15 Elemental Cyber Defense Controls for Micro, Small, and Medium Enterprises (MSMEs)

Indian Computer Emergency Response Team (CERT-In)

Ministry of Electronics and Information Technology

Government of India

Version 1.0 Dated 01.09.2025

Contents

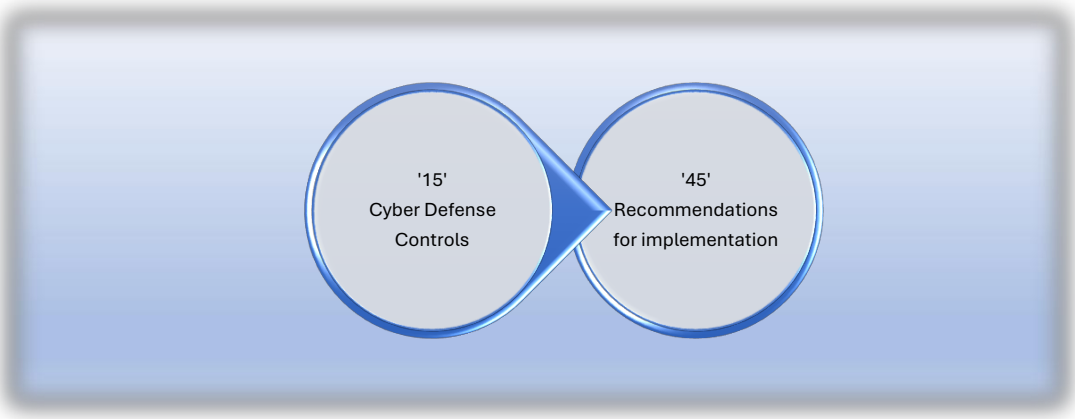
1. Introduction

To safeguard Cyber Infrastructure, confidential data, adhere to legal requirements, reduce financial risk, maintain customer confidence, guarantee operational continuity, gain a competitive advantage, support digital projects, and sustain business growth in an increasingly digital environment, cybersecurity is essential for Micro, Small, and Medium Enterprises (MSMEs) in India.

This document containing 15 Elemental Controls of Cyber Defense has been issued for MSMEs by Indian Computer Emergency Response Team (CERT-In).

This document is applicable to Micro, Small & Medium Enterprises (MSMEs) which are covered as per the criteria for classification of micro, small and medium enterprises, notified by Ministry of Micro, Small & Medium Enterprises, Government of India vide notification no. 2020 S.O. 1702(E) dated 1st June 2020 in exercise of the powers conferred by sub-section (1) read with sub-section (9) of section 7 of the 'Micro, Small and Medium Enterprises Development Act, 2006

Organizations may protect themselves from the most prevalent type of cyberattacks from the Internet by implementing the mentioned Cyber Defense Controls. These are the cyber security baseline criteria that give organizations the chance to benchmark against a minimal set of cyber security controls and assist them in choosing where to start when developing a cyber-security program. Organizations can begin their road towards adopting a comprehensive cyber security framework by utilizing a minimum set of cyber security measures.



2. Utilization of this document

A. For MSMEs:

i. MSMEs may use the 45 security baseline recommendations mapped to the 15 Elemental Cyber Defense Controls to strengthen their cybersecurity posture and conduct self-assessments to gauge their current level of preparedness.

ii. MSMEs may conduct Baseline Audits through CERT-In Empaneled Auditing Organizations for these elemental controls at least once in a year.

iii. This document, outlining Elemental cyber defense controls, can be integrated into the organization's cybersecurity policy to enhance security measures and ensure comprehensive protection.

B. For CERT-In Empaneled Auditing organizations:

i. The auditing organizations may utilize this document to evaluate the auditee organizations based on evidences against this cyber security baseline criterion. Auditing Organizations should clearly mention and educate that this is minimum requirements against which audit was performed.

3. Disclaimer

This Cybersecurity Baseline Document provides a minimum set of security controls recommended for Micro, Small and Medium Enterprises (MSMEs) to establish a foundational level of cybersecurity. It serves as a starting point to help MSMEs implement essential security measures and move toward a more robust security posture.

However, cybersecurity threats are constantly evolving, and each organization faces unique risks based on its industry, size, infrastructure, and data sensitivity. Therefore, MSMEs must go beyond these baseline controls and implement additional security measures based on their specific risk assessments and operational needs.

MSMEs should regularly review, update, and strengthen their cybersecurity practices in alignment with emerging threats, industry standards, and regulatory requirements. Seeking professional cybersecurity guidance is encouraged for a more tailored and comprehensive security strategy.

By using this document, MSMEs acknowledge that cybersecurity is an ongoing process, and they are responsible for assessing and implementing appropriate security measures beyond this baseline.

