Last Updated: June, 2022

Security Policy - Amorphic Data Cloud for AWS

This Security Policy for Amorphic Data Cloud for AWS (Amorphic) outlines the technical and procedural measures that Amorphic and thereby, Cloudwick, undertakes to protect Customer Data from unauthorized access or disclosure. Cloudwick maintains these security measures in a manner consistent with SOC 2 (Type II) and addresses the mitigation strategies for the OWASP top 10 vulnerabilities.

Cloudwick has a written information security plan to implement the terms of this Security Policy that is reviewed and approved annually by its senior management team. As used in this Security Policy: “Cloud Provider” means the third-party cloud provider, specifically - Amazon Web Services, Inc. (“AWS”) and “Cloud Private Network” means the VPC from which the Service is provided and “Cloudwick Personnel” or “Amorphic Product Team” means Cloudwick employees and individual subcontractors. This Security Policy is referenced in and made a part of your customer agreement with Cloudwick (the “Agreement”) and any capitalized terms used but not defined herein shall have the meaning set forth in the Agreement or Documentation, as applicable. In the event of any conflict between the terms of the Agreement and this Security Policy, this Security Policy shall govern. This Security Policy may be updated from time to time upon reasonable notice to Customer (which may be provided through the Service or the AWS Marketplace) to reflect process improvements or changing practices, but any such modifications will not materially diminish either party’s obligations as compared to those reflected below.

1. Customer Data Access and Management

1.1 Customer controls access to its Account(s) in Amorphic via User IDs and passwords.

1.2 Cloudwick Personnel do not have access to unencrypted Customer Data unless Customer provides access to its Amorphic account to such Cloudwick Personnel. If such access is granted, Cloudwick Personnel are prohibited from storing Customer Data on local desktops, laptops, mobile devices, shared drives, removable media such as USB drives, or on public facing systems that do not fall under the administrative control or compliance monitoring processes of Amorphic and thereby – the Customer Amorphic associated AWS account that is managed by Cloudwick Personnel.

1.3 Cloudwick uses Customer Data only as necessary to provide services to Customer, as provided in the Agreement.

1.4 Customer Data is stored only in the Customer's Amorphic production environment in the Cloud Private Network.

1.5 Customer Data is stored in the available Amorphic AWS Region for the account requested by Customer.

1.6 Cloudwick shall create and maintain flow diagram(s) indicating how Customer Data flows through the Service ("Flow Diagrams") and shall provide Flow Diagrams upon Customer's reasonable request. Flow Diagrams are Cloudwick Confidential Information.

2. Encryption and Logical Separation of Customer Data

2.1 Amorphic always encrypts Customer Data while at rest using the AWS Key Management Service (KMS) symmetric key encryption – managed keys which use AES-256-bit encryption. These AWS KMS managed encryption keys are automatically rotated by AWS.

2.2 Amorphic encrypts traffic with Transport Layer Security ("TLS") 1.2 when communicating across untrusted networks such as the public internet.

2.3 The encryption keys are logically separated from Customer Data. Specifically, Amorphic employs AWS KMS managed keys to safeguard the encryption keys.

3. Service Infrastructure Access Management

3.1 Access to the systems and infrastructure that support Amorphic service is restricted to Cloudwick Personnel who require such access as part of their job responsibilities.

3.2 Unique User IDs are assigned to Cloudwick Personnel requiring access to Amorphic in order to support the Service.

3.3 Amorphic password policy in the production environment adheres to the PCI-DSS password requirements and is defined by Cloudwick in the Customer's Amorphic corresponding AWS account's - IAM service.

3.4 Access privileges of separated Cloudwick Personnel are disabled promptly. Access privileges of persons transferring to jobs requiring reduced privileges are adjusted accordingly.

3.5 User access to the systems and infrastructure that support the Service is reviewed quarterly.

3.6 Access attempts to the systems and infrastructure that support the Service are logged, monitored, and alerted for suspicious activities.

3.7 Cloud Provider network security groups have deny-all default policies and only enable business required network protocols for egress and ingress network traffic. The Service only allows TLS 1.2 protocol from the public internet.

