Vulnerability Assessment and Penetration Testing (VAPT) is a critical service provided to both public and private organisations to identify and address security weaknesses within their IT environment. This comprehensive service involves a detailed assessment of the system to uncover vulnerabilities and potential entry points that could be exploited by cyber threats.

Security Posture Assessment (SPA) **identifies security vulnerabilities within an organisation** based on internationally recognised standards, including the Open Worldwide Application Security Project (OWASP), Open Worldwide Application Security Project (OSSTMM), and PCI Security Standards Council (PCI-DSS) to help prevent breaches, reduce the impact of any incidents, and protect organisational reputation.

Mobile App Security Assessment

Identifies security weaknesses in mobile applications, devices, and operating systems and evaluates risks such as data leaks, insecure Application Programming Interface (APIs), weak authentication, and malware.

Technology Security Assurance (TSA) **is a national scheme** initiated by CyberSecurity Malaysia. It is an assurance where ICT products are evaluated based on Mandatory Security Functional Requirements (MSFRs) developed by the Information Security Certification Body (ISCB).

MyCC Certification

MyCC Scheme assists in raising the quality and competitiveness level of Malaysian ICT products, benchmarked against global Common Criteria requirements.

Business Continuity Management System (BCMS) Certification

The scheme is based on the ISO 22301 international standard for organisation that envisions for resiliency. It helps to plan an effective business continuity management to protect against, reduce the likelihood of, and ensure business recovers from disruptive incidents. This is in line with the national requirement towards creating a resilient National Critical Information Infrastructure (NCII).

Penetration Test Service Provider Scheme (PTSP)

PTSP ensures penetration testing service is delivered by local cyber security consulting companies that are meeting the requirement set by CyberSecurity Malaysia

Malaysian Cryptography Validation (MyCV) Scheme

MyCV is a national scheme for validating and certifying the Cryptographic Module Validation (CMV) and the Cryptographic Algorithm Validation (CAV) services based on ISO/IEC 19790 and ISO/IEC 24759 standard and also to supports Dasar Kriptografi Nagara (DKN) or National Cryptoraphy Policy (NCP) (NCP) implementation.

Mobile Application Certification (MAC)

Mobile application assessment to ensure mobile applications meet the established required cybersecurity criteria.

Information Security Privacy Management System (ISPMS)

ISO/IEC 27701:2019 is a privacy extension to ISO/IEC 27001. The goal is to enhance the existing Information Security Management System with additional requirements in order to establish, implement, maintain, and continually improve a Privacy Information Management System. The standard outlines a framework for Personally Identifiable Information Controllers and PII Processors to manage privacy controls to reduce the risk to the privacy rights of individuals. ISO/IEC 27701 is intended to be a certifiable extension to ISO/IEC 27001 certifications.

ISMS Certification

The CSM27001 Scheme supports the National Security and Public Safety pillar under the Economic Transformation Programme (ETP) by enhancing the resilience of both the National Critical Information Infrastructure (NCII) and the broader industry. Additionally, the scheme contributes to the Catalyst for Industry Growth pillar by enabling ISO/IEC 27001-certified organisations to benchmark themselves against global standards, thereby enhancing their competitiveness in the international market.

Pre-emptive Technology & Services

Offensive Security Surface Risk Intelligence

Evaluates exposed assets of an organisation, including networks, systems, and applications, to identify and prioritise vulnerabilities that could be exploited by attackers. This proactive approach helps mitigate risks by addressing weaknesses before they are exploited.

Offensive Intelligence - Digital Exposure Monitoring

Continuously tracks online footprint of an organisation, including publicly accessible systems, leaked data, and potential vulnerabilities, to understand how adversaries might target them. It enables organizations to stay ahead of threats by monitoring and mitigating exposures in real-time.

SiberBlok / Automated Threat Prevention

Detects, analyses, and responds to cybersecurity threats in real-time by monitoring network traffic for malicious activities. It quickly blocks or mitigates threats, reducing response time, minimizing human error, and strengthening overall security resilience.

Offensive Security - Vulnerabilities Exploitation Analysis

Identify vulnerabilities and test their exploitability to assess potential impact of an attack. This analysis provides actionable insights to address weaknesses and strengthen overall security posture.

Behavioural Competency Assessment (BCA) **for information security personnel** is an instrument that assess the behavioural elements that contribute to a culture of high performance, which can be observed through people's actions and behaviours. Utilising psychometric science and methods, BCA can effectively complement

Outreach & Capacity Building

CyberSAFE®

CyberSAFE® (Cyber Safety Awareness for Everyone) is a public awareness programme developed by CyberSecurity Malaysia to educate and empower the general public on the importance of cybersecurity and to promote a safer digital environment for all.

CyberGURU

CyberGURU is a dedicated platform for nurturing information security practitioners and advancing cyber security professional development through a wide range of competencybased training programmes and certifications. The platform also promotes knowledge sharing by engaging leading industry experts, academicians, and policymakers, while fostering both local and international collaborations.

CyberGURU offers a diverse portfolio of competency and professional certification courses tailored to meet the evolving demands of the cyber security landscape. These include training tracks ranging from fundamentals to advanced certifications in areas such as Incident Handling, Digital Forensics, Security Assessment, Cryptography, Common Criteria, and Security Management.

Global ACE Certification

A national certification scheme designed to strengthen Malaysia's cyber security capacity and capability by recognising and certifying qualified personnel. The framework is aligned with international standards, including ISO/IEC 17024 for personnel certification, ISO/IEC 9000 for quality management processes, and ISO/ IEC 27001 for information security management.

Strategic Study & Engagement

Strategic Study

Strategic study provides:

- Strategic advice
- Feedback to stakeholders
- Collaborations with relevant local and international parties
- Implementation of cyber security technologies

Government Engagement

Government Engagement provides:

- Strategic engagement services with stakeholders within the Malaysian Government.
- Administrator for the Critical National Information Infrastructure (CNII) portal.

International Engagement

International Engagement provides:

- Multilateral relations service to enhance cyber security corporation globally
- To establish and support cross border collaboration, bilateral and multilateral platforms in the effort to achieve a safe and secured cyber space.
- Corporation globally among the Computer Emergency Response Teams (CERTs), World Trustmark Alliance (WTA) and other information security organizations

Industry & Research Development

CyberSecurity Malaysia Collaboration Program (CSM-CP) is a strategic initiative designed to foster collaboration between CyberSecurity Malaysia and the local cyber security industry, as well as other government entities. The programme aims to encourage the development and innovation of Malaysia's cyber security products and services. Through CSM-CP, participants gain access to potential collaborations and synergies not only with CyberSecurity Malaysia, but also with relevant government agencies and fellow collaborators. The programme leverages partners' strengths and helps bridge market gaps by supporting the creation of high-quality, locally relevant cyber security solutions.

MyCyberSecurity Clinic (MyCSC)- Data Recovery and Data Sanitization Services offers trustworthy and convenient data recovery and data sanitization services, ensuring that all data is handled in a safe, secure, and confidential manner.

- **Data Recovery Services**: Designed to retrieve data from digital storage media that are damaged, failed, corrupted, or otherwise inaccessible. Our expert team uses advanced techniques to maximise the chances of successful recovery while maintaining data integrity.

- **Data Sanitization Services:**
  Provide organisations with a reliable solution for the secure and permanent deletion of data from storage devices that are being retired, upgraded, or repurposed. This helps prevent data leakage and ensures compliance with data protection policies.

