Security and Compliance Posture Guideline

CloudWave developed this document to describe our security and compliance posture as an infrastructure as a service provider (IaaS). The responses describe our security program, physical and logical environment hardiness, standards for personnel access and behavior, and our certification and compliance record. Please contact CloudWave through your usual channel or use the 'Contact us' form on the gocloudwave.com website for additional information.

Author:

Ashini Surati
Director, Security, Compliance & Quality

Approver:

Mark Middleton
VP. Cloud Services & Chief Quality Officer

Part 1: Security Program			
	Question:	Answer:	Detail:
1	Does CloudWave have a formal Information Security Program?	Yes	The CloudWave security framework is based on a combination of HIPAA Security Requirements, ISO 27002, Cloud Security Alliance framework, NIST Cybersecurity Framework, and NIST Special Publication 800-53 as security baseline requirements.
2	Does CloudWave update its Information Security Program?	Yes	At least annually and upon significant change.
3	Does CloudWave perform internal risk assessments?	Yes	At least annually and upon significant change.
4	Does CloudWave perform internal contingency testing?	Yes	At least annually and upon significant change.
5	Does CloudWave perform annual audits?	Yes	SSAE18 SOC1 Type 2 and SSAE18 SOC2 Type 2 w. HITRUST Validation (performed by third-party assessors).
6	Does CloudWave have a HIPAA Privacy Officer?	Yes	The Director of Security and Compliance serves as the HIPAA Security Officer with privacy duties included.
7	Are security and privacy policies and procedures maintained?	Yes	All security and data privacy policies are reviewed at least annually and upon significant change.
8	Does CloudWave require vendors and other third-parties to sign a BAA?	Yes	All subcontractors are required to sign a BAA prior to execution of services. The BAA remains in effect until termination of the services or termination of the agreement due to breach.
9	Are employees and contractors required to comply with corporate policies?	Yes	All employees and contractors must accept and comply with all corporate security and privacy policies.
10	Are employees and contractors required to complete annual security training?	Yes	All employees and contractors must complete security and awareness trainings including, but not limited to, privacy, security and compliance as required by states, regions, and nations where CloudWave offers services.

CloudWave

Security and Compliance Posture Guideline

Part 1: Security Program			
	Question:	Answer:	Detail:
11	Are employees and contractors required to sign data and confidentiality agreements?	Yes	All employees and contractors must acknowledge and sign confidentiality and data protection agreements upon hire.
12	Do employees and contractors receive the minimum access required?	Yes	All access is given to employees and contractors on an as needed basis and is consistent with the principle of minimum necessary access and least privilege.
13	Does CloudWave have a data classification policy?	Yes	CloudWave has three levels of classification: • Confidential applies to data or systems that store or process personally identifiable information or protected health information. • Restricted applies to all other information. • Public/Unclassified applies to data needing no classification and no protection other than against loss or manipulation.
14	Does CloudWave enforce a password complexity and password change policy?	Yes	Password complexity and change parameters are technically enforced.
15	Does CloudWave use a vault to restrict access to passwords?	Yes	All passwords are stored in a secure vault where access is role based and activity is logged (login/credential access history).

Part 2: Risk Program			
	Question:	Answer:	Detail:
1	Does CloudWave have a formal risk management program?	Yes	The program assesses physical, administrative, technical, and logical risks.
2	Does CloudWave perform risk and vulnerability assessments?	Yes	At least annually and upon significant change.
3	Does CloudWave carry liability insurance?	Yes	CloudWave carries liability insurance as well as cyber insurance.
4	Is third-party risk assessment part of the risk program?	Yes	CloudWave performs annual review of the compliance certification and audits reports provided by third-party service providers to maintain an ongoing service level management agreement with the providers.
5	Does CloudWave assess its facilities for risk?	Yes	CloudWave performs an annual audit of the security, availability, and redundancy of all its facilities.
6	Does CloudWave maintain a complete inventory of IT assets?	Yes	CloudWave maintains an inventory of IT assets and manages the assets for uptime, availability, and capacity. Non-company owned devices (i.e., virtual non-persistent desktop instances at customer sites) are not included in this inventory, but monitoring, support, and anti-virus protection of these instances is performed.

