PKCERT

NATIONAL COMPUTER EMERGENCY RESPONSE TEAM

Government of Pakistan

National CERT Cyber Security Training Guidelines

info@pkcert.gov.pk | www.pkcert.gov.pk

Introduction

In alignment with the Digital Pakistan initiative spearheaded by the Government of Pakistan, cybersecurity stands as a fundamental pillar in ensuring the integrity, resilience, and security of national information systems and ICT products. As Pakistan accelerates its digital transformation, the increasing reliance on technology demands robust mechanisms to safeguard critical infrastructure, sensitive data, and digital services from an evolving array of cyber threats.

Recognizing this imperative, the National Computer Emergency Response Team of Pakistan (National CERT) is committed to strengthening the cybersecurity posture of the country by enhancing the skills and competencies of government employees and stakeholders across all professional levels. The development of a National Skilled Cyber Workforce is essential to bridging existing gaps and equipping personnel with the expertise necessary to mitigate cyber risks effectively.

This agenda is firmly rooted in the directives set forth by the National Cyber Security Policy 2021[1] and CERT Rules 2023[2], both of which emphasize the need for continuous capacity building and skill development to counter sophisticated cyber threats. In line with these frameworks, these training guidelines have been keenly designed to address the unique cybersecurity training requirements of non-technical staff, technical professionals, management teams, and top executives—ensuring a comprehensive and structured approach to cybersecurity preparedness.

Developed in accordance with national and international threat landscapes, these guidelines have been meticulously mapped to address the expanding attack surface, ensuring that Pakistan's cybersecurity readiness remains proactive and adaptive. By implementing these comprehensive training frameworks, National CERT aims to fortify Pakistan's cyber defenses, mitigate emerging threats, and foster a culture of cybersecurity awareness at every level of governance and industry.

Purpose

The purpose of these cyber security training guidelines from the National CERT is manifold:

1. **Empowering Employees**: Equip all employees, regardless of their technical expertise, with the knowledge and skills required to identify, mitigate, and respond to cybersecurity threats effectively.

---

[1] National Cyber Security Policy, 2021, Ministry of Information Technology & Telecommunications

[2] CERT Rules, 2023, Ministry of Information Technology & Telecommunications

2. **Enhancing Organizational Resilience:** Build a workforce capable of safeguarding the organization's critical assets and operations against emerging cyber risks through continuous education and training.

3. **Ensuring Strategic Alignment:** Enable senior management and top executives to integrate cybersecurity principles into organizational policies and decision-making, ensuring alignment with global standards and best practices.

4. **Promoting a Culture of Awareness:** Foster an environment where cybersecurity is a shared responsibility, ingrained in the organizational ethos, and actively championed by all members.

Guidelines Structure

These guidelines are organized into four tiers, each tailored to address the specific roles, responsibilities, and skillsets. The End User tier focuses on foundational cyber security best practices, the Technical & Operations tier emphasizes advanced cybersecurity and IT competencies, the Management tier highlights strategic governance and operational policy-making capabilities, and the Top Executives tier underscores leadership in aligning cybersecurity with global standards and organizational strategies.

Through structured and deliberate training, the National CERT aims to not only enhance individual competencies but also fortify the organization's collective ability to anticipate, withstand, and recover from cyber incidents. By adhering to these guidelines, constituents will contribute to a robust and secure digital environment, ultimately advancing the mission of the National CERT and supporting national cybersecurity objectives.

Tier 1: End User (Non-IT/Cybersecurity Resources)

Focus: Foundational knowledge and safe digital practices for end users.

Tier 2: Technical & Operations (IT and Cybersecurity Operations/Resources)

Focus: Advanced technical skills to implement and maintain robust cybersecurity measures.

Tier 3: Management (Policy Makers, Managers, and Team Leads)

Focus: Strategic oversight, governance, and policy-making to align cybersecurity with organizational goals.

Tier 4: Top Executives (Decision Makers, C-Level Executives & Directors)

Focus: Leadership in global cybersecurity standards, governance, and strategic preparedness.