Our services are aligned with industry best practices to support your organisation's data lifecycle management needs with confidence and peace of mind.

CORPORATE GOVERNANCE

BOARD OF DIRECTORS

The Board of Directors of CyberSecurity Malaysia helps lead the organisation by providing guidance and making key decisions. Their leadership has played an important role in keeping the agency focused on its mission to protect Malaysia's digital space and ensure a safer online environment for everyone.

Al-Ishsal Bin Prof. Dato' Ishak T. Kechik
Chairman

Tuan Fabian Bigar
Director / Secretary General,
Ministry of Digital

Dato' Ts. Dr. Haji Amirudin Bin Abdul Wahab FASc.
Director / Chief Executive Officer

Shaifubahrim Bin Mohd Saleh
Director

Dato' Dr. Suhazimah Binti Dzazali
Director

Datuk Ts. Dr. Fazidah Binti Abu Bakar
Director

Derek John Fernandez
Director

Norhayati Binti Masah
Director

CORPORATE GOVERNANCE

THE BOARD OF DIRECTORS OF CYBERSECURITY MALAYSIA IS PLEASED TO REPORT THAT FOR THE FINANCIAL YEAR UNDER REVIEW, CYBERSECURITY MALAYSIA HAS CONTINUED TO APPLY GOOD CORPORATE GOVERNANCE PRACTICES IN MANAGING AND DIRECTING THE AFFAIRS OF CYBERSECURITY MALAYSIA, BY ADOPTING THE SUBSTANCE AND SPIRIT OF THE PRINCIPLES ADVOCATED BY THE MALAYSIAN CODE ON CORPORATE GOVERNANCE ("THE CODE").

Board Responsibilities

The board maps out and reviews CyberSecurity Malaysia's strategic plans on an annual basis to ensure CyberSecurity Malaysia's operational directions and activities are aligned with the goals of its establishment by the government of Malaysia. The board considers in depth, and if thought fit, approves for implementation key matters affecting CyberSecurity Malaysia which include matters on action plans, annual budget, major expenditures, acquisition and disposal of assets, human resources policies and performance management. The board also reviews the action plans that are implemented by the management to achieve business and operational targets. The board also oversees the operations and business of CyberSecurity Malaysia by requiring regular periodic operational and financial reporting by the management, in addition to prescribing minimum standards and establishing policies on the management of operational risks and other key areas of CyberSecurity Malaysia's activities.

The board's other main duties include regular oversight of CyberSecurity Malaysia's operations and performance as well as ensuring that the infrastructure, internal controls and risk management processes are well in place.

The following Board Committees, which were set up, have also fulfilled their specific responsibilities.

The Human Resources and Remuneration Committees (HRRC)

Objectives:

- Develop and periodically review the overall remuneration policy and human resource strategies of CyberSecurity Malaysia to ensure that it is contributing effectively to the success of the company.
- Ensure the integrity of the remuneration policies and human resource practices and their effectiveness and compliance within the Company.

Duties:

Performance-based remuneration for CyberSecurity Malaysia's Chief Executive Officer (CEO).

- To review and recommend to the board a performance-based remuneration for the CEO, or the person performing the duties and assuming the responsibilities of the CEO, by reference to the corporate goals and objectives as resolved by the board from time to time.

The company's human resource matters including:

- To review the overall market positioning of the Company's remuneration package and policies, on an annual basis, with a view to retain and/or attract high caliber staff and thereafter submit an appropriate recommendation for the Board's consideration and approval.
- To review the Company's Human Resources development programmes and policies related to the remunerations and ensure compliance with the applicable laws and regulations of the country.
- To review the rewards and remunerations of the company staff as to demonstrate that rewards and remunerations are considered by a committee which has no personal interest in the outcome of its advice and which give due regards to the interest of the Company and its financial health.
- To undertake, consider and act on other human resource related issues or tasks as the committee consider appropriate or as may be referred to by the Board.
- To periodically review and participate in determining the organizational structure for the Company.
- To review potential candidates for hiring and promotion for the Top Management positions of the Company.

Members:

- YBhg. Tuan Fabian Bigar (Chairman)
- YBrs. Encik Shaifubahrim bin Mohd Saleh (Member)
- YBhg. Dato' Dr. Suhazimah binti Dzazali (Member)

Size and Composition:

- The HRRC shall consist of not less than three (3) directors from the board members. They are appointed by the CyberSecurity Malaysia's board of directors.
- The duration of HRRC membership shall be the same as appointment of the members for Board. The re-election of current members or appointment of new member shall be made by the Board after the expiring of the existing term.
- The board may from time to time appoint additional members to the HRRC from among its members and such other persons as the board deems fit.
- The HRRC may invite any director, member of the company's i.e. management or other person to attend its meeting(s) from time to time when it is considered desirable to assist the HRRC in attaining its objectives.

Meetings:

- The HRRC shall have meetings at least twice a year. Additional meetings may be conducted at any time with the consensus from all members of the committee.
- All decisions of the HRRC shall be by majority vote. In the event of a tie, the chairperson shall have the second or casting vote in addition to his or her original vote.
- The quorum for HRRC meeting shall be two (2) members of the appointed members.
- The Head of Human Capital Department ("HCD") is the secretary for this committee. In the absence of the Head of HCD, a representative from HCD shall replace the Head of HCD in carrying out the secretariat function.

Audit, Governance and Integrity Committee (AGI)

Duties:

Audit

- Ensure scheduled audits and planning of audit plans are undertaken by the department in charge of audit, governance and integrity as a control and monitoring measure on the financial and operational management of the company.
- Follow-up the audit issues raised in the *Laporan Ketua Audit Negara* (LKAN) or weaknesses highlighted by the *Jabatan Audit Negara* by ensuring that the management is performing immediate actions and corrective actions on the issues as well as establishing and monitoring the compliance of the expected completed dates and timeline of corrective actions.
- If the audit issue raised is brought to the attention of the Putrajaya Inquisition or *Jawatankuasa Kira-kira Wang Awam* (Public Accounts Committee), the AGI chairman is responsible to be present with the management to explain.
- Reviewing the requirements of the department in charge of audit, governance and integrity including its charter.
- The AGI Committee shall submit reports at Board meetings at least twice a year or at the frequency to be decided by the Committee or requested by the Board. If no audit observation is received, the AGI Committee shall report so at the Board meetings.
- To review the Company's final statements of accounts prior to submission to the Board, to ensure compliance with disclosure requirements and adjustments suggested by the auditors.
- To review the internal controls, performance and findings of the internal auditors and to recommend and implement appropriate remedial and corrective actions.
- To recommend to the Board the appointment of external auditors of the Company, the audit fee and any matter of resignation or dismissal.
- To discuss any matters arising from the previous year's audit, to review the scope of the current year's audit, the plans for carrying out the audit, the extent of planned reliance on the work of other independent auditors and the Company's own internal auditors.
- To review any significant audit problems that can be foreseen either as a result of the previous years' experience or because of new developments.
- To evaluate and review the role of the internal and external auditors from time to time.
- To review any significant related party transactions that may arise within the Company.
- To review any significant transactions which are not a normal part of the ordinary business of the Company.
- To place the internal auditors under the direct authority and supervision of the AGI Committee and to evaluate and approve their performance and remuneration package. Key Performance Indicator of the department in charge of the audit, governance and integrity to be evaluated by the Committee and Chief Executive Officer.
- To recommend changes in the accounting policies to the Board of Directors.
- To review the assistance given by the Company's officers to the auditors.
- To carry out such other responsibilities as may be delegated by the Board of Directors from time to time.