Part 2: Risk Program			
	Question:	Answer:	Detail:
7	Does CloudWave have a Business Continuity Plan (BCP) in place?	Yes	CloudWave's BCP includes plans for personnel and office operations as well as technical plans for backup and restoration of customer services. Annual audits are performed on BCP strategies.

Part 3: Data Centers			
	Question:	Answer:	Detail:
1	Are data centers audited for security?	Yes	In the Private/Hybrid Cloud, physical data centers undergo a SOC 2 Type 2+HITRUST examination. For Public Cloud, and any data center that CloudWave has no access, we review their certifications annually.
2	Do data centers exercise redundancy?	Yes	Data centers have fully redundant subsystems (power, cooling, network, etc.) as well as multiple ISPs (carrier diversity) with redundant paths into the data centers.
3	Are CloudWave racks separate from other customers?	Yes	In the Private/Hybrid Cloud all CloudWave equipment and power sources are secured within cages controlled by biometric access. For Public Cloud data centers, CloudWave ensures customer isolation is in place via an internal audit of data center compliance certifications.
4	Are data centers secure 24/7/365?	Yes	Physical security includes perimeters (fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks and security patrols). Ingress and egress points are monitored and controlled.
5	Does CloudWave restrict access to its own employees (need to know only)?	Yes	In the Private/Hybrid Cloud, physical access to cages is limited to authorized personnel as approved by management. For Public Cloud data centers, CloudWave ensures access is controlled via an internal audit of data center compliance certifications.
6	Are controls in place for physical data transfer?	Yes	In the Private/Hybrid Cloud, appropriate authorization and chain of custody processes, including signoffs, are obtained prior to relocating or transferring assets containing data (sent or received) from customers, suppliers or between CloudWave facilities. For Public Cloud data centers, CloudWave ensures physical data transfers are controlled via an internal audit of data center compliance certifications.
7	Is physical media/data destruction securely performed?	Yes	In the Private/Hybrid Cloud, storage media is properly stored and destroyed according to DoD handling and media destruction standards. For Public Cloud data centers, CloudWave ensures physical media/data destruction is securely performed

Part 3: Data Centers			
	Question:	Answer:	Detail:
			via an internal audit of data center compliance standards.
8	Is visitor access controlled?	Yes	Visitor access is tightly controlled, including identity verification and access logging. Visitors are required to remain with their escort.

Part 4: Change Management			
	Question:	Answer:	Detail:
1	Does CloudWave exercise change management?	Yes	Change management processes and procedures are used to minimize unintended service disruptions and deliver efficient environment changes.
2	Do change management processes include rollback plans or other safety measures?	Yes	The change management process includes change review, risk assessment, service impact, rollback plans, mitigation efforts, documentation, and authorization prior to applicable changes.
3	Are Customer requested changes subject to change control?	Yes	Change requests from any entity, including customers, require formal change control.

Part 5: Compliance Audits			
	Question:	Answer:	Detail:
1	Does CloudWave undergo annual audits?	Yes	CloudWave maintains an SSAE18 SOC 1 Type 2 and SOC2 Type 2 (for Security and Availability) with HITRUST validation performed by third-party assessors.
2	Does CloudWave assess against two of the five "Trust Service Principles" (SOC 2 Type 2)?	Yes	CloudWave assesses against "Security" and "Availability" as primary trust service principles.
3	Is the Security Audit far reaching?	Yes	CloudWave assessments include: • Third-party management • Human resource management • Physical security • Environmental controls • System and application backups • Continuous service • User access management • System event logging and monitoring • Incident management • Infrastructure management • Security and controls of confidential electronic information • IT risk assessment • Infrastructure patch management