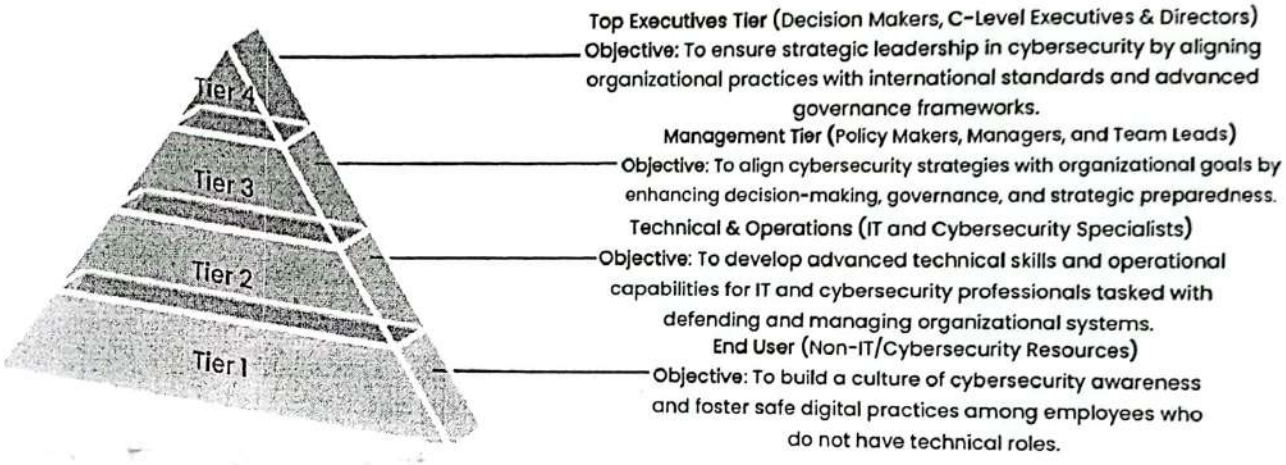

Fig 1: Pyramid Representing 4-Tiered National CERT's Training Guidelines.

National CERT has suggested core training modules essential for role-specific cybersecurity competence under each tier. However, these are not limited to the recommended modules; organizations can expand their training programs by including additional courses and modules tailored to their unique operational needs and security objectives. The guidelines serve as a framework for organizations to design and implement their own capacity-building initiatives.

Tier 1: End User (Non-IT/Cybersecurity Resources)

The Tier 1 is designed to equip non-technical employees with essential cybersecurity knowledge, ensuring they can identify, prevent, and respond to risks effectively. Given that cybercriminals often exploit human vulnerabilities through phishing, malware, and social engineering, it is crucial for employees to recognize these threats and adopt secure digital practices.

This tier covers basic cybersecurity awareness, data privacy, secure device usage, incident reporting, and safe social media habits, ensuring employees handle sensitive data responsibly, recognize suspicious activities, and follow secure communication practices. By integrating interactive workshops, phishing simulations, case studies, and hands-on exercises, it reinforces real-world applications of cybersecurity principles. At a national level, empowering the workforce with cybersecurity skills aligns with regulatory frameworks, strengthens overall cyber resilience, and mitigates the risks of data breaches and financial fraud. Ultimately, every employee plays a pivotal role in national cybersecurity, and this foundational training ensures they become the first line of defense against cyber threats, protecting both their organizations and the broader digital ecosystem.

Tier 2: Technical & Operations (IT and Cybersecurity Specialists)

The Tier 2 is designed to equip IT professionals and cybersecurity experts with the advanced technical skills and operational capabilities needed to defend and manage organizational systems against cyber threats. As organizations face increasingly sophisticated cyberattacks, professionals in this tier are tasked with securing infrastructures, identifying vulnerabilities, and ensuring robust defenses. This tier focuses on real-world applications of vulnerability assessments, penetration testing, security audits, risk management, and secure application development to enable the technical and operations personnel to effectively mitigate and respond to emerging threats. The tier covers penetration testing techniques to identify and exploit vulnerabilities, security audits to assess compliance and security controls, and risk assessment methodologies to prioritize and implement critical security measures such as firewalls, intrusion detection systems, and secure authentication protocols.

