CleanMax™
POWERING SUSTAINABILITY

Clean Max Enviro Energy Solutions Limited

Cyber Security Policy

June 2025

Copyright ©2026. All Rights Reserved. Clean Max Enviro Energy Solutions Limited.

Document Control

A. Document Identification

Code	Name	Type
	Cyber Security	Policy

B. Roles and Responsibilities

Name	Title	Role[1]
Vishal Sangewar	Assistant General Manager	Author
Sweta Sajnani	Chief People & Culture Officer	Reviser
		Owner

C. Versions and History

Version	Date	Author(s)	Summary of Changes
1.0	14th June 2023	Vishal Sangewar	First Draft
1.1	17th June 2025	Sameer Patil	- Updated role for cybersecurity specialist - Changed formatting

D. Approval and sign off.

Name	Title	Status	Date
Deepak Singh	IT – DGM		

E. Status and Classification

Version	Date	Status[2]	Classification[3]	Next Revision

1 Role: Author, Reviser, Advisor, Owner
2 Status: Draft, Approved, Published, Revised
3 Classification: IT Only, Internal Use, Public

Copyright ©2026. All Rights Reserved. Clean Max Enviro Energy Solutions Limited.

Contents

Copyright ©2026. All Rights Reserved. Clean Max Enviro Energy Solutions Limited.

Copyright ©2026. All Rights Reserved. Clean Max Enviro Energy Solutions Limited.

1 Purpose

The purpose of this policy is to define and establish controls and principles for initiating, implementing, maintaining, and improving the Cyber Security program at Clean Max Enviro Energy Solutions Ltd. and all the entities of Clean Max Enviro Energy Solutions Ltd. hereinafter collectively referred to as 'CMES.'.

This policy and its supporting standards are developed to:

- Provide management direction to all CMES employees and to contractors, suppliers,third-party vendors working at CMES or accessing CMES assets.
- Protect the Information Technology/ Operational Technology (IT/ OT) assets within CMES against consequences of breaches of confidentiality, failures of integrity and/or interruptions to its availability.

2 Scope

This policy applies to all personnel across CMES with access to IT/ OT environments. Environments include information resources, computing systems, IT/ OT infrastructure, and other technical assets managed by CMES. Personnel include all the employees, non-full-time employees and consultants and contractors etc. of CMES. And all the renewable energy entity(s) in India in which CMES has direct or indirect investments and all their controlled subsidiaries.

The tools and technologies mentioned in the policy will be deployed as per the Cybersecurity roadmap.

3 Audience

This document is intended to be used by the Assistant General Manager/IT Head, Assistant Manager- IT, and Cyber Security Specialist or any other personnel, as deemed appropriate by the management for implementation of CMES' cyber security program. This document shall also be referred to by all CMES employees, contractors, and third-party vendors to understand their roles and responsibilities to be compliant with this policy and its supporting standards.

4 Cyber Security Governance

Cybersecurity is an integral part of governance and consists of the company's leadership, organizational structures and processes that safeguard CMES information, its operations, and its reputation. CMES will maintain a management system and governance structure for the oversight of the company's IT/ OT security policies and guidelines. Furthermore, CMES will ensure that effective preventative measures and response to cyber security incidents are implemented. It is the management's responsibility to periodically review the company's approach to IT/ OT security and its corresponding policies. The management roles and responsibilities are:

Copyright ©2026. All Rights Reserved. Clean Max Enviro Energy Solutions Limited.

Role	Responsibility
Assistant General Manager/IT Head	• Sponsoring the development and implementation of a cybersecurity strategy and policy framework which will ensure IT/ OT environments are secured against threats that can impact the availability of CMES' assets. • Approving cybersecurity initiatives. • Communicating the policy framework. • Approval and management of policy exceptions.
Assistant Manager - IT	• The Assistant Manager-IT is accountable for the implementation of cyber security activities and initiatives which will ensure IT/ OT systems are secured against rapidly evolving threats that can impact the availability of the same. • Securing CMES' Systems, services, and network. • Communicating and soliciting input on the policy, and the creation of any required supplementary policies and standards. • Responsible for governance of CMES's cyber program, providin guidance, establishing, and maintaining security policies an guidelines as well as implementing and enforcing this policy fo the organization.
Cyber Security Specialist	• Review and update the Cybersecurity policy • The Cyber Security Specialist in consultation with the IT Head is responsible for the operation and implementation of systems according to relevant business requirements, IT/ OT security policies, standards, and procedures. • Managing the incident response, business continuity and disaster recovery as well as informing IT Head of any security violations or abnormal activity. • Serving as the point of contact for any cybersecurity related incident, implementing and maintaining cybersecurity policy documents, overall security of all IT/ OT assets, operations and remediating risks and vulnerabilities. • Acting as a liaison between operators, vendors, and CMES management on matters relating to cyber security. • Reporting to the management about the status of the OT cyber security governance program, OT security related risks, or OT cybersecurity incidents via reports.

5 Applicable Laws and Regulations

CMES, being a renewable energy generation company, is obligated to follow the CEA (Cyber Security in Power Sector) Guidelines, 2021 and NCIIPC (National Critical Information Infrastructure Protection Centre) Guidelines.

Copyright ©2026. All Rights Reserved. Clean Max Enviro Energy Solutions Limited.

6 Policy Review and Compliance

Key performance indicators (KPIs) shall be defined and measured to ensure compliance with this policy and continuous improvement of cyber security program at CMES. All policies and supporting standards/ frameworks shall be reviewed at regular intervals of time (at least once annually) or after any significant changes in CMES' Business strategy, regulatory requirements, or legal requirements.

7 Exceptions to the Policy

Where there is a justifiable business need that requires actions to be performed which are in conflict to this document, such exceptions shall be reported to the management team alongwith risk and approval obtained. Such approvals shall be valid for a pre-defined period mentioned in the exception form/ request, after which it shall be re-evaluated and re-approved.

8 Cyber Risk Management

8.1 Scope

- Cyber Risk Management policy applies to:
  - CMES information assets
  - Business environments
  - Business processes
  - Business applications
  - Information systems and networks that support business processes.
  - CMES OT assets and network

8.2 Policy Statements

- CMES shall perform a risk assessment as per its defined Cyber Risk Management Framework annually for the following:
  - CMES information assets
  - Business processes
  - Business applications
  - Information systems and networks that support business processes.
  - CMES OT assets and networks

- CMES shall perform a risk assessment prior to the following:
  - Significant changes throughout the organization
  - Onboarding a new vendor (e.g., outsourcing, using a cloud service provider (CSP),etc.)
  - Procuring of a new technology/ application
  - Initiating a new project which involves usage of CMES' Critical information.
  - Allowing access to critical assets of CMES by external vendors and third-party service providers
  - Exception to any CMES approved policy or procedure.