Part 5: Compliance Audits			
	Question:	Answer:	Detail:
4	Does CloudWave undergo penetration testing?	Yes	CloudWave conducts an annual external penetration test performed by an independent service provider.
5	Are CloudWave services HIPAA compliant?	Yes	CloudWave services are HIPAA compliant. CloudWave as an organization does not pursue HIPAA certification because it is a Business Associate not a covered entity.
6	Are CloudWave solutions GDPR compliant?	Yes	CloudWave services are GDPR compliant and, where applicable, national and other regional data and privacy regulations are also applied.
7	Are CloudWave solutions PIPEDA compliant?	Yes	CloudWave services are PIPEDA compliant and, where applicable, regional data and privacy regulations are also applied.
8	Are all data (including copies of backups) stored within my country/region of origin?	Yes	CloudWave services consist of geographically dispersed locations but maintains compliance with applicable region(s) or national requirements for data sovereignty.
9	Does the CloudWave environment remain outside of PCI requirements?	Yes	CloudWave does not process payment or card information. No portal for PCI service is offered.

Part 6: Access Control			
	Question:	Answer:	Detail:
1	Does CloudWave screen employees and contractors before hire?	Yes	All employees are screened during the hiring process using multiple background check methods. All employees agree to non-compete, acceptable use agreements and the employee handbook at the time of hire. Human Resources processes are completed prior to granting access to data, assets, and information systems.
2	Does CloudWave manage and audit employee access?	Yes	Employees receive account access through a process, beginning with a management request. Access is based on needs and follows the principles of least privilege. Access audits are performed bi-annually.
3	Does CloudWave control privileged access?	Yes	Privileged access to systems and sensitive data is restricted to only those who require access and are approved by manager justification. Systems with sensitive or confidential data are restricted by job classification.
4	Does CloudWave require MFA for employees to access systems?	Yes	Multi-factor authentication (MFA) is required for all system access.
5	Upon employee or contractor termination, are all accounts de-activated?	Yes	Termination procedures begin immediately after employee removal and include recovery of all physical items as well as removal of all entitlements and accounts.

Part 7: Shared Responsibilities			
	Question:	Answer:	Detail:
1	Does CloudWave participate in the Shared Responsibility model?	Yes	CloudWave follows a shared responsibility model where each organization shares some responsibility for environmental security.
2	Are customer responsibilities known?	Yes	Customer is responsible for the application and user access controls for the platform they use as well as application patching and/or upgrades.
3	Are CloudWave responsibilities known?	Yes	CloudWave enables access to the environment for the Customer, application vendor, and other approved third parties using a secure connection (LAN 2, L2L, VPN, or SSL). CloudWave is responsible for the infrastructure provided to customers.
4	Does CloudWave provide live-technical support?	Yes	Support hours are 24 x 7 x 365, Customers can reach the Service Center by toll-free phone, email, and ticketing system.

Part 8: Operations Management			
	Question:	Answer:	Detail:
1	Does CloudWave perform maintenance according to recommendations?	Yes	All scheduled maintenance and repairs will be performed in accordance with vendor specifications and business requirements.
2	Does CloudWave schedule patching according to customer needs?	Yes	CloudWave and customers work together to schedule patching. CloudWave offers monthly, bi-monthly, and quarterly patching cycles, with a minimum of every 90 days to patch requirement.
3	Does CloudWave test patching?	Yes	Patches or fixes are analyzed to the extent possible to validate service functionality and are applied following change management.
4	Does CloudWave scan the environment for vulnerabilities?	Yes	CloudWave performs periodic vulnerability scans, in addition to monitoring system alerts to manage and maintain the environment.
5	Does CloudWave perform emergency (out of band) patching?	Yes	CloudWave conducts out of band, unscheduled patching when vendors release critical alerts and/or patches that require more immediate action.
6	Does CloudWave employ A/V or EPP to protect customer assets?	Yes	Endpoint protection is deployed on servers and endpoints across the entire environment for malware protection. A third-party Security Operations Center (SOC) is also contracted to assist with detection and response 24/7/365.
7	Can customers install software and applications of their choice?	Yes	CloudWave works with the customer to develop an environment to suit primary applications and software. Customers should avoid installing applications and software that may adversely affect the security of the environment or may conflict with and/or duplicate CloudWave management functions. However,