Governance and Integrity

A. Policy

- To review and recommend amendments to any policy so as to overcome weaknesses in management, improve controls against corruption, malpractices, abuse of powers and administrative weaknesses.
- To evaluate and review strategic plans for enhancing the best governance practices, which are capable of achieving delivery system that is infused with integrity, accountability, trust, fairness, monitoring and stewardship, transparent and responsive to clients.

B. Systems and Work Procedures

To evaluate and review systems and work procedures:

- That are giving rise to various bureaucratic red-tapes, which could possibly weaken administration, reduce efficiency, non-accountability at the same time giving rise to avenues for bureaucratic hassles, delays, injustices and indiscriminate (usage of) discretion as well as providing opportunities for corruption, malpractices and abuse of powers.
- That are transparent and with accountability, optimisation of resources and information management system that is efficient and effective to achieve Company's missions and visions or objectives.

C. Noble Values and Code of Ethics

- To review activities that enhances integrity of staffs including consolidation and implementation of policies and procedures that are infused with noble values and code of ethics so as to prevent staff from committing all forms of negative conduct inclusive of corruption, malpractices, and abuse of powers.

- To review and validate organizational code of ethics.

D. Customer Management

To review the strategic and quality system of customer management in order to portray efficiency, sensitiveness, friendliness and responsiveness towards the needs of clients (be they stakeholders, internal or external clients) and be perceived as providing value-added and continuously improved delivery system, as well as to prevent being seen as slip-ups in the fulfillment of entrusted duties and responsibilities.

E. Detection, Punitive and Rehabilitation Action
To evaluate and review any matters primarily significant problems resulting from contravention of laws, regulations, system and work procedures or code of ethics including any form of offences or crime committed by staff.

F. Recognition and Appreciation
To evaluate and review the recognition and appreciation to staff who have shown exemplary services and exhibiting noble values through voluntary activities by giving religious advice and guidance and those who have reported cases of corruption, malpractices and misconduct within divisions/departments.

G. Ensure the direction of the company is clear with the goals and initiatives implemented by the department in charge of audit, governance and integrity, the Board plays a major role in shaping the climate and the tone of the company whether it is to put integrity on the right track or vice versa.

H. Ensure that the structure of the department in charge of audit, governance and integrity is separate and directly report to the Board to avoid any pressure, escalation, rejection and improper act on the part of the company.

I. Ensure the department in charge of audit, governance and integrity performs the core defined functionality of the department.

J. Provide instructions to the department in charge of audit, governance and integrity to ensure this department remains relevant as an entity responsible for the preservation of integrity in the company.

Members:

- YBhg. Dato’ Shuhairi bin Abd Ghani (Chairman of AGI1/2024 on 23 February 2024)
- YBhg. Datuk Ts. Dr. Fazidah binti Abu Bakar
- Note: Chaired AGI2/2024 on 1 August 2024 and AGI3/2024 on 22 November 2024 after the retirement of YBhg. Dato’ Shuhairi bin Abd Ghani on 22 April 2024.
- YBrs. Encik Shaifubahrim bin Mohd Saleh

Terms of reference of the AGI

Authority

- Authorised by the Board to investigate any activity within its terms of reference and all employees shall be directed to co-operate as requested by the Committee.
- Have unlimited access to all information and documents relevant to its activities, to the internal and external auditors and senior management of the Company.
- Authorised by the Board to obtain outside legal or other independent professional advice and to secure the attendance of outsiders with relevant experience and expertise as it considers necessary.

Size and composition

- The committee shall consist of at least three (3) but not more than five (5) members of whom the majority shall be independent non-executive Directors of CyberSecurity Malaysia.
- The members of the audit committee shall select a chairman from among them who is not an executive director or employee of the Company or any related organization. The chairman of the Committee may also be appointed by the Board executive director or employee of the Company or any related organisation. The chairman of the Committee may also be appointed by the Board.

Meetings

- Meetings of the committee shall be held at least two (2) times a year or at a frequency to be decided by the committee and the committee may invite any person to be in attendance at such meetings.
- The quorum for meetings shall be two (2).
- Meetings may be convened upon request of the auditors of the Company to consider any matter that the auditors believe should be brought to the attention of the directors.
- The Head of department in charge of audit, governance and integrity shall be the secretary for Audit, Governance and Integrity Committee.

COMPOSITION AND BALANCE

The board consists of members of high calibre, with good leadership skills and vastly experienced in their own fields of expertise, which enable them to provide strong support in discharging their duties and responsibilities. They fulfill their role by exercising independent judgment and objective participations in the deliberations of the board, bearing in mind the interests of stakeholders, employees, customers, and the communities in which CyberSecurity Malaysia conducts its business.

The ratio between Government Directors and other Directors appointed or to be appointed to the Board of CyberSecurity Malaysia may be determined by the Supervising Ministry; and the appointment of any person as a Director shall first be consented to by the Supervising Ministry. All selected members of the board must obtain the prior approval from the Minister of Domestic Trade and Consumer Affairs (MDTCA). Currently, there are seven (7) members of the Board of CyberSecurity Malaysia.

The board is fully and effectively assisted in the day- to-day management of CyberSecurity Malaysia by the Chief Executive Officer (CEO) and his management team. The profiles of the current members of the boards are set out on pages of the annual report.

SUPPLY OF INFORMATION TO THE BOARD

Board meetings are held regularly, whereby reports on the progress of CyberSecurity Malaysia's business and operations and minutes of meetings of the board are tabled for review by the members of the board. At these board meetings, the members of the board also evaluate businesses and operational propositions and corporate proposals that require board's approval.

The agenda for every board meeting, together with comprehensive management reports, proposal papers and supporting documents, are furnished to all directors for their perusal, so that the directors have ample time to review matters to be deliberated at the board's meeting and at the same time to facilitate decision making by the directors.

DIRECTORS' TRAINING

Directors are encouraged to attend talks, training programmes and seminars to update themselves on new developments in relation to the industry in which CyberSecurity Malaysia is operating.

ANNUAL GENERAL MEETING (AGM)

The annual general meeting represents the principal forum for dialogue and interaction with members of CyberSecurity Malaysia namely the Ministry of Finance (Inc.) ("MOF (Inc.)") and the Supervising Ministry. Members are given an opportunity to raise questions on any items on the agenda of the general meeting. The notice of meeting and annual report is sent out to the members of CyberSecurity Malaysia at least 21 days before the date of the meeting which is in accordance with the Constitution of CyberSecurity Malaysia.

NOTICE OF ANNUAL GENERAL MEETING

NOTIS MESYUARAT AGUNG TAHUNAN KE-19

DENGAN INI DIMAKLUMKAN BAHAWA Mesyuarat Agung Tahunan (“AGM”) ke-19 CyberSecurity Malaysia akan diadakan secara maya melalui penstriman langsung dari lokasi siaran di **CyberSecurity Malaysia, Bilik Jati, Level 10, Menara Cyber Axis, Jalan Impact, 63000 Cyberjaya, Selangor** pada hari **Rabu, 25 Jun 2025 pada jam 11.00 pag**i untuk membincangkan urusan-urusan berikut:

Urusan Biasa

1. Untuk menerima Penyata Kewangan Beraudit bagi tahun kewangan berakhir 31 Disember 2024 berserta laporan Pengarah dan Juruaudit yang berkaitan dengannya.