- The cyber risk management process shall be implemented in accordance with the Cyber Risk

Copyright ©2026. All Rights Reserved. Clean Max Enviro Energy Solutions Limited.

Management Framework and shall include the following steps at a high level:

- Identifying the cyber security risks
- Maintaining a consolidated risk register collating all the identified cyber risks
- Post consultation with the relevant business and support functions, analyzing the cost and effort to implement controls to act on the identified risks.
- Monitoring of implemented security controls to evaluate its efficiency and adequacy.

Results from the risk assessments conducted across CMES shall be reported to the executive management who in turn would help determine programs of work in consultation with the relevant business owners to perform remedial actions.

- CMES shall define and apply a risk treatment process by selecting an appropriate risk treatment option as per its Cyber Risk Management Framework.
- A risk treatment plan shall be documented and further communicated to the respective business owner and signed off from an authorized executive management representative.
- Reviews shall be conducted bi-annually to evaluate the adequacy of mitigating controls, residual risk, and acceptable level of risks.
- Implemented controls shall be monitored and tested for evaluating its effectiveness.

9 Acceptable Usage

Please refer to CMES' Acceptable Usage Policy.

10 Human Resources (HR) Security

10.1 Scope

Human Resources Security policy is applicable to all individuals having access to CMES Information systems which include but is not limited to employees and third-party personnel.

Copyright ©2026. All Rights Reserved. Clean Max Enviro Energy Solutions Limited.

10.2 Policy Statements

10.2.1 During Recruitment

- Background verification checks shall be performed during recruitment of employees or engagement of staff on a contract basis who have access to critical information systems and assets of CMES.
- CMES shall ensure that all employees and third-party personnel are made aware of their responsibilities towards information security.
- Terms and conditions of employment shall:
  - State that information security responsibilities extend outside normal working hours and premises and continue after employment has ended.
  - Include a non-disclosure/ confidentiality clause.
- CMES shall ensure that all personal data collected from employees and third-party personnel are kept confidential and are in line with the applicable laws and regulations.

10.2.2 During Employment

- All employees and third-party personnel shall perform their information security responsibilities and comply with CMES' Security requirements.
- All employees and third-party personnel shall be responsible for the protection of any sensitive information and assets assigned to them.
- All employees and third-party personnel shall use information processing systems and data residing on systems for authorized business purposes only.
- All employees and third-party personnel shall report any suspected information security incidents or weaknesses to his/ her reporting manager and the cyber security specialist.
- Relevant cyber security awareness and training sessions (upon hire as part of induction and subsequently on a regular basis) shall be conducted for all employees of CMES and, where required, third-party personnel who shall have access to CMES email.
- Any employee or third-party personnel found violating CMES Cyber Security Policy shall be subjected to disciplinary actions.
- The organization shall ensure screening processes are done for personnel who will have access to critical OT assets and network.

10.2.3 Termination or Change of Employment

- Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or third-party personnel, and enforced.
- All physical and logical access privileges shall be revoked within defined timelines when an authorized user no longer requires access to information or systems as part of their job, or when they leave CMES.
- Upon termination of employment, employees and third-party personnel shall
  - Return assets that belong to CMES.
  - Confirm the destruction of all copies of information owned by CMES that they Possess.
- The activities performed by employee or third-party personnel may be subject to additional monitoring at the time of termination or change of employment, on communication from respective business function representative.

Copyright ©2026. All Rights Reserved. Clean Max Enviro Energy Solutions Limited.

11 Asset Management

11.1 Scope

Asset Management policy applies to all information (IT) and Operational (OT) systems being used by CMES which includes but is not limited to the following:

- Software assets (applications, software licenses, etc.)
- Physical assets (computing and support infrastructure)
- Information assets – digital
- Information assets non-digital

This policy applies to all users such as employees, contractors and third parties accessing CMES' Information assets.

11.2 Policy Statements

11.2.1 Asset Ownership and Inventory

- CMES shall ensure that all its information assets have:
  - An asset owner who understands the nature of the asset, for which they are responsible, its appropriate usage and protection.
  - Criticality rating of the asset.
- All information assets shall be appropriately identified, classified, and maintained in an information asset inventory.
- Data repositories located on service provider hosted premises including cloud computing environments are to be included in the inventory.
- An asset inventory shall contain the following details at a minimum, the asset type, asset location, owner, custodians, criticality rating and name of the function/ processes that use those assets.
- Asset reconciliation and verification of assigned criticality rating shall be performed on **bi-annual** basis.

11.2.2 Information Classification and Handling

- CMES shall define and document an information classification scheme which shall be in line to the categories mentioned in Appendix A of this document.
- The information classification scheme shall be used to determine an appropriate level of protection for the information asset.
- CMES shall follow procedures on how to handle, store, and transport organization information by taking into consideration its classification category.

11.2.3 Asset Maintenance

- CMES shall maintain an up-to-date list of information assets (where applicable) that are covered under the Warranty/ Annual Maintenance Contract (AMC).
- The list of assets shall be updated as required. All information assets shall be maintained

Copyright ©2026. All Rights Reserved. Clean Max Enviro Energy Solutions Limited.

as per the maintenance contracts.

- CMES shall perform periodic review to monitor if Warranty/ AMC of any information asset is about to expire. AMC shall be renewed based on necessary approvals.
- CMES shall ensure that all information assets are tracked throughout the asset lifecycle.

11.2.4 Asset Retention and Disposal

- All information assets shall be disposed securely and made unrecoverable when no longer required.
- The information assets that must be retained for business purposes or to comply with judicial or regulatory requirements shall be retained in accordance with section 13.2.5 (i.e., Data Retention and Disposal) of this policy.
- The information classification category shall be considered while determining the disposal method for the respective asset.
- Any IT or OT asset that needs to be decommissioned shall be sanitized of all data, as per the manufacturer guidelines.
- Prior to disposal of system devices like Hard Drives, Random Access Memory (RAMs), etc., the same shall be sanitized by use of techniques like degaussing, low-level formatting, or physical destruction to ensure that data cannot be reconstructed.
- CMES shall maintain a record of all its disposed/ decommissioned assets.