Part 8: Operations Management			
	Question:	Answer:	Detail:
			customers have the ability to install software of their choice.
8	Should the customer notify CloudWave of any changes or reboots?	Yes	Any change that affects CloudWave's infrastructure environment, including reboots or downtime, should be coordinated with CloudWave.
9	Is the Customer accountable for separation and isolation between production and test environments?	Yes	It is up to the customer to ensure test and production environments and data are properly segregated and isolated.
10	Is each party accountable for their own actions in the event of a security breach or security incident?	Yes	CloudWave is not responsible for a security breach or security related incident that occurs due to negligence on the part of the customer or for lack of coordination of activities with CloudWave.
11	Do customers have access to a monitoring service to see SLA performance?	Yes	The MyOpSus Monitoring portal provides on demand access to service performance and the MyOpSus Ticketing portal displays SLA thresholds built into the alerts.

Part 9: Backup and System Recovery			
	Question:	Answer:	Detail:
1	Does CloudWave identify its minimum backup interval, schedule, and retention?	Yes	Backup intervals, schedules and retention options are listed in each applicable service within the Service Level Agreement. See each service on the corporate website for details.
2	Are backups encrypted?	Yes	Backup data is encrypted on the storage arrays, following industry best practices using the AES 256-bit data encryption standard.
3	For hosted services, are backup copies stored in separate locations?	Yes	Replication ensures a copy of each backup is stored in a secondary datacenter.
4	Are replications secure?	Yes	Replication occurs across a private WAN circuit or dedicated secure VPN tunnels.
5	Are all backups stored within my country/region of origin?	Yes	This service consists of geographically dispersed locations but maintains compliance with applicable regional or national regulatory requirements.
6	Does CloudWave store spare components in the event of service interruption?	Yes	Where applicable, spare components, or relationships with third-party vendors who provide spare components, are maintained to reduce service interruption.
7	For disaster recovery services, is the environment tested?	Yes	Disaster recovery tests are offered to Customers typically annually or as contracted.
8	For disaster recovery services, what are the RPO and RTO targets?	Yes	The Recovery Point Objective (RPO) and the Recovery Time Objective (RTO) are listed in each applicable service within the Service Level Agreement. See each service on the corporate website for details.

Part 9: Backup and System Recovery			
	Question:	Answer:	Detail:
9	Does CloudWave offer immutable backups?	Yes	Immutable backups can be implemented. However, you should expect greater storage consumption.