   (Rujuk nota keterangan 1)

2. Untuk meluluskan pembayaran elaun bulanan Pengerusi bukan Eksekutif dan Pengarah bukan Eksekutif berjumlah sehingga RM240,000 dan manfaat lain bermula dari tarikh AGM ke-19 sehingga AGM CyberSecurity Malaysia bagi yang berikutnya. **Resolusi 1**

   (Rujuk nota keterangan 2)

3. Untuk melantik semula Pengarah-pengarah berikut yang akan bersara mengikut giliran menurut Artikel 54 Perlembagaan CyberSecurity Malaysia, dan oleh kerana layak, menawarkan diri mereka untuk dilantik semula; **Resolusi 2**
   3.1 YBhg. Tuan Al-Ishsal bin Ishak;
   3.2 YBrs. Encik Derek John Fernandez; dan
   3.3 YBrs. Puan Norhayati binti Masah.

   (Rujuk nota keterangan 3)

NOTIS MESYUARAT AGUNG TAHUNAN KE-19

Resolusi 3

4. Untuk melantik Tetuan Atarek Kamil Ibrahim & Co. sebagai Juruaudit CyberSecurity Malaysia bagi tahun kewangan berakhir 31 Disember 2025 dan memberi kuasa kepada Lembaga Pengarah untuk menetapkan imbuhan mereka.

   (Rujuk nota keterangan 4)

5. Untuk melaksanakan apa-apa urusan lain yang mana notis sewajarnya telah diberikan mengikut Akta Syarikat 2016 dan Perlembagaan CyberSecurity Malaysia.

MENURUT PERINTAH LEMBAGA PENGARAH

JAILANY BIN JAAFAR
LS0008843
SSM PC No. 201908002687
Setiausaha Syarikat

Selangor Darul Ehsan
Tarikh: 3 Jun 2025

A. Nota

1. Anggota syarikat yang berhak untuk hadir dan mengundi di Mesyuarat Agung Tahunan ("AGM") adalah berhak untuk melantik proksi untuk hadir dan mengundi sebagai pengganti beliau. Seorang proksi tidak perlu menjadi anggota syarikat. Tiada sekatan mengenai kelayakan proksi. Proksi yang dilantik untuk hadir dan mengundi pada AGM akan mempunyai hak yang sama seperti anggota syarikat untuk bersuara di AGM.

2. Sebagai pengganti kepada pelantikan proksi, anggota korporat boleh melantik wakil korporatnya untuk menghadiri mesyuarat itu menurut Seksyen 333 Akta Syarikat 2016 ("Akta"). Untuk tujuan ini dan menurut Seksyen 333(5) Akta, anggota korporat hendaklah menyediakan perakuan/sijil di bawah meterai perbadanannya sebagai bukti prima facie mengenai pelantikan wakil korporat.

3. Suratcara pelantikan proksi bagi individu mestilah ditandatangani oleh pelantik atau wakil yang diberi kuasa sewajarnya secara bertulis atau, bagi sebuah perbadanan, suratcara pelantikan proksi atau proksi-proksi hendaklah di bawah meterai atau ditandatangani oleh pegawai atau wakil yang diberi kuasa sewajarnya.

4. Suratcara pelantikan proksi atau perakuan/sijil wakil korporat mestilah didepositkan di Pejabat Pendaftar CyberSecurity Malaysia, Level 7 Tower 1, Menara Cyber Axis, Jalan Impact, 63000 Cyberjaya, Selangor, Malaysia tidak kurang daripada 48 jam sebelum masa yang ditetapkan untuk mengadakan AGM atau pada mana-mana penangguhannya.

B. Nota Penerangan

1. **Penyata Kewangan Beraudit bagi tahun kewangan berakhir 31 Disember 2024**
   Perkara ini bertujuan untuk perbincangan sahaja. Peruntukan Seksyen 340(1) Akta Syarikat 2016 memerlukan Penyata Kewangan Beraudit dan Laporan Lembaga Pengarah dan Juruaudit mengenainya dibentangkan di AGM. Oleh itu, perkara ini bukanlah urusan yang memerlukan resolusi untuk diundi oleh Anggota syarikat.

2. **Bayaran elaun bulanan**
   Bayaran elaun bulanan Pengerusi bukan Eksekutif dan Pengarah bukan Eksekutif berjumlah sehingga RM240,000 dan manfaat lain yang perlu dibayar kepada Pengerusi dan Pengarah Bukan Eksekutif di bawah perkara 2.

3. **Pemilihan semula Pengarah yang akan bersara menurut Artikel 54**
   YBhg. Tuan Al-Ishsal bin Ishak dilantik menjadi Pengarah pada 20 September 2024 dan sebagai Pengerusi CyberSecurity Malaysia pada 9 Oktober 2024. Beliau hanya akan menjawat jawatan sebagai Pengarah dan Pengerusi untuk tempoh sehingga AGM ke-19 ini dan selepas itu menurut Artikel 54 Perlembagaan CyberSecurity Malaysia, beliau boleh dilantik semula sebagai Pengarah dan Pengerusi CyberSecurity Malaysia.

   Manakala, YBrs. Encik Derek John Fernandez dan YBrs. Puan Norhayati binti Masah pula telah dilantik menjadi Pengarah, masing-masing pada 2 Julai 2024 dan 18 Disember 2024. Mereka hanya akan menjawat jawatan tersebut sehingga AGM ke-19 ini dan selepas itu menurut Artikel 54 Perlembagaan CyberSecurity Malaysia, mereka boleh dilantik semula sebagai Pengarah CyberSecurity Malaysia.

   Berdasarkan Artikel 54 Perlembagaan CyberSecurity Malaysia, Pengarah-pengarah tersebut adalah layak untuk dilantik semula melalui resolusi AGM 2025 ini.

   Ketiga-tiga Pengarah tersebut telah bersetuju untuk dilantik semula sebagai Pengarah CyberSecurity Malaysia

4. **Pelantikan Juruaudit Kewangan Luar**
   Lembaga Pengarah CyberSecurity Malaysia di mesyuaratnya pada 29 Mei 2025 telah meluluskan untuk mengesyorkan pelantikan Tetuan Atarek Kamil Ibrahim & Co. sebagai juruaudit kewangan luar CyberSecurity Malaysia untuk kelulusan Anggota syarikat pada AGM yang akan datang.

FORM OF PROXY

CyberSecurity MALAYSIA
(Company No. 200601006881 / 726630-U)

Saya/Kami..(nama penuh dalam huruf besar)

No. Kad Pengenalan/No. Syarikat..

beralamat di ....

....sebagai

anggota CyberSecurity Malaysia, dengan ini melantik ....

....(nama penuh dalam huruf

besar) No. Kad Pengenalan/No. Syarikat ....

..................beralamat di ....

....

...............atau jika tidak kehadiran beliau ....

....(nama penuh dalam

huruf besar) No. Kad Pengenalan/No. Syarikat ....

.... beralamat di ....