11.2.5 Media Handling

- CMES media shall be adequately protected and safeguarded against unauthorized access, misuse, or corruption during transit or transfer.
- All media movements inside or out of CMES premises, shall be logged and approved by an authorized individual.
- Additional controls (such as use of encryption, locked containers, and tamper-evident packaging) shall be implemented to protect media containing CMES Information classified as 'Confidential' and/ or 'Sensitive'.
- With respect to laptops and mobile devices provided to users, CMES'Acceptable UsagePolicy shall be followed by the users and further he/ she shall be responsible for handlingthe information asset in a secure manner.
- Use of removable media shall not be allowed. Any request for removable media allocation shall be treated as an exception and provided only for valid business requirements and post approval from an authorized individual.
- All removable media shall be scanned for viruses and malwares before connecting to CMES' Information assets.
- Removable media shall be encrypted and protected during transit and disposed of in a secure manner when no longer required.

11.2.6 Operational Technology Assets

OT environment shall meet the requirements of clauses mentioned in Sections 11.2.1 to 11.2.5of this document. Additionally, the OT environment should comply with the following rules:

- CMES shall ensure security of OT assets (including redundant components) through regular firmware / software updates and patching, vulnerability management, securing configuration, supplementing security controls.

Copyright ©2026. All Rights Reserved. Clean Max Enviro Energy Solutions Limited.

- CMES shall maintain details of the latest updated version of each firmware and software and the software certification if received from the original equipment manufacturer.
- CMES shall ensure that OT assets will be used for operations they are assigned or authorized to perform.
- The site in charge and operators are responsible for the preservation and correct use of the OT assets they have been assigned.
- CMES shall ensure that physical access to OT assets is permitted to authorized personnel.
- The site in charge and lead SCADA engineer is responsible for maintenance and configuration of the OT devices. Only authorized personnel should be allowed to modify OT asset configurations, including any modification to interfacing hardware or software.
- Usage of security tools on the OT network shall be approved by the IT security team in consultation with the lead SCADA engineer.
- The concept of least privilege must be followed when authorizing access to OT assets.
- Accessing IT devices or internet use from the OT network, or OT assets, unless authorized,is prohibited.
- Use of personal devices to access OT resources is prohibited.

12 Access Control

- The objective of access control is to authenticate and authorize personnel to access CMES' Information.
- Whether on-premises or cloud system, physical or logical, all CMES resources must be protected from unauthorized access, use, alteration, deletion, or destruction.
- System owners and information asset owners are responsible, with the assistance of the IT team, to determine appropriate physical and logical access control rules, rights, and restrictions for assigned assets.
- Access to CMES environments must only be granted to specifically authorized personnel.
- Access to all assets, particularly assets classified as sensitive, must not be granted unless authorized by the system owner or information asset owner. When granting access, only the minimum level of access required for an individual or entity to perform its task will be provisioned. Access that is no longer required must be revoked in a timely manner.
- Please refer *CMES' User Access Management Policy for* detailed information on areas suchas identity management, privileged access management, remote access, application access control, etc.

13 Data Protection and Privacy

13.1 Scope

- Data protection and privacy policy is applicable to all information, IT and OT assets of CMES. Further this policy is also applicable to all users such as employees, contractors and all third-party vendors creating, using, storing, and processing CMES' Data.

13.2 Policy Statements

- CMES shall ensure that all its data, IT and OT assets are protected from unauthorized or accidental access, modification, destruction, or disclosure, as well as from misuse and

Copyright ©2026. All Rights Reserved. Clean Max Enviro Energy Solutions Limited.

abuse.

- While conducting business activities which involve the processing and usage of CMES data, CMES shall ensure that all the confidentiality, integrity and availability of data is maintained.
- CMES shall ensure that all personal data processing and handling is done in accordance with CMES' Data Privacy Policy and other application local regulations.
- Users shall be educated on their roles and responsibilities and made aware of the impact of their actions on data security.
- Awareness of data protection shall be promoted throughout the organization.
- Access to sensitive data must be authorized by the supervisor.
- Data should not be shared informally. When access to sensitive information is required, personnel can request access from the supervisor and should take all necessary steps to prevent unauthorized access.
- The supervisor must immediately be notified in the event a device is lost containing sensitive data (e.g., laptops, USB devices).
- Furthermore, the following sections shall be referred by CMES while implementing its data protection program.

13.2.1 Data creation and classification

- Data shall be classified at the creation stage based on the categories and data types listed in Appendix A and B of this document.
- Information owner shall be responsible to upgrade and downgrade the classification category as per the business needs.
- The assigned classification categories shall be used to determine the necessary data protection controls that need to be leveraged to secure CMES data.

13.2.2 Data at rest/ storage

- CMES shall ensure that the data at rest is protected by implementation of necessary access control and authentication measures.
- CMES shall ensure that the data is encrypted and masked as per section 21 (i.e., Cryptography Policy) of this document.
- Data shall only be stored on CMES approved information storage systems. Furthermore, CMES should have a well-maintained asset inventory of all its information systems whichare used for storage of critical data.
- Data stored and processed by cloud services, shall be protected by encrypting sensitive and confidential data using the default encryption solution provided by the cloud service provider.
- Portable or removable storage devices should be protected by using encrypting techniques (e.g., using encryption software installed on the device, or using file-encryption software on the computing device to which the portable storage device connects).
- CMES shall ensure that the physical copies of data should be stored in a secure location when not in use.
- Personnel should ensure physical copies of sensitive data are not left unattended (e.g., on a printer or a desk).

13.2.3 Data in transit

- CMES shall ensure that information transmitted outside of CMES networks, including the

Copyright ©2026. All Rights Reserved. Clean Max Enviro Energy Solutions Limited.

internet shall be encrypted or sent via secured channels.

- CMES shall identify and document appropriate security standards to be followed for in-transit confidentiality protection based on the communication protocol used in their system.
- CMES shall ensure that data that shared in a physical format is appropriately labelled (asper Appendix A), sealed and protected while in transit.

