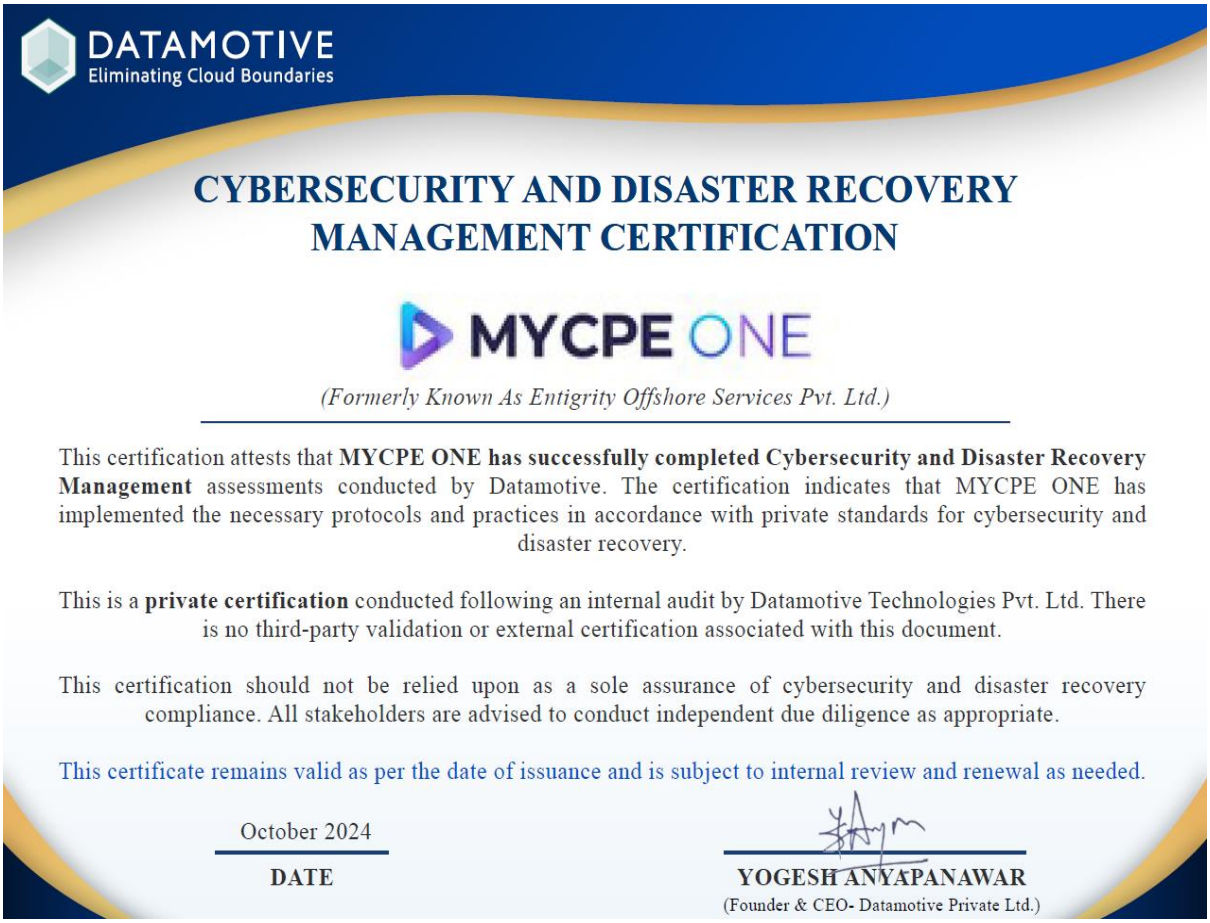
MYCPE ONE	BCP & DRP Overview

Disaster Recovery

MYCPE ONE has set up an automated process replicating all critical servers to Microsoft Azure. All servers are regularly replicated, and recovery can be tested and verified. The Recovery Point Objective (RPO) is 30 minutes, and the Recovery Time Objective (RTO) is 60 minutes.