.............................sebagai proksi saya/kami untuk mengundi bagi pihak saya/kami di Mesyuarat Agung Tahunan ke-19 yang akan berlangsung secara maya melalui penstriman langsung dari lokasi siaran di Bilik Jati, Level 10 Tower 1, Menara Cyber Axis, Jalan Impact, 63000 Cyberjaya, Selangor pada hari Selasa, 24 Jun 2025 jam 11.00 pagi atau pada sebarang penangguhan, seperti yang tertera :

RESOLUSI	BERSETUJU	TIDAK BERSETUJU
PERKARA 1 Menerima Penyata Kewangan yang telah diaudit bagi tahun kewangan berakhir 31 Disember 2024, berserta laporan-laporan Pengarah dan Juruaudit.		
RESOLUSI 1 Meluluskan pembayaran elaun bulanan Pengerusi Bukan Eksekutif dan Pengarah bukan Eksekutif berjumlah sehingga RM240,000 dan manfaat lain bermula dari tarikh AGM ke-19 sehingga AGM CyberSecurity Malaysia bagi yang berikutnya.		
RESOLUSI 2 Melantik semula Pengarah berikut, yang akan bersara mengikut giliran menurut Artikel 54 Perlembagaan CyberSecurity Malaysia dan oleh kerana layak, telah menawarkan diri untuk dilantik semula; a) YBhg. Tuan Al-Ishsal bin Ishak b) YBrs. Encik Derek John Fernandez c) YBrs. Puan Norhayati binti Masah		
RESOLUSI 3 Melantik Tetuan Atarek Kamil Ibrahim & Co. sebagai Juruaudit CyberSecurity Malaysia bagi tahun kewangan berakhir pada 31 Disember 2025 dan memberi kuasa kepada Pengarah bagi menetapkan imbuhan mereka.		
PERKARA 2 Melaksanakan apa-apa urusan lain yang mana notis sewajarnya telah diberikan mengikut Akta Syarikat 2016 dan Perlembagaan CyberSecurity Malaysia.		

Sila tandakan “X” dalam ruang yang disediakan di atas untuk menandakan pilihan anda. Jika tiada arahan tertentu, proksi akan mengundi atau tidak mengundi mengikut budi bicaranya.

Bertarikh .... hari bulan 2025

....

Tandatangan Anggota/Meterai

OPERATIONAL REVIEW

FOREWORD FROM THE CEO

Malaysia experienced a remarkable surge in digital transformation, touching every layer of society from critical infrastructure and government services to small and medium enterprises, and into the daily lives of citizens. As the nation embraced this unprecedented connectivity, the cyber threat landscape grew in both complexity and intensity. Against this backdrop, CyberSecurity Malaysia stood resolute at the frontline, defending the integrity of our cyberspace and reinforcing public confidence in the national digital ecosystem.

Our mission, which is to ensure a safer and more secure cyberspace for all Malaysians has never been more essential. We continued to strengthen our role as the nation's principal cybersecurity specialist agency, serving as a trusted advisor, enabler, and capacity builder across government, industry, and civil society. Through advanced threat intelligence, state-of-the-art digital forensics, rapid incident response, comprehensive capacity development, and strategic international collaborations, CyberSecurity Malaysia remained a steadfast pillar of the country's cyber defence strategy.

One of the key highlights in 2024 was the performance of Cyber999, the Cyber Incident Response Centre under CyberSecurity Malaysia, which recorded a total of 6,209 reported incidents, with fraud-related cases accounting for 4,219 incidents. This underscores both the persistent surge in malicious cyber activities and the growing public confidence in our capabilities to respond swiftly and effectively.

We also observed a significant rise in sophisticated threat vectors, including ransomware, AI-driven phishing campaigns, and malware targeting Operational Technology (OT) environments. These evolving threats demanded equally advanced, adaptive, and proactive responses. In anticipation, we enhanced our threat intelligence capabilities and fortified national incident response mechanisms to ensure greater resilience, precision, and agility in mitigating cyber risks.

"THE CYBER INCIDENT RESPONSE CENTRE UNDER CYBERSECURITY MALAYSIA, WHICH RECORDED A TOTAL OF 6,209 REPORTED INCIDENTS, WITH FRAUD-RELATED CASES ACCOUNTING FOR

4,219 INCIDENTS.

Dato' Ts. Dr. Haji Amirudin
Bin Abdul Wahab FASc
Chief Executive Officer

Operationally, enhancements were made within the Malaysia Computer Emergency Response Team (MyCERT) and the Digital Forensics Department. With upgraded capabilities in real-time monitoring, rapid threat analysis, and digital evidence handling, we significantly elevated our capacity to detect, assess, and respond to cyber incidents, delivering timely insights and support across key sectors.

Yet, cybersecurity, at its core, is not only a technological pursuit — it is a collective human responsibility. At the heart of every secure system are informed and vigilant individuals. In line with this, CyberSecurity Malaysia continued to invest heavily in human capital development, delivering structured training programmes, professional certifications, and wide-reaching awareness initiatives.

Our outreach impacted over 30,000 individuals across Malaysia. The CyberSecurity Awareness and Training (CSAT) programme delivered a spectrum of initiatives — from grassroots awareness campaigns to advanced professional certification under the Global Accredited Cybersecurity Education (ACE) framework. This holistic approach ensured inclusivity, equipping schoolchildren, educators, professionals, and communities alike with the knowledge and skills to safely navigate the digital realm.

Our flagship CyberSAFE® initiative also gained strong momentum, reaching diverse communities, including students, educators, and parents across both urban and rural areas. Under the National Anti-Scam Campaign 2024, we conducted high-impact engagements in Johor, Kedah, and Perak — reaching over 2,400 participants through both physical and digital platforms. These efforts reaffirm our commitment to making digital safety inclusive and accessible for all, regardless of geography or background.

Cyber threats know no borders and the defence against them must be equally borderless. In 2024, CyberSecurity Malaysia significantly enhanced its regional and international collaboration through strategic engagements with ASEAN and its member states, global Computer Security Incident Response Team (CSIRTs) / Computer Emergency Response Team (CERTs), and renowned cybersecurity centres of excellence. Furthermore, Malaysia is an active member of the Organisation of Islamic Cooperation – Computer Emergency Response Team (OIC-CERT), contributing to global cybersecurity innovation and reinforcing Malaysia's position as a key player on the international stage.

This international focus is well aligned with Malaysia's ASEAN Chairmanship in 2025, under the theme "Inclusivity and Sustainability". In this context, CyberSecurity Malaysia remains committed to fostering trust, resilience, and collaboration in the regional cybersecurity landscape, supporting a safer and more inclusive digital future for all.

Equally important is our dedication to cultivating the next generation of cybersecurity leaders. Through strategic partnerships with academia, industry, and international bodies, we are developing robust talent pipelines via future-ready curricula, innovation-led research, and comprehensive skills development programmes. Our mission is to nurture ethical, competent, and visionary professionals who will not only defend our cyberspace, but also shape its future with integrity, ingenuity, and purpose.

Our vision is bold and resolute: to transform Malaysia into a digitally secure, resilient, and trusted nation where innovation thrives in a safe and empowered environment.

These achievements would not have been possible without the unwavering commitment and professionalism of the extraordinary team at CyberSecurity Malaysia. I extend my deepest appreciation to every member of our organisation for their resilience, excellence, and dedication to public service. I would also like to express my sincere gratitude to the Ministry of Digital, our Board of Directors, and all our strategic partners for their continued trust, support, and guidance.