Part 10: Data at Rest/Data in Motion			
	Question:	Answer:	Detail:
1	Does CloudWave encrypt data at rest?	Yes	Encryption is enabled on all storage arrays using AES 256-bit data encryption standards.
2	Are CloudWave computers encrypted?	Yes	All laptops used by CloudWave employees are encrypted with bitlocker and have endpoint protection.
3	Is data stored on CloudWave computers encrypted?	Yes	Employees are not allowed to store data on laptops or local workstations unless the data is encrypted.
4	Is data deleted in accordance with any standard or policy?	Yes	All customer data is purged upon contract termination, component removal from contract, and according to retention policies, as described in the Master Terms and Conditions.
5	Is physical media/data destruction performed to any U.S. government standard?	Yes	Storage media is properly stored and destroyed according to DoD handling and media destruction requirements.
6	Does CloudWave encrypt data in motion?	Yes	While accessing confidential or sensitive data over the public network, CloudWave uses Secure Socket Layer (SSL) which uses approved encryption (i.e., TLS 1.2, TLS 1.3 or other secure communications tunnels such as Virtual Private Network).
7	Does CloudWave enable secure communication with Customers or necessary vendors?	Yes	Secure L2L VPN tunnels are setup with Customers and third-party services for requisite communications between sites. Where secure L2L tunnels are not feasible, a client VPN connection is enabled.
8	Are CloudWave communication tools encrypted?	Yes	All employee communications (i.e., email, chat, etc.) containing sensitive or confidential data is encrypted when shared from company email to an external email address and remains subject to any applicable industry or government regulation.
9	Does CloudWave restrict employees from sharing sensitive information online (i.e., social media)?	Yes	CloudWave prohibits employees from sharing sensitive or confidential information in any unofficial or unapproved fashion.
10	Does CloudWave restrict employees from using removable storage devices?	Yes	Employees are not allowed to use USB devices/flash drives or CDs/DVDs for sensitive or confidential data and remains subject to any applicable industry or government regulation.
11	Are confidential paper documents securely stored?	Yes	All confidential paper documents are marked as such and stored under lock and key when not in use.
12	Are confidential paper documents securely disposed of when no longer needed?	Yes	Appropriate disposal methods, including deposal in secure bins for shredding, is used for sensitive paper documents. In the event that a bin is not available,

Part 10: Data at Rest/Data in Motion			
	Question:	Answer:	Detail:
			employees are responsible for shredding the paper prior to appropriate disposal.
13	Does CloudWave have security requirements for the use of mobile devices when employees access data?	Yes	All employees must password enable their smart phones, at a minimum, if sensitive or confidential information is viewable or downloadable. CloudWave has a Mobile Device Management (MDM) policy, and enforces the policy to ensure all employees maintain compliance.
14	Does CloudWave allow customers to manage third-party access?	Yes	Customers are responsible for managing and maintaining user access for third-party vendors accessing data on the CloudWave platform.
15	Does CloudWave require customer approval before authorizing third-party access?	Yes	Third-party vendors and service providers must be approved by the customer before CloudWave enables access. Third-party use and access are subject to CloudWave security guidelines.

Part 11: Network Security and Isolation			
	Question:	Answer:	Detail:
1	Does CloudWave use firewalls to secure the network?	Yes	CloudWave maintains firewalls (physical and/or virtual), as well as perimeter firewalls and virtual firewalls between VLANs.
2	Does CloudWave restrict untrusted traffic through the firewall?	Yes	External or “untrusted” traffic is not permitted to pass through the firewall unless permitted on an approval list.
3	Does CloudWave enable secure access to Customers over the internet?	Yes	A de-militarized zone (DMZ) is maintained for devices accessible from the internet via a public IP address (but separated from the internal network by firewall).
4	Does CloudWave monitor, manage and maintain the DMZ?	Yes	All devices in the DMZ are maintained in the configuration management database (CMDB) and are subject to standard change management.
5	Does CloudWave secure confidential network information?	Yes	All network interfaces, Domain Name Server records, and all additional system configuration documentation is secured and only available to those who need access.
6	Does CloudWave monitor network traffic?	Yes	Intrusion detection systems maintain and monitor traffic.
7	Does CloudWave monitor network logs?	Yes	Logging is enabled for network/critical devices to the maximum extent possible and logs are sent to the centralized log collector for aggregation, correlation, and analysis.
8	Are customer networks securely isolated from one another?	Yes	The network architecture separates customers from one another, including both the internal network and management framework. Customers are isolated using VLAN and VRF technology and can only access their own environment.

Part 11: Network Security and Isolation			
	Question:	Answer:	Detail:
9	For archive services, is data securely isolated from other customers?	Yes	Restriction of "archive" data is performed by a multi-tenancy function of the security architecture.
10	For backup services, is data securely isolated from other customers?	Yes	Restriction of "backup" data is performed by dedicated backup servers isolated for each customer.
11	Do customers manage and control network access?	Yes	Customers manage user access and provide the unique credentials to CloudWave for login and environment management.
12	Does CloudWave perform Change Management before accepting a modification?	Yes	All modifications or waiver requests are subject to a risk assessment presented to the governance committee for potential security impact analysis prior to change approval.
13	Does CloudWave provide country blocking functionality?	Yes	CloudWave offers country blocking services as an option.