DATAMOTIVE
Eliminating Cloud Boundaries

CYBERSECURITY AND DISASTER RECOVERY MANAGEMENT CERTIFICATION

MYCPE ONE

(Formerly Known As Entigrity Offshore Services Pvt. Ltd.)

This certification attests that **MYCPE ONE has successfully completed Cybersecurity and Disaster Recovery Management** assessments conducted by Datamotive. The certification indicates that MYCPE ONE has implemented the necessary protocols and practices in accordance with private standards for cybersecurity and disaster recovery.

This is a **private certification** conducted following an internal audit by Datamotive Technologies Pvt. Ltd. There is no third-party validation or external certification associated with this document.

This certification should not be relied upon as a sole assurance of cybersecurity and disaster recovery compliance. All stakeholders are advised to conduct independent due diligence as appropriate.

This certificate remains valid as per the date of issuance and is subject to internal review and renewal as needed.

October 2024
DATE

YOGESH ANYAPANAWAR
(Founder & CEO- Datamotive Private Ltd.)

BCP Overview

MYCPE ONE has a comprehensive business continuity plan to ensure operations can continue in the event of a disruption.

Sr No	Disruption Scenario	Impact on Information Security Arrangement	Continuity Arrangement
Internal Failure			
1	Fire	Physical Access Control System may not work. The server room may be impacted, restricting access to servers.	Building evacuation plan in place. Fire suppression systems protect critical areas. Staff communication maintained via mobile devices and secure remote access. Backups are stored offsite to ensure data availability.
2	Power Failure / Interruption	Power loss or fluctuation may cause hardware/network device failures. Physical Access Control System may not work.	UPS for critical devices, generator backup for prolonged outages, and a power monitoring system for early warnings.
3	Internet Connectivity Loss	Internet and VPN access may be unavailable.	Redundant ISP with SD-WAN ensures connectivity failover. Wireless dongles are available for temporary access. Periodic failover testing ensures smooth redundancy.
4	Email Server Failure	Difficulty in exchanging information.	Microsoft Office 365, a SaaS-based solution with a 99.99% SLA, minimizes downtime. Redundant email gateways provide backup communication options.
5	Communication Network Failure	Client communication and internal information transfer may be disrupted.	Alternative communication methods, including mobile phones, Microsoft Teams, and email, ensure continued information exchange.
6	Manmade Incidents	Core functions may be disrupted.	Cross-training and skill distribution minimize dependency on specific personnel. Incident response playbooks outline recovery steps.
7	Major HW/SW Failure	Information exchange, client communication, and internal information transfer may be impacted.	Redundancy for critical hardware/software. SLAs with vendors ensure timely replacements. Cloud backups and alternative hardware options minimize downtime.
External Failure			

8	Flood/Storm	Network and information processing assets may become inaccessible.	Remote work capabilities supported by a tested WFH policy. Secure VPN access and data protection measures in place. Physical safeguards for data centers, such as elevated storage, ensure asset safety.
9	Earthquake	Physical damage to assets and loss of network control. Access to critical infrastructure may be restricted.	Building evacuation plan in place. Staff at different locations maintain communication via a tested WFH policy. Secure remote access through VPN ensures operational continuity. Cloud backups and disaster recovery procedures ensure data availability.
10	Bomb Threat/Criminal Attempt/Terrorist Attack	Physical and digital assets may be compromised.	Building evacuation plan and secure remote access protocols are implemented. Data encryption ensures confidentiality if assets are compromised. Crisis management team coordinates with law enforcement.
11	Pandemic Outbreak	Reduced onsite staff availability.	WFH policy tested extensively during COVID-19 ensures operational continuity. Endpoint security measures, including VPN and MFA, are implemented for secure remote work.
12	Adverse External Environment Conditions	Reduced physical access to office locations.	WFH policy with secure VPN and endpoint protections ensures operational continuity. Communication via Teams and email keeps staff connected.