13.2.4 Data Security Solution

- Data Security Solution (e.g., Data Loss Prevention (DLP), Information Rights Management (IRM), etc.) should be used to identify specific types of sensitive data, monitor channels of data leakage, and take actions accordingly to prevent any data loss.
- Data Security Solution should be configured to monitor and control the flow of sensitive data using the in-built technical policies, defining:
    - what data can and cannot be sent, posted, uploaded, moved, or copied and pasted.
    - where the data can be transmitted
    - who can send and receive data (such as email)
    - how can data be shared.
- A register of keywords, electronic document characteristic and specific types of sensitive information shall be identified, and the data security solution shall be configured against the same.
- Data security solution should be configured to monitor data leakage channels where sensitive data is in motion (e.g., data traversing a network such as internet), in use (e.g., data processed on endpoints) or at rest (e.g., data stored in file systems, databases, cloudor end points).

13.2.5 Data retention and disposal

- Data retention period shall be defined, and records shall be retained for the defined period. Retention periods shall define and reviewed at least once in a year based on the following:
    - CMES's business requirements
    - Legal or regulatory compliances
    - Contractual obligations
- Records shall be maintained in a safe and secure environment to prevent unauthorized access and tampering.
- Storage media like floppy disk, hard drives, Compact Disks (CDs), tapes, SSD, Thumb drives, mobile devices etc. shall be erased using a degaussing device or "disk-wiping" software before being discarded.
- If the data cannot be erased, then media shall be physically destroyed in such a way that data should be beyond retrieval.
- Physical copies of sensitive data should be shredded or disposed in a secure manner when no longer required.

14 Physical and Environmental Security

14.1 Scope

Physical and Environmental Security policy applies to all assets of CMES which includes.

- Employees, third-party personnel, and visitors accessing CMES facilities.
- Information processing and operations facilities.

Copyright ©2026. All Rights Reserved. Clean Max Enviro Energy Solutions Limited.

- Infrastructure such as building premises, equipment, physical documents, and otherelectro-mechanical installations.

14.2 Policy Statements

14.2.1 Physical Security

- Physical access controls shall be implemented and physical access to offices, information processing facilities and shall be effectively controlled for employees, third-party personnel, and visitors to prevent unauthorized access or damage to information systems.
- Physical access provided to secure areas such as the data centers, network rooms, server rooms, disaster recovery sites, etc. to employees/ vendors/ visitors shall be reviewed on a regular basis.
- Facilities shall be classified into zones and physical safeguards for each zone shall be designed and implemented at a level appropriate to the classification of the zone.
- CCTV cameras shall be installed at key locations of CMES premises.
- Offices and information processing facilities shall have a manned reception area to control physical access to the premises.
- Entry and exit to CMES premises shall be logged and monitored. These records must be reviewed periodically. In case of any major deviations/ suspected events noted, the same shall be notified to appropriate authorities.
- Visitor details shall be verified and entered in a visitor register/ visitor management system. Details regarding laptops, pen drives, CDs/ DVDs, etc. shall also be entered.
- Every visitor shall be provided with a visitor badge and the visitor shall always display the badge within the CMES premises.
- Visitors/ vendors/ third-party personnel shall be always escorted inside the CMES facilities housing critical information systems or equipment.
- Monitoring events and physical access records shall be stored for a duration based on business and legal requirements.
- Unauthorized removal of any company documentation, equipment, or media from thefacility is restricted, unless permitted by an authorized individual.
- All activities of visitors, contractors, and maintenance personnel will be subject to monitoring while onsite.

14.2.2 Equipment Security

- Equipment shall be secured from potential threats to prevent loss, damage, theft, or compromise.
- All cables, including power and telecommunication network cables, shall be protected from damage or interception.
- Physical access to networking equipment, wireless access points, telecommunication lines, OT assets and network, and cabling racks/ distribution points shall be restricted.
- Loading and unloading areas shall be isolated, kept away from information resources and monitored.
- All incoming equipment shall be inspected for hazardous and combustible materials at entry points to ensure the same is not allowed inside CMES premises.

14.2.3 Environment Security

HVAC systems shall be installed to support information systems and equipment in server rooms,

Copyright ©2026. All Rights Reserved. Clean Max Enviro Energy Solutions Limited.

network rooms, OT command and control center, inverter room, and disaster recovery sites.
Smoke detectors, fire alarms, fire detection and fire suppression equipment shall be installed in CMES premises for protection against any fire incidents.
CMES shall conduct fire drills, emergency evacuation drills and necessary trainings for allemployees on a regular basis to ensure readiness in case of any emergency.
Uninterruptible power supply (UPS) systems and generators shall be installed to support controlled shutdown or continued functioning of equipment supporting critical business operations.
Critical information systems, storage media, document and assets shall not be in areas susceptible to water seepage or flooding, or near combustible materials.
A preventive maintenance exercise for all utility equipment shall be carried out at regular intervals to ensure their continued availability and integrity.

15 Operational Security

15.1 Scope

Operational Security policy shall apply to all CMES'Information systems, as mentioned butnot limited to:

- Network Devices (routers, switches, etc.)
- Network Security Tools (firewalls, Antivirus, DLP, etc.)
- Operating Systems
- Applications
- Databases
- Virtual Machines
- OT Devices and infrastructure (*Section 15.2.4.2 (i.e., Mobile Device Management) of this document shall not be applicable*)

15.2 Policy Statements

15.2.1 Patch Management

- CMES shall define a patch management process and implement a centralized patch management system to monitor and implement the patching across all information systems. Centralized patch management solution shall ensure that the patches are deployed across information systems as soon as they are available.
- Operating systems without Original Equipment Manager (OEM) support must not be connected to the CMES network or used to process CMES information.
- CMES shall ensure that all vulnerabilities observed shall be remediated/patched as per the timelines defined in Appendix D of this document.
- CMES shall monitor updates received from providers of software (including application andsystem software such as operating systems and databases) for software 'patches' made available to remove security vulnerabilities.
- CMES shall ensure that scenarios wherein the security patches are not installed due to a business requirement are treated as an exception and handled with compensating security controls.
- CMES should implement a systematic, accountable, and documented OT patch management process for managing exposure to vulnerabilities.
- CMES shall separate the process for OT patch management from the automated process fornon-OT

Copyright ©2026. All Rights Reserved. Clean Max Enviro Energy Solutions Limited.

applications. Patching should be deployed during planned OT outages.