Additionally, SOC operations training enhances the efficiency of security teams in detecting and responding to incidents in real time, while the secure application development module focuses on embedding secure coding practices throughout the software development lifecycle. Through virtual labs, hands-on challenges, scenario-based exercises, and case studies, employees will refine their technical expertise and gain practical experience. This comprehensive training ensures that cybersecurity professionals are equipped to protect systems, improve organizational resilience, and

maintain compliance with industry standards, ultimately strengthening the overall security posture of their organizations and contributing to national cybersecurity efforts.

Tier 3: Management Tier (Policy Makers, Managers, and Team Leads)

The Tier 3 is designed to align cybersecurity strategies with organizational goals by enhancing the decision-making capabilities, governance structures, and strategic preparedness of key leadership roles. As organizations face increasingly complex cyber threats, decision-makers must develop the ability to oversee, guide, and enforce robust cybersecurity measures while ensuring alignment with organizational objectives. This tier is designed to empower managers and team leads to craft and enforce effective cybersecurity governance frameworks, establish clear policies, and define roles and responsibilities for policy implementation. It also focuses on incident response management, equipping leaders with the skills to make informed decisions during crises, manage communication strategies, and navigate complex incidents through incident escalation paths.

The tier further addresses the critical importance of cybersecurity standards and compliance, ensuring that managers are familiar with industry frameworks and regulatory requirements, and can prepare their organizations for audits and address compliance gaps. An additional critical module, Third-Party Risk Management, helps managers understand the vulnerabilities introduced by external vendors and partners, and how to assess and mitigate risks associated with third-party relationships. The training ensures that leaders can manage risks posed by third-party systems, ensuring that appropriate security measures and controls are in place. Through executive briefings, policy workshops, tabletop exercises, and compliance-focused workshops, this tier ensures that managers are well-prepared to lead their organizations in safeguarding digital assets, responding effectively to incidents, and maintaining compliance with global standards, thereby strengthening the organization's overall cybersecurity posture and contributing to national resilience against cyber threats.

Tier 4: Top Executives Tier (Decision Makers, C-Level Executives & Directors)

The Tier 4 is designed to ensure strategic leadership in cybersecurity by aligning organizational practices with international standards and advanced governance frameworks. As cyber threats continue to evolve and pose significant risks to national security and global economies, top executives play a pivotal role in shaping the cybersecurity direction of their organizations. This tier equips executives with the knowledge to navigate national and global cybersecurity frameworks, ensuring compliance with key standards such as ISO 27001 and GDPR, and best practices for enterprise-level implementation. The training enhances cybersecurity governance by helping leaders understand the importance of establishing effective governance structures and integrating cybersecurity into broader organizational objectives, facilitating strategic decision-making at the highest levels.

Additionally, it emphasizes crisis leadership by preparing executives to respond to large-scale cyber incidents, employing crisis management frameworks, and building organizational resilience through strategic foresight. As emerging technologies like AI, IoT, and quantum computing continue to shape the cybersecurity landscape, executives must be trained to anticipate the implications of these advancements and develop proactive strategies to mitigate advanced threats. Lastly, the tier also delves into the role of cyber diplomacy, focusing on international collaboration, cross-border threat intelligence sharing, and diplomatic negotiations in tackling global cybersecurity challenges. Through high-level policy discussions, expert briefings, tabletop exercises, and diplomatic strategy workshops, this tier ensures that decision-makers are prepared to lead their organizations with a forward-thinking cybersecurity strategy that aligns with both national and global security priorities.

Tier-Wise Detailed Modules and Underlying Contents

Tier 1: End User (Non-IT/Cybersecurity Resources)

Core Training Modules	Objective	Content	Delivery Methods
1. Basic Cybersecurity Awareness	Help employees recognize and avoid common threats such as phishing and malware.	i. Overview of phishing attacks and social engineering tactics. ii. Identifying secure websites and links. iii. Password security essentials.	Workshops, phishing simulations, interactive quizzes, instructor-led sessions.
2. Data Privacy Essentials	Ensure employees handle organizational data responsibly and understand privacy principles.	i. Types and classifications of sensitive data. ii. Data sharing protocols and legal implications of data breaches. iii. Examples of successful and failed privacy measures.	Video tutorials, case studies with role-specific focus, instructor-led sessions.
3. Secure Device Usage	Reduce vulnerabilities associated with endpoints and personal devices.	i. Importance of timely patch management and regular software updates to maintain system security. ii. Safe practices for email and file sharing.	Hands-on exercises, practical guides, instructor-led sessions.
4. Incident Awareness and Reporting	Encourage early detection and timely reporting of cybersecurity incidents.	i. Recognizing signs of suspicious activity. ii. Steps for reporting incidents through proper channels.	Scenario-based training, reporting simulations, instructor-led sessions.
5. Safe Social Media Usage	Educate employees on responsible and secure social media behavior.	i. Risks of oversharing personal and corporate information. ii. Recognizing and avoiding social media scams. iii. Best practices for securing social media accounts.	Interactive webinars, real-world case studies, security checklists.