As we look ahead to 2025, I am confident that CyberSecurity Malaysia will continue to lead with purpose, protect with precision, and empower with passion. Together, we will build a cyberspace that all Malaysians can trust today, and for generations to come.

MANAGEMENT COMMITTEE MEMBERS

The Management Committee of CyberSecurity Malaysia provides important key guidance and leadership to help the organisation achieve its goals. In 2024, the Management Committee continued to support key efforts to improve cybersecurity of the nation and ensure the effective operationof the agency. The experience and dedication of our Management Committee members provided theeded impetus to move our mission forward.

Dato' Ts. Dr. Haji Amirudin Bin Abdul Wahab FASc.
Chief Executive Officer (CEO)

Roshdi Bin Hj Ahmad
Chief Operating Officer (COO)

Ts. Wan Roshaimi Bin Wan Abdullah
Chief Technology Officer (CTO)

Jailany Bin Jaafar
Head, Legal & Secretarial/
Company Secretary

Azman Bin Ismail
Senior General Manager,
Management Services Division

“ Our Leadership is our Greatest Asset

Ts. Mohd Zabri Adil Bin Talib
Principal Specialist,
Technology & Services Division

Zulfeka Bin Zainal Aibidin
General Manager,
Development & Industry Affairs

Mohd Adlyn Mughni Bin Shamsudin
General Manager,
Chief Executive Officer’s Office

Hamidun Bin Katemin
Acting General Manager,
Corporate Planning & Strategy Division

Sabariah Binti Ahmad
Acting Principal Specialist,
Pro-active Technology & Services
Division

Fazlan Bin Abdullah
Acting General Manager,
Pre-emptive Technology & Services
Division

REVIEW OF CORPORATE PERFORMANCE

CORPORATE KPI ACHIEVEMENT AS FOR THE YEAR 2024 IS:

99.84%

The following table details the 2024 KPI – the indicators, and our performance in relations to the targets.

KPI	Target	Achievement	%
Collaborators In Driving the National Agenda			
1. # Trained knowledge workers	1,600	1,824	100
2. # Strategic paper received by stakeholders/ customers	1	1	100
3. # Leading a cybersecurity programme	7	8	100
4. # Beneficiary of a cybersecurity programme	26,500	28,150	100
5. # Recognition and awards at the national and/or international level	5	7	100
Deliver Quality and Impactful Services			
6. # Organizations participating in the Cybersecurity Empowerment Promotion Programme (PGPKS)	100	100	100
7. # Industry partners participating in the CyberSecurity Malaysia Collaboration Program (CCP)	10	20	100
8. # Corporate social responsibility (CSR) initiatives	2	2	100
9. % Customer Satisfaction Level	88	94.48	100
10. # Companies benefiting from the Cybersecurity Industry Collaboration Programme	5	7	100
11. # ICT products and organisations certified under schemes managed by CyberSecurity Malaysia	35	39	100
Financial Sustainability			
12. $ Net Profit before tax	1,700,000	3,096,979	100
Integrated Development and Delivery			
13. % Service Level Agreement (SLA) Assurance	100	99.87	99.87
14. % Implementation of Transformation Plan Programme	100	96.88	96.88
15. % Resolution of Cyber Cases / Incidents at CyberSecurity Malaysia Level	90	93.95	100
16. % Improvement of IT Infrastructure and Systems	100	100	100
17. # Registered Intellectual Property	2	4	100
Technical Excellence and Capacity Enhancement			
18. # Articles published in domain of cybersecurity	12	29	100
19. % Employee Engagement Satisfaction Level	80	83	100
20. # Implementation of innovation programmes	2	2	100

2024 CALENDAR OF ACTIVITIES

In the past year, CyberSecurity Malaysia engaged in various activities to enhance cybersecurity measures and raise awareness. By undertaking these activities, we have achieved significant milestones, strengthened our position as Malaysia's national cybersecurity specialist agency, and enhanced stakeholder value.

9 JANUARY 2024

Working Visit by YB Wilson Ugak Kumbong, Deputy Minister of Digital to CyberSecurity Malaysia.

9 FEBRUARY 2024

SIBER
MALAYSIA
MADANI
Amalkan adab serta budi pekerti yang baik, berusaha melengkapkan diri dengan ilmu pengetahuan bagi membudayakan penggunaan teknologi digital yang positif. Bersama-sama ke arah kesejahteraan siber.
6 Februari 2024
www.cybersafe.my/saferinternetday

Safer Internet Day 2024 Celebration (SID).

14 MARCH 2024

Working Visit by YBhg. Datuk Haji Rodzi Bin Md Saad, Secretary-General of the Ministry of Digital to CyberSecurity Malaysia and Iftar Ceremony.

25 MARCH 2024

CyberSecurity Malaysia CSR Programme 2024 "Kembara Amal CyberSAFE" with Orphans from Bait Al Amin, Parit, Perak Darul Ridzuan.

2 May 2024

Visit by the Royal Malaysian Air Force (RMAF) Air Operations Command Headquarters to CyberSecurity Malaysia.

5-6 May 2024

National Anti-Scam Campaign 2024 – Johor at Sultan Iskandar Hall, Universiti Teknologi Malaysia (UTM), Skudai, Johor.

14 May 2024

Launch Ceremony of the Study Report on the Demand and Supply of TVET Workforce in the Field of Cybersecurity.

MAJLIS PELANCARAN
LAPORAN KAJIAN PERMINTAAN DAN PENAWARAN TENAGA KERJA PENDIDIKAN DAN LATIHAN TEKNIKAL DAN VOKASIONAL (TVET) DALAM BIDANG KESELAMATAN SIBER
DIRASMIKAN OLEH
YB ENCIK STEVEN SIM CHEE KEONG
MENTERI SUMBER MANUSIA
14 MEI 2024 | DEWAN SERBAGUNA, MENARA CYBER AXIS, CYBERJAYA

23-26 May 2024

Sambutan Minggu Perpaduan 2024 National at Angsana Mall, Johor Bahru.

19-20 June 2024

ASEAN Region Cyber Workshop – "Protecting ASEAN Critical Infrastructure in the Age of AI", Kuala Lumpur.

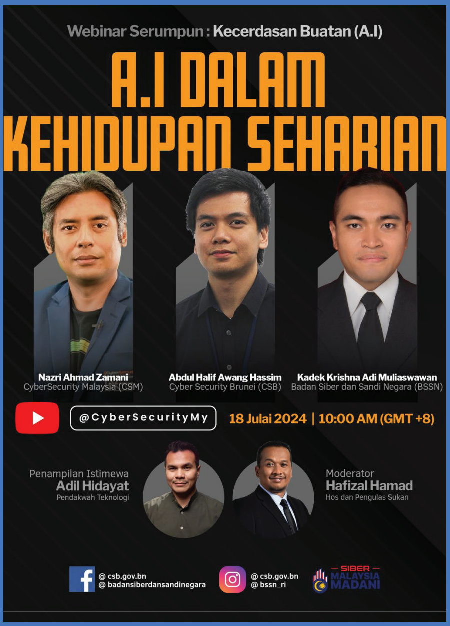
24 June 2024

Memorandum of Understanding Signing Ceremony between Universiti Sains Islam Malaysia (USIM) & CyberSecurity Malaysia at USIM Chancellery Building.