Patch Schedule: -

System/Application	Schedule	Patch Details
Laptops/Desktops	All Day/ During Availability	Windows Only (Critical and Security Updates)
Servers	Friday, Saturday, or Sunday (Third week of every Month)	Windows Only (Critical and Security Updates)

15.2.2 Change Management

A change management process shall be documented and established that shall at leastinclude types of changes, recording of changes, business and security approvals, impact assessment due to the change, testing the change, roll back procedures and post implementation review of changes.

- All change requests raised shall be classified, prioritized, and assessed for impact to information security.
- Changes to system components shall be adequately controlled and shall be carried out only after changes are validated, documented, and approved by authorized individuals.
- All changes shall be tested in accordance with the defined test plan in the test environment,prior to release to production environment.
- CMES shall migrate all changes to the production environment in a controlled manner post approval from authorized personnel.
- CMES shall perform post implementation review of the change to ensure that the desired objectives are achieved.
- Emergency changes shall be exempted from following the defined change management process with a valid business justification.
- CMES shall document and obtain post facto approvals for all emergency changes carriedout.
- A formal change management program shall be established at the site level.
- The risk assessment shall be performed whenever there is a significant change or upgrade tothe OT network that could affect safety, environment, and security, including configuration changes, the addition of network components, and the installation of software.
- After implementation of changes respective documents shall be updated to reflect the current state.

15.2.3 Backup and Restoration

- CMES shall identify the backup requirements for information systems based on the criticality of the data, impact on the operation and business, business continuity metrics(such as RTO, RPO, etc.), applicable legal/ regulatory requirements as a part of its Data Backup and Restoration Standard.
- The Data Backup and Restoration Standard shall clearly specify the backup and restoration timelines for its information systems.
- CMES shall ensure that only official CMES data is backed up. Backups shall be performed only on CMES approved sites. (For e.g., user data backup on endpoints such as laptops, desktops shall be done on OneDrive).

Copyright ©2026. All Rights Reserved. Clean Max Enviro Energy Solutions Limited.

- CMES shall maintain appropriate backup logs and conduct periodic backup restoration tests.
- CMES shall ensure measures for secure storage and transit of the backup tapes.
- CMES shall ensure that the backup copies are stored in a separate facility or in a fire rated container. Further, all data backup transfer to alternate storage sites should be done either electronically or by the physical shipment of storage media.

  - Endpoint Management

15.2.3.1 Endpoint Protection

- All information systems and access points connecting to the CMES network shall be protected against malicious activities (such as viruses, malware, spyware, adware,ransomware, etc.).
- CMES shall implement adequate endpoint protection controls and solutions on all its systems to detect, contain and eradicate malicious code. The endpoint solutions shall include the following at a minimum:
  - Endpoint antivirus solutions
  - Endpoint detection and response (EDR) solutions
  - Content filtering for web browsing
  - Firewall, intrusion-detection systems/intrusion-prevention systems (IDS/IPS)
  - Advanced Persistent Threat (APT) solutions
  - Email scanning
  - Hardening of operating systems
  - Patching of all endpoint protection solutions deployed.
- CMES shall ensure that all malicious file extensions are blocked at the network and emailgateway. Automated scans shall be performed for all email attachments and removable media.
- CMES shall maintain a list of authorized software that can be used within the CMESnetwork. Any software installation outside the list shall only be done on receiving a validbusiness justification and authorized approval against it.
- The IT team at CMES shall ensure that the antivirus solution is configured to conductperiodic scans.
- OEM approved antivirus software shall be configured to scan periodically on all OT workstations at periodic intervals to detect potential virus/malicious code.

15.2.3.2 Mobile Device Management

- The IT team shall implement the mobile device management program at CMES in accordance with CMES' Mobile Device Management Standard.
- CMES shall prohibit the usage of mobile devices for accessing the OT environment.
- User access to CMES environments and information from mobile devices must be provisioned through an established approval process.
- This process should mandate every user to accept the terms and conditions associated with the access through mobile devices, namely CMES' Acceptable Usage Policy.
- Appropriate controls such as authentication, encryption, remote wipe-out, and backups shall be implemented on mobile devices.
- Secure containers shall be created on personal mobile devices to segregate business information from user's personal information.
- Mobile device policies shall only be applied on such secure containers to ensure users personal information is unaffected. For e.g., remote wipe option shall only be configured to delete business information stored on the user's personal mobile device. However, in the event user information is deleted by this remote wipe, CMES shall not be held liable.
- Changes to or termination of user access to CMES environments and information frommobile

Copyright ©2026. All Rights Reserved. Clean Max Enviro Energy Solutions Limited.

devices must be de-provisioned through an established approval process.

- The enrollment process must be documented and auditable to ensure reasonable scrutiny.

15.2.4 Logging and Monitoring

15.2.4.1 Event Logging

- Security logging, monitoring, and reporting capabilities shall be implemented to detect security events within CMES' Network and information assets in accordance with applicable laws, regulations, and industry standards.
- Logs of all critical servers, network devices and system components that support security functions (for example, firewalls, IDS/IPS, authentication servers, etc.) shall be stored, reviewed, and monitored to detect malicious activities.
- Relevant event attributes such as IP address, username, time and date, protocol used, port accessed, method of connection, name of device and object name, etc. shall be capturedin the event entries.
- Security relevant logging shall be always enabled.
- CMES should include relevant OT events (e.g., alerts, alarms, configuration and statuschanges, operator actions) in their event logging.
- Security-related event logs shall be analyzed regularly to help identify anomalies.Anomalies detected shall generate alerts in SIEM (Security information and event management) tool. Various use-cases to be defined in SIEM to detect security eventscovering all possible threat landscapes.
- Security Operations Center (SOC) team shall monitor security alerts generated in the SIEM tool 24x7. Any incident identified or reported shall be handled as per CMES' Cyber Security Incident Response Plan.

15.2.4.2 Protection of logs

- Logs shall be protected against unauthorized access, misuse, and modification. Sufficient storage space shall be allocated based on expected volume of logs.
- Event logs shall be retained as per the data retention and disposal section of this documentand other legal/ regulatory requirements.
- Firewall logs shall be retained and stored for a period of 180 days.

15.2.4.3 Clock Synchronization

- The real time clock of systems shall be set accurately to ensure the accuracy of audit logs,which may be required for investigation or as evidence in legal or disciplinary cases.
- The real time clock of systems and communication devices shall be in sync with central NTP (Network Time Protocol) server. Further there shall be a procedure that checks and corrects drift in the real time clock.