4. Cyber Defense Controls and Security Baseline Recommendations for Implementation

S. No	Elemental Cyber Defense Controls	Objective	Identifier	Security Baseline Recommendations for Implementation
1	Effective Asset Management (EAM)	Establish and maintain an efficient asset management framework and enhance ability to track, monitor, and optimize the utilization of both physical and digital assets.	EAM.1	Establish and maintain a centralized, continuously updated inventory of all hardware, software, and information assets, with proper identification, labeling, and classification of sensitive assets to ensure appropriate handling and access control.
			EAM.2	Track the full asset lifecycle- from acquisition through deployment, use, and secure disposal- updating records for any change in location, status, or condition.
2	Network and Email Security (NES)	To safeguard networks and email systems against unauthorized access, data breaches, and cyber threats through secure communication.	NES.1	Deploy firewalls at the network perimeter and enable Host-based firewall. Ensure firewalls are properly configured.
			NES.2	Ensure secure wireless connectivity by configuring Wi-Fi networks with WPA2/WPA3 encryption, strong passwords, and hidden SSIDs; avoid factory-default credentials and segregate guest networks from internal systems. Additionally, prevent endpoints from auto-connecting to open or public Wi-Fi and enforce secure wireless configurations across all devices.
			NES.3	Implement VPNs with encryption and MFA to secure remote access and protect remote work environments.
			NES.4	Protect email and messaging systems from phishing and spoofing using SPF, DKIM, DMARC.
3	Endpoint & Mobile Security (EMS)	To safeguard end-user devices by enforcing security policies and practices that ensure secure access, data protection, and resilience against threats.	EMS.1	Install antivirus or endpoint protection software on all devices, using only licensed versions to ensure vendor support and regular updates. Do not disable built-in operating system security features (e.g., Windows Defender, Windows Firewall).
			EMS.2	Avoid pirated or unauthorized software to reduce legal and security risks, and restrict software installation to authorized personnel only.
			EMS.3	Onboard with CERT-In's Cyber Swachhta Kendra (CSK) (Botnet Cleaning and Malware

S. No	Elemental Cyber Defense Controls	Objective	Identifier	Security Baseline Recommendations for Implementation
				Analysis Centre) to receive alert & advisory on Malware & Botnet infection.
			EMS.4	Restrict or control USB and removable media usage, and consider disabling autorun features to prevent malware spread.
4	Secure Configurations (SC)	Implement and manage secure configuration of hardware and software installed within the network. Implement strict configuration rules and change control/approval process.	SC.1	Implement and maintain baseline security configurations for Server & Endpoint operating systems, network devices, browsers, and and commercial off-the-shelf (COTS) software, based on configurations approved by the entity.
			SC.2	Disable unnecessary features, ports, services, protocols, and default applications to reduce the attack surface.
			SC.3	Remove unused software and system functions, and change all default passwords and settings before deployment.
5	Patch Management (PM)	To reduce security vulnerabilities by systematically identifying, testing, and applying patches and updates to software, systems, and devices in a timely manner.	PM.1	Regularly apply security patches and updates to operating systems, applications, and firmware.
			PM.2	Monitor vendor notifications and security advisories, CERT-In advisories and other relevant sources to remain informed about the latest patches and vulnerabilities affecting your IT environment.
6	Incident Management (IM)	To ensure timely detection, reporting, response, and recovery from cybersecurity incidents through a structured and coordinated incident management process.	IM.1	Develop and document a formal Incident Response Plan (IRP) covering reporting, containment, investigation, recovery, and communication procedures.
			IM.2	Conduct regular testing of the Incident Response Plan (IRP) to ensure its effectiveness and readiness during actual incidents.
			IM.3	Adhere to Directions under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet which are published on CERT-In's website. Including Report cybersecurity incidents to CERT-In within 6 hours of detection or notification.
7		Implementing continuous logging and	LM.1	Enable comprehensive logging on all key ICT systems to ensure traceability and

S. No	Elemental Cyber Defense Controls	Objective	Identifier	Security Baseline Recommendations for Implementation
	Logging and Monitoring (LM)	monitoring of systems, networks, and user activities, ensuring timely alerts and auditability.		accountability, and retain system and application logs for a minimum of 180 days with secure storage within Indian jurisdiction.
			LM.2	Continuously monitor network activity and privileged user actions to detect suspicious behavior and unauthorized access attempts.
			LM.3	It is recommended to deploy monitoring security solutions to enhance log analysis, threat detection, and response.
8	Awareness and Training (AT)	To enhance cybersecurity posture by educating personnel on security policies, risks, and best practices through regular awareness programs and role-based training.	AT.1	Conduct basic cybersecurity awareness training at least twice a year for all employees and contractors, covering key topics such as phishing, password hygiene, social engineering, BYOD risks, safe internet usage, acceptable use policies, handling of sensitive/classified information, and responsible email practices.
			AT.2	Actively participate in cybersecurity awareness workshops, capacity-building programs, and national-level cybersecurity exercises and drills conducted by CERT-In to enhance preparedness and strengthen organizational response capabilities.
9	Third Party Risk Management (TPRM)	To protect organization from potential vulnerabilities introduced by external service providers.	TPRM.1	Conduct thorough due diligence for each vendor or third party based on potential business impact or likelihood of compromise.
			TPRM.2	Hold all third-party providers to the same security standards applied internally (at minimum, as per this baseline), ensuring consistency and resilience across the entire supply chain.
10	Data Protection, Backup and Recovery (DPBP)	To ensure the confidentiality, integrity, and availability of data by implementing robust protection measures, maintaining regular and secure backups, and establishing effective recovery mechanisms to restore data and services in the event of	DPBP.1	Establish a regular backup schedule (e.g., daily or weekly) and store encrypted backup copies in secure, other network sites—combining offsite, and offline (e.g., USB or tape).
			DPBP.2	Test backup restoration procedures periodically to ensure data recoverability and system resilience.
			DPBP.3	Develop and maintain a minimum Business Continuity Plan (BCP) for identified critical applications to ensure timely recovery and continuity of operations.