26-27 June 2024

National Anti-Scam Campaign 2024 – Kedah at Seri Negeri Hall, Wisma Darul Aman, Alor Setar, Kedah.

18 July 2024



Webinar Serumpun : Kecerdasan Buatan (A.I)

A.I DALAM KEHIDUPAN SEHARIAN

Nazri Ahmad Zamani
CyberSecurity Malaysia (CSM)

Abdul Halif Awang Hassim
Cyber Security Brunei (CSB)

Kadek Krishna Adi Muliaswawan
Badan Siber dan Sandi Negara (BSSN)

@CyberSecurityMy

18 Julai 2024 | 10:00 AM (GMT +8)

Penampilan Istimewa
Adil Hidayat
Pendakwah Teknologi

Moderator
Hafizal Hamad
Hos dan Pengulas Sukan

@ csb.gov.bn
@ badansiberdansandinegara

@ csb.gov.bn
@ bssn_ri

SIBER MALAYSIA MADANI

Serumpun Webinar 2024 – "AI in Daily Life".

3 August 2024

Program Komuniti Jelajah Digital Anak Muda, Kapit, Sarawak at SMK Kapit 2, Kapit, Sarawak.

6-8 August 2024

CyberDSA 2024 at Kuala Lumpur Convention Centre.

6 August 2024

Gala Dinner in Conjunction with the Malaysia Cybersecurity Awards 2024 at Kuala Lumpur Convention Centre.

14 August 2024

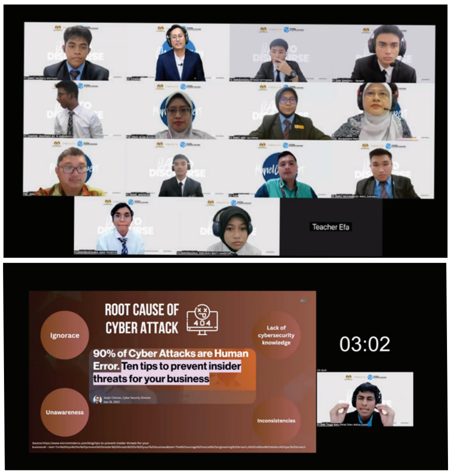
Opening Ceremony of the Course: "Cyber Darkweb and Virtual Currency: An Overview", Capsule Room, CyberSAFE^{TM} L.I.V.E Gallery.

15 August 2024

Personal Data Protection Conference (Organized by JPDP), Impiana Hotel Senai, Johor.

19-22 August 2024

National ICT Security Discourse – CyberSAFE Challenge Trophy 2024 (NICTSeD 2024), Octo and Quarter Finals.


Teacher Efa
ROOT CAUSE OF CYBER ATTACK
Ignorace
Unawareness
Lack of cybersecurity knowledge
Inconsistencies
90% of Cyber Attacks are Human Error. Ten tips to prevent insider threats for your business
03:02

4 September 2024

Semi-Finals of the National ICT Security Discourse 2024, Terengganu.

22-26 September 2024

MyCryptology Week 2024.

24 September 2024

Finals of the National ICT Security Discourse 2024 (NICTSeD 2024).

18 OCTOBER 2024

Program Galakan Pemerkasaan Keselamatan Siber (PGPKS) for Small and Medium Enterprises (SMEs) in Conjunction with the Madani Rakyat Programme 2024 “Love Sabah”, Kota Kinabalu.

24-26 OCTOBER 2024

MDEC
MD
MALAYSIA DIGITAL XCELERATION SUMMIT 2024
24-26 October 2024 | MITEC, KL
MDX
SUMMIT 2024

Malaysia Digital Experience 2024 (MDX 2024), Kuala Lumpur.

12-13 NOVEMBER 2024

National Anti-Scam Campaign 2024 – Perak.

16 NOVEMBER 2024

Hari Bersama Pelanggan Jabatan Perlindungan Data Peribadi (JPDP), IOI City Mall, Putrajaya.

19-21 NOVEMBER 2024

SMART Nation Expo 2024, MITEC, Kuala Lumpur.

9 JANUARY 2024

Program 2 Tahun Kerajaan Madani & Konvensyen Nasional Reformasi Perkhidmatan Awam 2024, MITEC, Kuala Lumpur.

ACHIEVEMENT AND AWARDS 2024

4 April 2024
The Chief Executive Officer of CyberSecurity Malaysia was appointed as Adjunct Professor at the College of Computing, Informatics and Mathematics (KPPIM), Universiti Teknologi MARA (UiTM), Shah Alam.

May 2024
The Chief Executive Officer of CyberSecurity Malaysia was appointed as CEO@POLYCC under the Department of Polytechnic and Community College Education for the term of May 2024 to April 2026.

5 July 2024
The Chief Executive Officer of CyberSecurity Malaysia was appointed as CEO@Faculty Programme 2024–2026 at Universiti Sains Islam Malaysia (USIM).

30 July 2024
The Chief Executive Officer of CyberSecurity Malaysia was conferred the National Technologist Award by the Ministry of Science, Technology and Innovation (MOSTI) through the Malaysia Board of Technologists (MBOT).

1 October 2024
Dr. Maslina Binti Daud, Head of the Proactive Services and Technology Division, was awarded the Standards and Accreditation Award for the Year 2023 by the Department of Standards Malaysia.

17 October 2024
The Chief Executive Officer of CyberSecurity Malaysia received the AJCCA Cyber Resilience Award from the ASEAN-Japan Cybersecurity Community Alliance (AJCCA).

20 November 2024
CyberSecurity Malaysia was honoured with the Digital Society Award at the Malaysia Digital Transformation Awards 2024, organised by GovInsider.

PROFESSIONAL CERTIFICATION

As the national cybersecurity specialist agency, CyberSecurity Malaysia is deeply committed to fostering a skilled and resilient cybersecurity workforce. In line with our mission to strengthen Malaysia's cybersecurity capabilities, we take pride in recognising individuals who have achieved professional certifications over the past year. These certifications demonstrate not only personal commitment to excellence but also contribute to our national agenda of building a secure and trusted cyber environment.

This section highlights the names of CyberSecurity Malaysia personnel who have obtained industry-recognised certifications. Their achievements reflect a strong foundation of expertise, professionalism, and continuous improvement. We commend these individuals for their dedication and thank them for their role in advancing Malaysia's cybersecurity readiness and resilience.