15.2.5 Technical Vulnerability Management

- CMES shall obtain and process the threat and vulnerability information received frominternal and external tools and services, memberships in industry associations and subscriptions to advisories and government and regulatory agency interactions.
- CMES shall analyze and review all potential threats and vulnerabilities and implement application measures.
- CMES shall ensure that Vulnerability Assessment is performed periodically for the below listed systems:
    - Servers (including standalone servers), databases.

Copyright ©2026. All Rights Reserved. Clean Max Enviro Energy Solutions Limited.

- Network Devices (such as router, switches, and other network components).
- Firewalls, perimeter defense systems such as intrusion detection systems (IDS) and intrusion prevention systems (IPS)

- The scope of devices/ systems for which VAPT exercise is to be conducted is defined as partof the "*VAPT Scope Document".*
- CMES shall perform periodic assessments as per Appendix C of this document.
- In addition to this, CMES shall also perform a VA assessment prior to deploying any newserver/ system/ network device within its production environment.
- Use caution when running vulnerability assessment scans against OT networks.
- Prior to initiating any VAPT exercises, following points should be noted:
- The IT team shall ensure back-up of running systems configurations is taken prior to commencement of the exercises.
- The IT team shall highlight any system unavailability that might occur during the exercise and shall only proceed once necessary management approval is obtained.
- All intrusive tests shall be performed during off-peak time.
- Denial of Service of Distributed Denial of Service tests will not be permitted.
- The tester will perform limited exploitations (exploitation without changes tosystem or configuration files) to confirm vulnerabilities.
- Vulnerabilities identified shall be categorized based on the severity level, potential impactto CMES, criticality of the impacted system/asset and compensatory controls in place.
- All the identified vulnerabilities shall be remediated as per the timelines defined in Appendix D of this document. CMES shall ensure that the usage of tools and supporting utilities for performing VAPT is in a controlled manner by authorized and qualified individuals only.
- System utilities (RDP, PowerShell etc.) must remain blocked and be enabled for official purposes only subject to approval from the IT team. Such system utilities must be blocked after use.

15.2.6 Ensuring High Availability

- The systems and component that are critical to operation (workstation, network backbone, critical measurements, PLCs, protection relays, etc. shall be deployed with redundancy.

16 Network and Communications Security

Please refer CMES' Network and Communications Security Policy.

17 System Acquisition, Development and Maintenance

17.1 Scope

System Acquisition, Development and Maintenance Policy is applicable to all informationsystems of CMES.

17.2 Policy Statements

17.2.1 Information Security Requirements, Analysis and Specification

Copyright ©2026. All Rights Reserved. Clean Max Enviro Energy Solutions Limited.

- CMES shall identify and address the security requirements during the requirements gathering and analysis phase of acquisition, development of new systems or enhancements to existing information systems.
- Information security requirements shall be integrated within all CMES project delivery lifecycles and phases.

17.2.2 Secure Development Principles and Environment

- CMES shall develop a secure software development lifecycle (SDLC) process that shall be followed for development of all new systems and any changes to existing systems.
- CMES shall segregate the production, development, and test environments to reduce the risks of unauthorized changes to the production. Adequate segregation of duties needs to be enforced.
- CMES shall review the developed code prior to deployment in production environment. Also, CMES shall perform source code review for its application on annual basis.

17.2.3 System Change Control

- CMES shall ensure that all new changes and major changes to existing systems a formal change management process in accordance with section 15.2.2 (i.e., Change Management) of this document.
- CMES shall manage and control the migration of data to new / upgraded system to ensurethe integrity, completeness, confidentiality, consistency, and continuity of data.

17.2.4 Outsourced Development and Procurement

- All third-party vendor agreements and contracts shall include the cyber security requirements for any system/ product procurement.
- CMES shall ensure that all outsourced systems are free from malwares and vulnerabilities.
- CMES shall either obtain the source code from vendor or enter into a software escrow agreement for critical outsourced applications.
- Contractor and external suppliers that supply the products and services that are critical and high impact shall be approved and added to repository after ensuring that the entity complies with CMES' Security policies.

17.2.5 System Security and Acceptance Testing

- CMES shall document the system acceptance criteria for new developments/ enhancements and perform the testing as per the defined criteria.
- CMES shall ensure that the production test data is sanitized before testing in the test environment.
- CMES shall ensure that test data is protected and controlled in accordance with its level of sensitivity.
- CMES shall perform vulnerability assessment for any new system before deployment in production environment and application security testing at the time of on boarding of the application based on criticality.
- Testing shall be conducted in non-production environment.

17.2.6 System Documentation

- CMES shall acquire and include documentation from the contractor/ third parties on the security controls employed within systems (asset, process, network, software, etc.) that are in their scope.

Copyright ©2026. All Rights Reserved. Clean Max Enviro Energy Solutions Limited.

- The system shall be reviewed and updated periodically for additional controls from contractors, third-party provided components, or services after updates to software/ hardware/ firmware.

17.2.7 Legacy System

- CMES shall develop procedures to periodically evaluate risks associated with legacy systems and handle identified risk.
- CMES shall develop procedure to upgrade its legacy components or systems based on the level of risk tolerance.

17.2.8 System maintenance

- CMES shall schedule, perform, document, review records of maintenance of different components of the system in accordance with maintenance specification and manuals provided by the suppliers, third parties or OEM of those components.
- CMES shall maintain policies to approve personnel authorized to perform maintenance of different components of the system.
- Maintenance personal should only be allowed under supervision of CMES authorized employee.
- CMES shall identify and obtain maintenance support and spare components required for critical system and operations.

18 Incident Management

18.1 Scope

Incident Management policy is applicable to all IT/ OT assets. Further, this policy applies to all users such as employees, contractors and third parties accessing CMES' Information assets.

18.2 Policy Statements

- A formal incident management plan shall be defined and implemented to manage cyber security incidents including but not limited to incident detection, reporting, ownership, classification, investigation, resolution, and closure.
- Security incidents shall be reported from all relevant sources, including users, audit process, SOC, customers, etc.
- Escalation and communication processes and lines shall be established and documented within CMES' Cyber Security Incident Response Plan.
- All reported security events shall be analyzed before being classified as security incidents. Further the IT team shall make necessary changes to the cyber security policies as per the learnings from the incident.
- CMES's shall ensure that all security incidents are logged and categorized according to their severity. The classification shall be done as per the categories defined within CMES' Cyber Security Incident Response Plan.
- CMES's shall ensure that all incidents are reported to the applicable legal/ regulatory, industry bodies, and all other stakeholders who may have to face the implications of the incident.
- The IT team shall verify all reported security incidents for closure and conduct post-incident analysis by reviewing the appropriateness of actions taken for closure.

