



Service Definitions

API: Application Programming Interface is a programming tool that enables programmers and developers to connect and interact with one or more software programs.

Appliance: Computing device with hardware and software bundled within to immediately begin working tasks in its program.

BCP: Business Continuity Planning is one or more organizational processes enabling the business to keep running after a disruptive event.

Compute: Application, processing and workload functions used to input data or complete tasks.

CSM: Customer Success Manager is the customer's advocate provided by CloudWave.

Deduplication: A backup technique that recognizes the same data between backup sets and removes duplicate data to conserve storage space.

Disaster Declaration: Formal request from Customer authorizing CloudWave to initiate recovery of data and operations in the OpSus Live environment.

DLP: Data Loss Prevention software scans and recognizes sensitive information to defend against data breaches and data leakage.

DMZ: De-Militarized Zone is the network perimeter that provides an interface to an external/untrusted network.

DNS: Domain Name System assigns a conventional name or phrase to an IP address better enabling humans to access and recall a site (i.e., gocloudwave.com).

EHR Provider: Electronic Healthcare Record providers use software and applications to enable end users to securely access and share sensitive healthcare records and data.

EPP: Endpoint protection is a suite of security solutions providing protection to devices (e.g., desktops, laptops, mobile devices, etc.).

FEC: Forward Checking Error Correction is an investigative program used to detect a series of errors and apply a corresponding repair to prevent a break in transmission or the requirement to re-transmit.

FW Instance- Appliance: Application level firewall (virtual).

Hardened OS Image: A set of known configurations configured to optimize and secure a system for safe, repetitive installation.



Service Definitions

High Availability: Computing instances with greatest performance, reliability and fault protection through redundancy, automatic failover, and instance replication.

IaaS: Infrastructure as a Service is a business model where a service provider offers scalable computing, storage, network and security services, etc. to the customer.

Immutable Backups: a backup system where the data in a backup is unchangeable and cannot be deleted or encrypted.

Instance- Monitoring Performance: Tool used to measure the performance of running compute instances against a baseline.

Instance- Monitoring Capacity: Tool used to measure the load of running compute instances to recognize level of consumption.

IOPS: Input/output Operations Per Second is a method used to measure the performance of a storage system or storage device.

IPsec: Internet Protocol Security provides encrypted communication between two devices over the internet, typically used to secure data sent through public networks.

ITIL: Information Technology Information Library is a business framework that uses a set of best practices to align an organization's IT operations and services.

LAN: Local Area Network is computer network operating within a limited area (i.e., residence, hospital, school, etc.).

L2L: LAN to LAN networks is a connection between two separate networks.

MDM: Mobile device management is security and privacy driven administration of devices.

MFA: Multi Factor Authentication is a security application used to verify user access and authorization prior to granting system, site, or network access.

NOC: Network Operations Center is a location for network monitoring and management.

Object Storage: is a data archiving technology that breaks data into small components (objects) to be stored in isolated storehouses, metadata and an identifier system enable data to be stored efficiently and recalled quickly.

PACS: Picture Archiving and Communication Systems is a digital system used to store, transfer and display medical images.

Private Circuit: An unshared telecommunication circuit connecting two or more locations.



Service Definitions

RADIUS: Remote Authentication Dial-In User Service is a networking authentication protocol.

RAID: Redundant Array of Independent Disks is a storage technology used to improve data drive reliability and efficiency.

RPO: Recovery Point Objective is a target describing the minimum recovery of data (point in time from the past) carried forward to the return of normal operations.

RTO: Recovery Time Objective is a target describing the maximum duration of time between a point of failure (disaster) and the return of normal operations.

SAN: Storage Area Network provides network access to block level data storage.

SIEM: Security Information and Event Management is a security tool that monitors, logs, detects and manages security alerts in networking, infrastructure and application environments.

Snapshot: a picture in time of a server capturing the entire file system.

SOC: Security Operations Center is a central location for security issues and management.

SSL: Secure Sockets Layer is a security encryption linking a server and client enabling both sides to pair cryptographic keys for secure connection.

TLS: Transport Layer Security encrypts data sent over the internet.

TCO: Total Cost of Ownership is a financial analysis used to recognize the difference between the actual cost of a technology against the total expense required to use and manage the technology.

VDI: Virtual Desktop Infrastructure is a software tool that hosts the physical client device on a virtual server, enabling end users to remotely access the physical device.

VLAN: Virtual LAN links a collection of devices from several networks into one logical network.

VRF: Virtual Routing & Forwarding allows multiple instances of a routing table to exist at once.

VTM: Vulnerability Threat Management is a healthcare centered PHI security service.

WAN- Dedicated: Internet access point assigned to a single customer with unshared network resources.

WAN- VPN: Internet access point shared between multiple customers using encryption to protect traffic other users and networks.