S. No	Elemental Cyber Defense Controls	Objective	Identifier	Security Baseline Recommendations for Implementation
		loss, corruption, or cyber incidents.	DPBP.4	Ensure secure disposal of both physical and digital media using proper sanitization or destruction methods.
11	Governance and Compliance (GC)	To ensure accountability and compliance with cybersecurity policies, regulations, and standards through defined responsibilities, oversight, and regular reviews.	GC.1	Assign a security incharge/Single POC to oversee all information security activities and serve as the primary point of contact for CERT-In and regulators.
			GC.2	Establish and formally approve an Information Security Policy tailored to the organization's scale and operations, covering data protection, access control, incident response, password policies, third-party management, and audits.
			GC.3	Periodically review and update security policies to reflect major business, technological, or regulatory changes.
			GC.4	Adhere to guidelines and directions issued by CERT-In and regulators.
12	Robust Password Policy (RPP)	Strengthen passwords to protect sensitive data from unauthorized access.	RPP.1	Enforce the use of strong, unique passwords across all systems, requiring a minimum of 8 to 12 characters with a mix of uppercase and lowercase letters, numbers, and special characters. Set password expiry intervals and restrict password reuse; educate users against sharing credentials.
			RPP.2	Temporarily lock accounts after 3 to 5 failed login attempts to prevent brute force attacks.
			RPP.3	Enable Multi-Factor Authentication (MFA) for all critical systems, administrative accounts, and remote access tools.
			RPP.4	Use secure encryption and hashing algorithms to store passwords safely.
13	Access Control and Identity Management (ACIM)	To ensure that only authorized users and systems can access resources based on defined roles and privileges	ACIM.1	Assign unique user IDs to all individuals to avoid shared accounts and ensure full traceability of system activity.
			ACIM.2	Implement role-based access controls aligned with defined job responsibilities, following the principle of least privilege.
			ACIM.3	Review and update user access privileges periodically at least quarterly or immediately upon role changes, transfers, or employee exits, using a formal offboarding checklist.
			ACIM.4	Grant administrative privileges only when essential, and enforce segregation of duties

S. No	Elemental Cyber Defense Controls	Objective	Identifier	Security Baseline Recommendations for Implementation
				across administrative, financial, and data functions.
14	Physical Security (PS)	To prevent unauthorized physical access to critical infrastructure, systems, and data	PS.1	Implement robust physical access controls for critical infrastructure and systems. Use security guards, electronic badges, and biometric access for server rooms, network equipment, and other sensitive areas. Monitor entry and exit using CCTV.
			PS.2	Maintain a comprehensive asset-return checklist (ID cards, laptops, USB drives, and other equipment) for every employee exit to prevent data loss and asset leakage.
15	Vulnerability Audits and Assessments (VAA)	To evaluate an organization's security posture, policies, and practices to ensure they effectively protect against threats and vulnerabilities.	VAA.1	Ensure that independent third-party vulnerability assessments of business-critical assets and applications are conducted at least once a year, and establish effective remediation strategies to address identified vulnerabilities in a timely manner.
			VAA.2	Perform periodic risk assessments to identify organization-specific threats and guide mitigation strategies.

5. Acknowledgement

Micro, Small, and Medium Enterprises (MSMEs) form the backbone of the Indian economy, contributing significantly to employment, innovation, and GDP. As key enablers in national and global supply chains, MSMEs increasingly rely on digital infrastructure — making them critical targets for cyber threats. Strengthening their cybersecurity posture is essential for ensuring resilient and secure digital ecosystems across sectors.

With this vital context, The Indian Computer Emergency Response Team (CERT-In) acknowledges the valuable contributions and insights provided by the following experts during the review and development of the document on Cyber Defense Controls and Recommendations for Micro, Small, and Medium Enterprises (MSMEs).

1. Dr. Shekhar Pawar, SecureClaw and Inventor of "Business Domain Specific Least Cybersecurity Controls Implementation (BDSLCCI)" Framework
2. Mr. Salil Kapoor, Netrika Consulting
3. Mr. Santosh Desai, Allied Boston
4. Mr. Vikram Taneja, CyberSRC Consultancy
5. Mr. Apurva Krishna Malviya, Panacea Infosec Pvt. Ltd
6. Mr. Sheltan T T, Xiotz Private Limited