Copyright ©2026. All Rights Reserved. Clean Max Enviro Energy Solutions Limited.

- CMES shall ensure that significant evidence is collected for conducting necessary investigation. These logs shall be retained for at least a period of 90 days and in accordance with Section 13.2.5 (i.e. Data Retention and Disposal) of this policy.
- The retention timeline shall vary in case it is necessitated by relevant legal or regulatory obligations.
- All security incidents and breaches shall be discussed with senior management on quarterly basis.
- CMES shall ensure that the Cyber Security Incident Response Plan is reviewed at least annually.

19 Business Continuity and Disaster Recovery

19.1 Scope

Business Continuity and Disaster Recovery policy is applicable to all CMES information systems,locations, operating businesses, and service providers.

19.2 Policy Statements

19.2.1 Business Continuity

- Business Impact Analysis (BIA) shall be carried out to identify critical business applications and processes and based on the results of the BIA, CMES shall define and document a business continuity plan. Recovery Time Objectives (RTOs), Recovery Point Objectives (RPOs), Maximum Tolerable Period of Downtime (MTPD) and other business continuity metrics shall be determined for the identified critical business applications and processes.
- Risk assessments shall be carried out at regular intervals of time to identify threats that may cause disruption to the availability of the information systems supporting the business processes and operations.
- CMES shall establish, document, implement and maintain processes and controls to ensure the required level of continuity for information security during an adverse situation.
- CMES shall implement sufficient redundancies for information processing facilities to meet availability requirements.
- CMES shall plan for additional communication redundancies remote operations to ensure uninterrupted operation.
- CMES shall establish cybersecurity incident criteria that trigger the execution of continuityplans communicate to incident response and continuity management team.
- Continuity plans shall address IT, OT, and information assets important to the delivery of the function, including the availability of backup data and replacement, redundant, and spare IT and OT assets.
- The results of continuity plan testing/activation should be compared to recovery objectives, and plans shall be improved accordingly.
- Continuity plans shall be periodically reviewed and updated based on cybersecurity incidents.

19.2.2 Disaster Recovery

- CMES shall develop a disaster recovery plan to ensure efficient recovery and continuity of critical business processes.
- Disaster recovery sites shall be set up to ensure continuity of business in the event of a disaster.
- Disaster recovery drills shall be conducted on a regular basis to verify the effectiveness of

Copyright ©2026. All Rights Reserved. Clean Max Enviro Energy Solutions Limited.

the disaster recovery plan. All records with respect to disaster recovery drills shall be documented and maintained as per CMES requirements.

19.2.3 Testing and Review

Business continuity plan and disaster recovery plan shall be tested and reviewed on a regular basis, and whenever there's a major change in the operating environment. The findings of the review shall be incorporated in the respective plans to make them more efficient.

20 Cloud Security

Please refer CMES' Cloud Security Policy.

21 Cryptography

21.1 Scope

Cryptography policy is applicable to all information and information assets of CMES. Further this policy is also applicable to all users such as employees, contractors and all third-party vendors creating, using, storing, and processing CMES' Data.

21.2 Policy Statements

21.2.1 Use of Cryptography

- CMES shall implement approved and secure encryption algorithms for encryption of information at rest and information in transit, depending on the classification and sensitivityof information.
- Legal and regulatory requirements of cryptographic controls shall be complied with by only using standard publicly released and tested algorithms.

21.2.2 Key Management

- CMES shall ensure security of encryption keys and their backup by implementing access restriction and secure storage mechanisms.
- CMES shall ensure that secure mechanisms are implemented for key generation, issuance, access, distribution, storage, processing, and destruction.

22 Third-Party Management

22.1 Scope

Third-Party Management policy applies to all third parties (e.g., suppliers, vendors,contractors, consultants, OEM partners, service providers).

22.2 Policy Statements

- The information security requirements, supplier obligations, region specific legal, and regulatory requirements shall be formally documented and made part of all contractual agreements.

Copyright ©2026. All Rights Reserved. Clean Max Enviro Energy Solutions Limited.

- Due diligence assessment shall be performed for all third parties during vendor empanelment. CMES shall assess the third-party's capability to meet the information security requirements.
- Prior to being given access to CMES' Information and information systems, all third partiesneed to sign non-Disclosure agreements (NDAs).
- All third-party onboarding and access provisioning activities shall be conducted in accordance with CMES'User Access Management Policy and Section 10 (i.e., HR Security)of this document.
- The service level agreements (SLAs) shall be defined at the time of empanelment of third parties and their performance shall be monitored and reviewed on a periodic basis.
- CMES shall closely monitor the service delivery of the third-party to assure adherence to security policies and requirements that have been contractually agreed upon.
- The third-party contract shall have a 'Right to Audit' clause to ensure that CMES assesses the information security posture of its empaneled vendors.
- All third parties shall be contractually bound to utilize licensed products and systems while providing services to CMES.
- Information sharing and retention arrangements with the third-party shall be as per section 13 (i.e., Data Protection and Privacy) of this document.
- Upon termination or expiry of the contract, the third-party shall handover all information and information assets belonging to CMES.

23 Legal and Compliance

23.1 Scope

Legal and Compliance Policy is applicable to all areas and business activities of CMES. Furtherthis policy is applicable to all employees, contractors and third parties of CMES.

23.2 Policy Statements

- CMES shall identify and document all applicable legal, statutory, regulatory, and contractual requirements pertaining to cyber security.
- CMES shall perform technical compliance review periodically on its information systems to check compliance with its defined Cyber Security Policy and procedures.
- CMES shall define and conduct internal and external audit plan for performing information security audits on its information systems.
- CMES shall ensure protection and retention of all legal compliance documents as per legal, regulatory, and contractual requirements in accordance with section 13.2.5 (i.e., Data Retention and Disposal) of this document.
- With respect to protection of Personally Identifiable Information (PII), CMES shall implement adequate security controls in accordance with its Data Privacy Policy to be compliant with applicable local regulatory requirements.
- CMES shall incorporate procedure for identifying and reporting of sabotage.
- CMES shall prepare a detailed report on disturbances or unusual occurrences, identified, suspected, or determined to be caused by sabotage in the Critical System of CMES, and shall submit the report to the Sectoral CERT (CERT-In) and NCIIPC.