4. Risk Management

4.1 Cloudwick's Amorphic - Risk Management process is modeled on SOC 2 Type II.

4.2 Cloudwick conducts risk assessments of various kinds throughout the year, including self- and third-party assessments, audits, tests, automated scans, and manual reviews.

4.3 Results of assessments, including formal reports as relevant, are reported to the VP of Security. A Security Committee meets weekly to review reports, identify control deficiencies and material changes in the threat environment, and make recommendations for new or improved controls and threat mitigation strategies to senior management.

4.4 Changes to controls and threat mitigation strategies are evaluated and prioritized for implementation on a risk adjusted basis.

4.5 Threats are monitored through various means, including threat intelligence services, vendor notifications, and trusted public sources.

5. Vulnerability Scanning and Penetration Testing

5.1 Vulnerability scans are automatically performed weekly on systems required to operate and manage Amorphic. The vulnerability database is updated regularly.

5.2 Scans that detect vulnerabilities meeting Cloudwick-defined risk criteria automatically trigger notifications to security personnel.

5.3 Potential impact of vulnerabilities that trigger alerts are evaluated by staff.

5.4 Vulnerabilities that trigger alerts and have published exploits are reported to the Security Committee, which determines and supervises appropriate remediation action.

5.5 Vulnerabilities are prioritized based on potential impact to the Service, with "critical" and "high" vulnerabilities typically being addressed within 30 days of discovery and "medium" vulnerabilities being addressed within 90 days of discovery.

5.6 Security management monitors or subscribes to trusted sources of vulnerability reports and threat intelligence.

5.7 Penetration tests by an independent third-party expert are conducted at least annually.

5.8 Penetration tests performed by Cloudwick Security are performed regularly throughout the year

6. Remote Access & Wireless Network

6.1 All access by Cloudwick Personnel to the Cloud Private Network requires successful authentication through a secure connection via approved methods such as VPNs and enforced with mutual certificate authentication and multi-factor authentication ("MFA").

6.2 VPN access is further enforced by mutual TLS authentication.

6.3 Cloudwick corporate offices, including LAN and Wi-Fi networks in those offices, are considered to be untrusted networks.

7. System Event Logging, Monitoring & Alerting

7.1 Monitoring tools and services are used to monitor systems including network, service events, and Cloud Provider API security events, availability events, and resource utilization.

7.2 Amorphic infrastructure Security event Logs are collected in a central system and protected from tampering. Logs are stored for a minimum of 12 months.

7.3 All Amorphic provided user endpoints have Endpoint Detection & Response ("EDR") tools to monitor and alert for suspicious activities and potential malware.

7.4 All Cloud Private Networks leverage advanced threat detection tools to monitor and alert for suspicious activities and potential malware.

8. System Administration and Patch Management

8.1 Cloudwick shall create, implement and maintain system administration procedures for systems that access Customer Data that meet or exceed industry standards, including without limitation, system.

8.2 Cloudwick Security reviews US-Cert new vulnerabilities announcements weekly and assess their impact to Amorphic based on Cloudwick-defined risk criteria, including applicability and severity.

8.3 Applicable US-Cert security updates rated as "high" or "critical" are addressed within 30 days of the patch release and those rated as "medium" are addressed within 90 days of the patch release.

9. Amorphic Security Training and Cloudwick Personnel

9.1 Cloudwick maintains a security awareness program for Cloudwick Personnel, which provides initial education, ongoing awareness and individual Cloudwick Personnel acknowledgment of intent to comply with Amorphic corporate security policies. New hires complete initial training on security, SOC, HIPAA, OWASP and PCI, sign a proprietary information agreement, and digitally sign the information security policy that covers key aspects of the Cloudwick's Amorphic Information Security Policy.

9.2 All Cloudwick Personnel acknowledge they are responsible for reporting actual or suspected security incidents or concerns, thefts, breaches, losses, and unauthorized disclosures of or access to Customer Data.