Tier 2: Technical & Operations (IT and Cybersecurity Specialists)

Core Training Modules	Objective	Content	Delivery Methods
1. Vulnerability Assessment & Penetration Testing (VAPT)	Train professionals to identify and fix vulnerabilities and assess the effectiveness of security controls	i. Simulating real-world attacks to identify and exploit vulnerabilities in target systems ii. Conducting systematic scans and controlled exploitation to validate and assess vulnerabilities iii. Reviewing findings, analyzing attack vectors, and recommending security improvements	*Virtual labs, hands-on challenges, scenario-driven exercises, instructor-led sessions (for guided multi-subtopics and structured learning where needed)*
2. Security Audits	Develop expertise in evaluating organizational systems and ensuring compliance with security standards and best practices	i. Reviewing and analyzing security policies, procedures, and controls ii. Performing gap analysis to identify non-compliance with industry frameworks and regulatory requirements iii. Generating detailed audit reports with actionable recommendations for remediation	*Case studies, audit simulation exercises, report preparation workshops, instructor-led sessions (for reviewing frameworks, compliance, and structured auditing techniques)*
3. Risk Assessment & Cybersecurity Control Implementation	Equip professionals with skills to assess and mitigate cybersecurity risks, as well as to deploy, configure, and maintain robust security controls	i. Risk frameworks and analysis techniques ii. Real-time risk assessment and prioritization iii. Implementation of network security controls (firewalls,	*Workshops featuring real-world scenarios, step-by-step implementation guides, risk-based practices, system configuration simulations, risk assessment tools, instructor-led sessions (for foundational risk management principles and control deployment training)*

		IDS/IPS, endpoint protection). iv. Configuring access control measures, encryption protocols, and secure authentication mechanisms. v. Regular monitoring, updating, and fine-tuning of security controls for optimal performance.	
4. SOC Operations and Orchestration	Enhance the efficiency of Security Operations Centers (SOC).	i. Use of tools for threat detection. ii. Development of incident response playbooks.	Scenario-driven SOC simulations with live data.
5. Secure Application Development (Exclusive to Development-Related Sectors)	Foster secure coding practices to prevent application vulnerabilities.	i. Secure Software Development Lifecycle (SDLC). ii. Mitigation strategies for common application vulnerabilities.	Peer code reviews, interactive coding sessions, and case studies.

Tier 3: Management Tier (Policy Makers, Managers, and Team Leads)

Core Training Modules	Objective	Content	Delivery Methods
1. Cybersecurity Governance and Policy Making	Strengthen governance frameworks and policy enforcement.	i. Drafting and updating cybersecurity policies. ii. Defining roles and responsibilities for policy implementation.	Policy workshops, case studies on governance challenges, instructor-led Sessions (*(hands-on policy development and role-based discussions are best conducted in an interactive setting*).
2. Incident Response Management Frameworks	Enable effective oversight during incidents.	i. Crisis communication strategies. ii. Incident escalation paths and decision-making during crises.	Tabletop exercises simulating multi-faceted attacks, workshop/instructor-led sessions (*incident handling requires interactive simulations for real-time decision-making practice*).
3. Cybersecurity Standards and Compliance	Ensure adherence to regulatory and industry standards.	i. Exploration of relevant standards and frameworks. ii. Preparing for audits and addressing compliance gaps.	Compliance-focused workshops with hands-on audits, instructor-led sessions (*regulatory training benefits from instructor-led guidance and practical exercises*).
4. Emerging Threats and Strategic Preparedness	Equip managers with the knowledge to anticipate and address future threats.	i. Trends in ransomware, AI threats, and zero-day vulnerabilities. ii. Cross-sector collaboration for intelligence sharing.	Executive briefings and strategic discussions.
5. Third-Party Risk Management	Mitigate security risks arising from vendors, partners, and supply chains.	i. Assessing and managing risks associated with third-party vendors and suppliers. ii. Establishing security requirements in vendor contracts. iii. Continuous monitoring and auditing of third-party security practices.	Vendor risk management workshops, contract review sessions, and case studies, workshop/instructor-led sessions (*risk assessment and contract negotiations require guided discussions and scenario-based exercises.*)