Copyright ©2026. All Rights Reserved. Clean Max Enviro Energy Solutions Limited.

24 Training and Awareness

24.1 Scope

Training and Awareness policy is applicable to all employees, contractors and third parties ofCMES.

24.2 Policy Statements

- CMES should establish, document, implement, and maintain an annual cyber security training program for personnel having authorized cyber or authorized physical access (unescorted or escorted) to their critical IT/ OT systems.
- Online training and awareness programs shall be conducted annually for all employees based on current Cyber Security Threat Landscape. Relevant records shall be maintained for reporting purpose.
- CMES shall review annually their cyber security training program and shall update it whenever necessary. Annual review shall record evaluation of the effectiveness of the trainings held.
- CMES shall ensure that cyber security training program designed for their IT as well as OT operation and maintenance personnel is as per Central Electricity Authority (CEA) guidelines 2021. Mandatory online trainings shall be assigned to newly joined employees with respect to organizations polices, standards and guidelines. Trainings with respect to cyber security awareness shall also be mandated.
- Completion and attendance shall be mandated where required and possible consequencesshall be defined for non-adherence by the IT team.
- An overall assessment of the employee's understanding where required shall be conducted at the end of an awareness, education, and training course to test knowledge transfer.

25 Glossary

AMC	Annual Maintenance Contract
APT	Advanced Persistent Threat
CMES	Clean Max Enviro Energy Solutions Ltd.
CCTV	Closed-Circuit Television
CD	Compact Disk
CEA	Central Electricity Authority of India
CIA	Confidentiality, Integrity, Availability
CSP	Cloud Service Provider
DLP	Data Loss Prevention
DVD	Digital Versatile Disc
EDR	Endpoint detection and response
HVAC	Heating, ventilation, and air conditioning
IaaS	Infrastructure as a Service

Copyright ©2026. All Rights Reserved. Clean Max Enviro Energy Solutions Limited.

IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IRM	Information Rights Management
IT	Information Technology
KPI	Key Performance Indicator
MTPD	Maximum Tolerable Period of Downtime
NDA	Non-Disclosure Agreement
NCIIPC	National Critical Information Infrastructure Protection Centre
NTP	Network Time Protocol
OEM	Original Equipment Provider
OT	Operational Technology
PaaS	Platform as a Service
PII	Personally Identifiable Information
PLC	Programmable Logic Controller
RAM	Random Access Memory
RDP	Remote desktop protocol
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SaaS	Software as a Service
SCADA	Supervisory control and data acquisition
SDLC	Software Development Life Cycle
SIEM	Security information and event management
SLA	Service-Level Agreement
SOC	Security Operations Center
UPS	Uninterruptible power supply
USB	Universal Serial Bus
VAPT	Vulnerability Assessment and Penetration Testing

26 Appendix A:

Data Classification Categories

Copyright ©2026. All Rights Reserved. Clean Max Enviro Energy Solutions Limited.

Classification Level	Definition
Public	Data that is not sensitive in nature; can be posted to public facing websites, discussed openly with anyone and has no existing national, international, or legal restrictions on access or usage.
Internal	Data that is not sensitive in nature and has no existing national, international, or legal restrictions. However, use of this data externally could have a low negative impact if disclosed
Sensitive	Data that is collected through normal business activities or generated through the management of the same. Its use is restricted to smaller teams within the organization who have a legitimate business reasonto access it. Compromise of this data could have a moderate negativeimpact with threats or legal implications on stakeholders.
Confidential	Data that is collected through business transactions or generated through the strategic execution of business activities. Its use is intended for an exclusive group or team of personnel. Compromise of this information could have a significant negative impact on stakeholders with critical threats or legal implications.

27 Appendix B:

Types of data handled at CMES.

Type of Data	Definition
Personally identifiable information (PII)	Personally identifiable information (PII) is information that, when use alone or with other relevant data, can identify an individual. This data typ refers to customer PII and Vendor PII. It includes personal information tha is collected, managed, or stored by CMES service providers. This include customer personal information including contact details, background chec information, customer personal financial information (credit scores, accoun numbers etc.), vendor data (contact information and banking details) and leaseholder data
Human Resource Information	Any data stored, managed and/ or handled by the HR including personal data that relates to an employee, consultant, or a contractor (current or past).
Legal Information	Any data created or handled by the legal department. This data includes and not limited to legal contracts, records, audit information, court documents, attorney's information, litigation history.
Operational Data (OT)	Information stored and/ or utilized for operations including criticalasset dat and SCADA systems data.

Copyright ©2026. All Rights Reserved. Clean Max Enviro Energy Solutions Limited.

Financial Information	Data related to the financial health of a business or customer relateddata including balance sheet, invoice, treasury, costing, and pricinginformation. This also includes the data used by internal management to analyze business performance and determine whether tactics andstrategies must be altered.

28 Appendix C:

VA Schedule

VA Type	Frequency	Responsibility	Expected Results
Vulnerability Assessment	Half Yearly	IT team	• Determine the set of active hosts, open ports, and available services. • Identify potential vulnerabilities on the active hosts, open ports, and available services. • Compare services that are listening on each machine against a list of authorized services. • Validate the operating systems and major applications. • Validate that up-to-date security patches. and software versions are used and unwanted ports and services are closed

Copyright ©2026. All Rights Reserved. Clean Max Enviro Energy Solutions Limited.

Penetration Testing	Annually	IT team	• Determine how vulnerable an organization's network is to penetration and the level of damage that can incur. • Test the effectiveness of security devices such as IPS/ firewall against covert attacks
Configuration Review	Annual	IT team	• Determine whether the applications and network components, servers are configured as per the baseline standards at the minimum.

29 Appendix D:

Vulnerability Remediation Timelines

Vulnerability Severity Rating	IT Internal Systems	IT – External Systems	OT – Internal Systems	OT – External Systems
Critical (CVSS 9-10)	30 days	15 days	90 days	60 days
High (CVSS 7-8.9)	30 days	15 days	90 days	60 days
Medium (CVSS 4-6.9)	90 days	45 days	180 days	120 days
Low (CVSS 0.1-3.9)	180 days	90 days	365 days	365 days

Copyright ©2026. All Rights Reserved. Clean Max Enviro Energy Solutions Limited.