SEC699: ADVANCED PURPLE TEAMING ADVERSARY EMULATION & DETECTION ENGINEERING

1. Ahmad Aizuddin Aizat Bin Tajul Arif

SANS SEC599: DEFENDING ADVANCED THREATS

1. Muhammad Fitri Bin Mohd Sultan

FOR578: GIAC CYBER THREAT INTELLIGENCE

1. Lukman Hakim Bin Abd Rahman
2. Nur Qurratu 'Aini Binti Rohizan

SANS SEC 497: PRACTICAL OPEN-SOURCE INTELLIGENCE (OSINT)

1. Mohd Rizal Bin Abu Bakar
2. Ikmal Halim Bin Jahaya

SANS SEC522 : GIAC CERTIFIED WEB APPLICATION DEFENDER

1. Nur Syahidah Binti Yunos

CRASH DATA RETRIEVAL OPERATORS COURSE

1. Sharifah Nurul Asyikin Binti Syed Abdullah

DARK: DARKNET INVESTIGATIONS FOR LAW ENFORCEMENT

1. Mohammad Zaharudin Bin Ahmad Darus
2. Nurshahira Binti Mohd

DARK WEB COUNCIL CERTIFIED

1. Nurshahira Binti Mohd

CERTIFICATION OF CERTIFIED IN CYBERSECURITY

1. Muhammad Syahreen Bin Zulkifli

CERTIFIED THREAT INTELLIGENCE ANALYST (C|TIA)

1. Mohammad Zaharudin Bin Ahmad Darus
2. Hairul Anuar Abu Hanipah
3. Mohamad Hafiz Bin Rahman
4. Nurshahira Binti Mohd
5. Muhammad Amirul Bukhari Bin Razak
6. Mohamed Iqbal Bin Tajol Azmi
7. Mohammad Faisal Bin Ismail
8. Suraya Hani Binti Ahmad Zaki
9. Nur Afiqah Naqiah Binti Mohd Sabri
10. Sarah Binti Abdul Rauf

CompTIA SECURITY PLUS

1. Zafreida Binti Zahrullayali

CompTIA CLOUD ESSENTIALS

1. Ahmad Hisyamudin Bin Salleh
2. Mohammad Asyran Fitri Bin Dunya
3. Shahrin Bin Baharom
4. Zul Hafiy Ikmal Bin Mohd Marzuki
5. Ahmad Azizul Iqram Bin Musa
6. Nurul Asha Binti Jeffridin
7. Farhan Arif Bin Mohamad
8. Noraqilah Binti Azlan
9. Muhammad Ikhwan Bin Mohammad Faisal

CompTIA ADVANCED SECURITY PRACTITIONER

1. Izzatul Hazirah Binti Ishak

CERTIFIED ASSOCIATES PYTHON PROGRAMMER PCAP PYTHON

1. Nur Syahidah Binti Yunos

CERTIFIED ETHICAL HACKER (C|EH)

1. Nor Azeala Binti Mohd Yusof
2. Suhairi Bin Mohd Jawi
3. Dr. Isma Norshahila Binti Mohammad Shah
4. Dr. Abdul Alif Bin Zakaria
5. Ahmad Rabbani Bin Omar
6. Mohamed Iqbal Bin Tajol Azmi

VIDEO ANALYSIS IN COLLISION RECONSTRUCTION

1. Sharifah Nurul Asyikin Binti Syed Abdullah

ASSOCIATE CYBER RESILIENCE PROFESSIONAL

1. Fazlan Bin Abdullah
2. Rushidan Bin Ghazali
3. Noor Azwa Azreen Binti Abd Aziz
4. Nurfarhana Nasrulhaq Binti Mohd Zulkifli
5. Muhamad Zaim Bin Mohd Rozi
6. Yuzida Binti Md Yazid
7. Najatul Faghira Binti Abdul Hamid

CERTIFIED INFORMATION PRIVACY MANAGER

1. Sabariah Binti Ahmad
2. Ida Rajemee Binti Ramlee
3. Naqliyah Binti Zainuddin

PMI RISK MANAGEMENT PROFESSIONAL (PMI-RMP)

1. Ahmad Hisyamudin Bin Salleh

PRINCE2 FOUNDATION

1. Ahmad Hisyamudin Bin Salleh
2. Noraqilah Binti Azlan

CERTIFIED DIGITAL FORENSIC FOR FIRST RESPONDER

1. Shawn Slyvester A/L Damotharam
2. Syarifah Nabilah Syahirah Binti Syed Abd Wahab

CERTIFIED CRYPTOCURRENCY FORENSIC INVESTIGATOR (CCFI)

1. Hanania Aida Binti Mohd Hilmi
2. Akmalsuriani Binti Mohd Rakof
3. Norhafizah Binti Hashim

CERTIFIED INFORMATION SECURITY MANAGEMENT SYSTEM AUDITOR (CISMSA)

1. Marziaton Binti Omar

CERTIFIED INFORMATION SECURITY AWARENESS MANAGER (CISAM)

1. Noor Atiqah Binti Abd Manan
2. Yang Kalsum Binti Ibrahim
3. Aina Mardhiah Binti Zolkapile
4. Azlin Binti Samsudin
5. Noor Azleena Bt Kamarudin
6. Aziim Anwar Bin Abd.Wahid
7. Abdul Hakim Bin Mohd Raidzoh
8. Nor Syafiza Abdul Rahim
9. Siti Aishah Binti Omar

LEAD ASSESSOR ISO/IEC 17025:2017 LABORATORY QMS (LAL01)	
1.	Ahmad Dahari Bin Jarno
2.	Nor Zarina Binti Zamri
3.	Nur Iylia Binti Roslan
4.	Shahrin Bin Baharom
5.	Mohd Muslim Bin Mohd Aruwa
6.	Nur Sharifah Idayu Binti Mat Roh
7.	Nurul Syahirah Binti Aspawi
8.	Nurul Asha Binti Jeffridin
9.	Nor Fatihah Binti Mohd Zabidi
10.	Azatulsheera Binti Mohd Azman

LEAD ASSESSOR ISO/IEC 27001:2022 ISMS	
1.	Mohammad Azree Bin Yahaya
2.	Nor Salwani Binti Jaa'far
3.	Syarifah Nabilah Syahirah Binti Syed Abd Wahab
4.	Ummu Razanna Binti Abdul Razak
5.	Akmal Suriani Binti Mohamed Rakof

ISO/IEC 17025:2017 UNDERSTANDING & IMPLEMENTING (QL01)	
1.	Noraqilah Binti Azlan
2.	Nor Muhammad Ikhwan Bin Mohammad Faisal Binti Jaa'far

EDITORIAL COMMITTEE

SENIOR EDITORIAL TEAM

Hamidun Katemin

Roshdi Hj Ahmad

Mohd Shamil Mohd Yusoff

CONTENT CONTRIBUTOR

Azlim Anwar Abd. Wahid

Azlin Samsudin

Ernieza Ismail

Azrina Md Saad

Alifa Ilyana Chong Abdullah

DIGITAL TEAM

Zul Akmal Abd Manan

Nurul 'Ain Zakariah

Zaihasrul Ariffin

Farhana Natasha Mazlan

Nurrul Syafina Md Yahaya

LIKE • COMMENT • SHARE • FOLLOW

KEMENTERIAN DIGITAL

CyberSecurity MALAYSIA

STAY CONNECTED WITH US ON SOCIAL MEDIA

CyberSecurityMalaysia

cybersecurity_malaysia

CyberSecurity Malaysia

cybersecuritymy

cybersecuritymy

CyberSecurityMy

SCAN THE QR CODES ABOVE TO FOLLOW US!

LIKE • COMMENT • SHARE • FOLLOW

Get the latest news, exclusive updates, and exciting content

Get the latest news, exclusive updates, and exciting content

Corporate Office:
CyberSecurity Malaysia
Level 7, Tower 1, Menara Cyber Axis,
Jalan Impact, 63000 Cyberjaya,
Selangor Darul Ehsan,
Malaysia.

Tel: +603 - 8800 7999
Fax: +603 - 8008 7000
Email: enquiry@cybersecurity.my
Customer Service Hotline: 1 300 88 2999
www.cybersecurity.my

MINISTRY OF DIGITAL