Tier 4: Top Executives Tier (Decision Makers, C-Level Executives & Directors)

Core Training Modules	Objective	Content	Delivery Methods
1. National & Global Cybersecurity Standards and Frameworks	Equip leaders with an understanding of key national and international cybersecurity standards and frameworks.	i. Overview of global frameworks such as ISO 27001 and GDPR. ii. Key national cybersecurity policies, laws, regulatory, and legislative frameworks. iii. Best practices for enterprise-level implementation.	Expert-led workshops and executive roundtables, instructor-led training *(to ensure in-depth discussion and regulatory clarity)*.
2. Strategic Cybersecurity Governance	Enhance leadership capabilities in implementing cybersecurity governance.	i. Governance structures and decision-making models. ii. Integrating cybersecurity into organizational objectives.	Scenario-based governance training and case studies, instructor-led training *(to facilitate interactive discussions on governance challenges)*.
3. Crisis Leadership and Strategic Preparedness	Develop leadership strategies for responding to large-scale cyber incidents.	i. Crisis management frameworks and decision-making during incidents. ii. Building resilience through strategic foresight.	Tabletop exercises and strategic simulation activities, instructor-led training (*to simulate real-world crisis scenarios for better preparedness*).
4. Emerging Technologies and Future Risks	Prepare for the implications of emerging technologies and evolving threats.	i. Impacts of AI, IoT, and quantum computing on cybersecurity. ii. Proactive strategies for mitigating advanced threats.	Expert briefings and collaborative strategy sessions.
5. Cyber Diplomacy	Strengthen international collaboration and policy-making in global cybersecurity efforts.	i. Understanding the role of cybersecurity in international relations. ii. Cross-border threat intelligence sharing and diplomatic negotiations. iii. Legal and ethical considerations in cyber warfare and state-sponsored attacks.	High-level policy discussions, international cybersecurity forums, and diplomatic strategy workshops, instructor-led training (*to foster direct engagement and diplomatic skill-building*).

Implementation Strategy

1. **Training Cycles**: Conduct periodic training sessions for all tiers, supplemented by updates based on emerging threats and regulatory changes.

2. **Customization**: Adapt training content to organizational needs, national laws, policies, frameworks and specific industry requirements.

3. **Feedback Mechanism**: Incorporate post-training evaluations and organizational feedback to refine programs.

4. **Multi-Modal Learning**: Use a blend of in-person workshops, virtual simulations, and e-learning platforms for maximum engagement.

Conclusion

The National CERT's cybersecurity training guidelines are a crucial step towards building a resilient and proactive cybersecurity framework for Pakistan. By empowering employees across all levels with the necessary knowledge and skills, strengthening organizational defenses, and ensuring alignment with global standards, these guidelines aim to address the evolving cyber threat landscape. Through continuous capacity building, Pakistan can foster a culture of cybersecurity awareness, ensuring that both public and private sectors are well-prepared to defend against cyber risks and contribute to the country's digital transformation and security goals.

References

1. **Ministry of Information Technology and Telecommunication (MoITT).** (2021). *National Cyber Security Policy 2021.* Retrieved from https://moitt.gov.pk/SiteImage/Misc/files/National%20Cyber%20Security%20Policy%202021%20Final.pdf

2. **Ministry of Information Technology and Telecommunication (MoITT).** (2023). CERT Rules 2023. Retrieved from https://moitt.gov.pk/Detail/MTBmMGQ3NDItOWM2MI00N2M0LWE1ZGUtMjRlNWJlOGYwZGU0