Part 12: Vulnerability Management			
	Question:	Answer:	Detail:
1	Is CloudWave subscribed to security alerts from industry and government experts?	Yes	CloudWave receives information system security alerts, advisories, and directives from the United States Computer Emergency Readiness Team (US-CERT) agency and applicable vendors.
2	Does CloudWave act on security alerts and recommendations?	Yes	CloudWave disseminates the information to the appropriate CloudWave personnel operating the environment. These advisories, alerts, and directives, in addition to other alerts, received from various sources assist in the fulfillment of patching and vulnerability management in the environment.
3	Does CloudWave perform external vulnerability scans?	Yes	External vulnerability scans are performed daily on the environment to identify, report, and remediate vulnerabilities. Remediation activities, if any, are tracked and updated in the assurance program.
4	Does CloudWave perform internal vulnerability scans?	Yes	Internal vulnerability scans are performed on a periodic basis. All alerts presenting a false positive will be noted and all high, medium, and low severity vulnerabilities will be analyzed and remediated unless they affect the functionality of the application or how a customer uses the infrastructure. All activities will follow defined change management processes.
5	Does CloudWave perform or subscribe to penetration testing?	Yes	Penetration testing is performed annually by independent third-party assessors as part of assurance planning. Remediation activities, if any, are tracked and updated in the assurance program. Any additional penetration testing on external devices is performed on an as-needed basis.

Part 13: Security Incident Management and Breach Notification			
	Question:	Answer:	Detail:
1	Does CloudWave respond to real or potential security incidents with urgency?	Yes	Security incidents and security threats are investigated in real-time. All events identified as a potential security incident follow the incident management process.
2	Can customers report real or potential security incidents?	Yes	Security incidents can be reported by customers or opened by employees (service desk, engineers, support staff etc.).
3	Can security Incidents be created by a non-human monitoring service?	Yes	Automated alerts such as logging and monitoring tools or endpoint protection platforms can create security incidents.
4	Does CloudWave audit logs for security incidents?	Yes	CloudWave's centralized audit logging with continuous monitoring investigates the following: • Antivirus alerts (endpoint) • Abnormal ingress traffic indications • Cleared audit logs • Privileged user additions • Unapproved modifications
5	Does CloudWave notify customers of real or potential security incidents?	Yes	In the event a security incident is discovered with the potential to compromise a customer's environment, CloudWave will be able to immediately inform the customer.
6	Does CloudWave have a breach policy?	Yes	CloudWave maintains all breach notification processes and procedures required to perform business in the region, state, or nation where services are provided.
7	Does the CloudWave environment remain without incident of breach?	Yes	CloudWave has never experienced a data breach.
8	Does CloudWave adhere to legal standards and regulations regarding breach notifications?	Yes	CloudWave adheres to legal, compliance and government regulations as required by the region, state, or nation where services are provided.
9	Does CloudWave perform breach notifications according to legal standards and regulations?	Yes	In the event a breach is discovered, CloudWave will notify the customer based on a region or nation's regulatory requirements. CloudWave's breach notification includes governance, processes, and procedures to be followed in the event of a breach.
10	Does CloudWave deny any and all requests for data from outside entities unless lawfully required?	Yes	CloudWave will not provide any data or records of data unless authorized by the customer or a lawful legal order requires disclosure.
11	Does CloudWave have a public privacy policy?	Yes	CloudWave's Privacy Policy identifies how CloudWave uses and manages personal data encountered while operating the services.
12	Does CloudWave have a public cookie policy?	Yes	CloudWave's Cookie Policy identifies how, when, and why cookies are used. It also identifies how to manage or remove your approval for our use of cookies.