9.3 All Cloudwick Personnel are required to satisfactorily complete quarterly security training.

9.4 Cloudwick performs criminal background screening as part of the Cloudwick hiring process, to the extent legally permissible.

9.5 Cloudwick will ensure that its subcontractors, vendors, and other third parties (if any) that have direct access to the Customer Data in connection with the services adhere to data security standards consistent with the compliance standards.

10. Physical Security

10.1 Amorphic hosted with Amazon Web Services (AWS) Cloud Provider and all physical security controls are managed by AWS. Cloudwick reviews the Cloud Provider's SOC 2 Type 2 report annually to ensure appropriate physical security controls, including:

> **10.1.1** Visitor management including tracking and monitoring physical access.
>
> **10.1.2** Physical access point to server locations are managed by electronic access control devices.
>
> **10.1.3** Monitor and alarm response procedures.
>
> **10.1.4** Use of CCTV cameras at facilities.
>
> **10.1.5** Video capturing devices in data centers with 90 days of image retention.

11. Notification of Security Breach

11.1 A "Security Breach" is (a) the unauthorized access to or disclosure of Customer Data, or (b) the unauthorized access to the systems/services within Amorphic that transmit or analyze Customer Data.

11.2 Cloudwick will notify Customer in writing within seventy-two (72) hours of a confirmed Security Breach.

11.3 Such notification will describe the Security Breach and the status of Cloudwick's investigation.

11.4 Cloudwick will take appropriate actions to contain, investigate, and mitigate the Security Breach.

12. Disaster Recovery & Business Continuity

12.1 Cloudwick maintains a Disaster Recovery Plan ("DRP") for Amorphic. The DRP is tested annually. However, changes to the DRP based on the Customer's required Recovery Time Objective (RTO) and Recovery Point Objective (RPO) will be made by Cloudwick upon mutual agreement.

12.2 For the AWS Cloud Provider, Amorphic is managed in different AWS Regions as standalone deployments, which can be employed as part of Customer's DRP strategy. To effectively use the AWS cross regional availability of the Service for disaster recovery purposes, Cloudwick is responsible for the following:

> **12.2.1** Requesting the Customer information pertaining to the deployment of additional Amorphic accounts as needed in different AWS regions to support the Cloudwick-Customer defined DRP program. Cloudwick will work with the Customer to ensure the DRP includes detailed Service Level Agreements for Disaster Recovery and defines the Recovery Point Objective (RPO) and Recovery Time Objective (RTO) for the respective Amorphic components.
>
> **12.2.2** Managing the Customer's Amorphic data replication across applicable regions.
>
> **12.2.3** Configuring and managing the Customer's Amorphic accounts in the identified AWS regions.
>
> **12.2.4** Managing the Customer's Amorphic backup and restoration strategies.

12.3 Cloudwick will define a Business Continuity Plan ("BCP") with the Customer and maintain the defined Business Continuity Plan ("BCP") for the Customer's Amorphic. The BCP is assessed annually.

13. Customer Responsibilities

13.1 Customer acknowledges that Cloudwick does not assess the contents of Customer Data and that Cloudwick is responsible for enabling appropriate security controls in the Customer's deployment of Amorphic to ensure a level of security appropriate to the particular nature of Customer Data, managing and protecting its accounts, roles and credentials. The Customer agrees to take appropriate steps to pseudonymize Customer Data where appropriate, and to update their Client Software (if any) as required whenever Cloudwick announces an update to Amorphic.

13.2 Customer will promptly notify Cloudwick if a user credential has been compromised or if Customer suspects possible suspicious activities that could negatively impact security of Amorphic or Customer's account.

13.3 Customer may not perform any security penetration tests or security assessment activities without the express advance written consent of Cloudwick.

13.4 Customers whose Customer Data includes PCI, PHI, PII or other sensitive data must agree to the implementation of Cloudwick provided IP whitelisting and MFA in Amorphic and, to the extent Customer Data is subject to PCI-DSS, HIPAA, or FEDRAMP, Customer may only upload such data to Amorphic.