Papaya

Information Security Policy - Security In Cloud

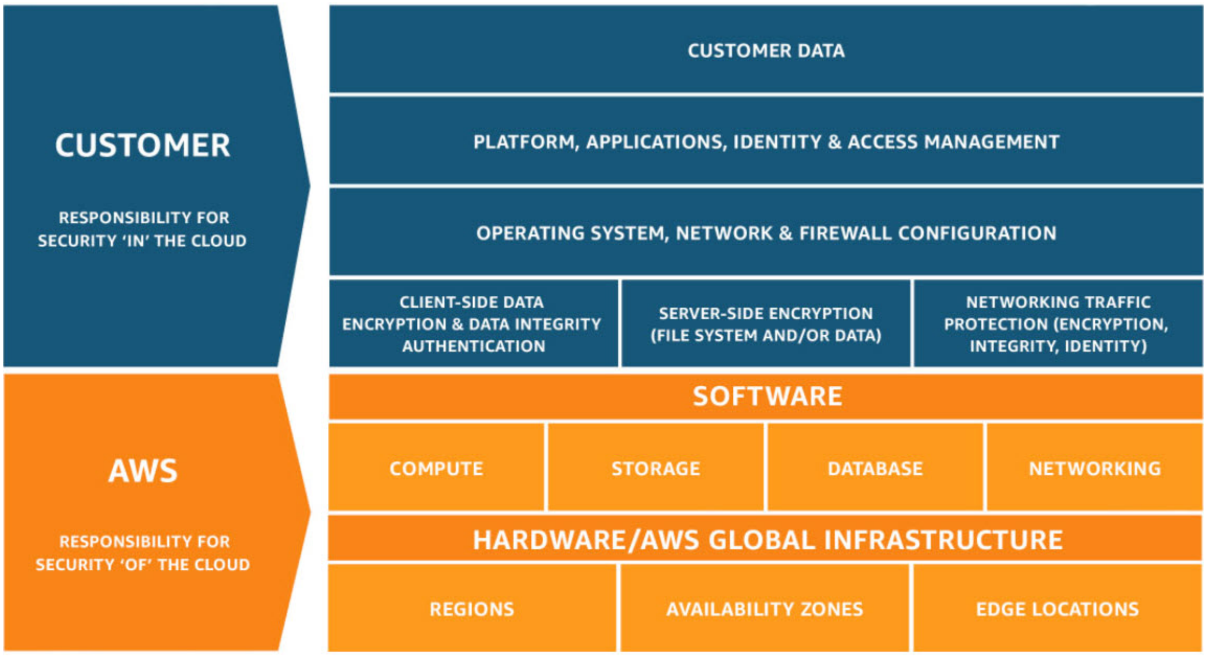
Overview

This document outlines the information security policy in the cloud for Papaya Insurtech. It covers the firewall protection, disaster recovery, data encryption, and data deletion policy.

Version	Review Date	Reviewer	Reviewer Title
1.1	2025-03-10	Loc Truong	CTOO
1.0	2024-03-15	Loc Truong	CTO

Table of Contents

AWS Shared Responsibility Model



CUSTOMER

RESPONSIBILITY FOR SECURITY 'IN' THE CLOUD

CUSTOMER DATA

PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT

OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION

CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION	SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)	NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)

AWS

RESPONSIBILITY FOR SECURITY 'OF' THE CLOUD

SOFTWARE

COMPUTE	STORAGE	DATABASE	NETWORKING

HARDWARE/AWS GLOBAL INFRASTRUCTURE

REGIONS	AVAILABILITY ZONES	EDGE LOCATIONS

Firewall Protection

Firewall Protection Introduction

Papaya's infrastructure is built on AWS, a highly reliable and secure cloud service platform. AWS provides a suite of security features, including Firewall, which Papaya uses to safeguard data. AWS's compliance with various global standards ensures that our encryption practices meet stringent security requirements.

Firewall Protection Strategy

To safeguard our infrastructure, we implement a multi-layered firewall protection strategy. This includes:

- **AWS Security Groups**: Act as virtual firewalls for EC2 instances to control inbound and outbound traffic.
- **AWS Network Firewall**: Provides network-level protection across our Virtual Private Cloud (VPC).

Security Groups

AWS Security Groups are a fundamental component of our security architecture. They enable us to define rules that control the flow of traffic to and from EC2 instances. Key features of our Security Groups configuration include:

- White-listing IPs: Only allow traffic from trusted IP addresses.
- Port Management: Restrict access to specific ports based on application requirements.

Reference: AWS Security Groups Documentation

AWS Network Firewall

While Security Groups provide instance-level protection, AWS Network Firewall offers network-level security for our entire VPC. It allows us to define and enforce policies to protect against threats and ensure compliance.

Reference: AWS Network Firewall Documentation

Implementation Best Practices

To maximize the effectiveness of our firewall protection, we adhere to the following best practices:

- **Least Privilege Principle**: Only allow the minimum necessary access.
- **Regular Audits**: Periodically review and update firewall rules.
- **Logging and Monitoring**: Enable AWS CloudWatch and AWS CloudTrail for continuous monitoring and logging of firewall activity.

Conclusion

Implementing robust firewall protection is crucial for securing Papaya's infrastructure on AWS. By utilizing Security Groups and AWS Network Firewall, we ensure that our applications and data are safeguarded against threats. This layered approach to security not only helps in maintaining compliance but also enhances the overall trust and reliability of our services.

Disaster Recovery (DR)

DR Overview

This Disaster Recovery (DR) outlines the procedures and guidelines for restoring critical databases, and files in the event of a disaster. This document focuses on leveraging AWS cloud services, including RDS, S3 to achieve our DR objectives.

Objectives

- Minimize downtime: Ensure that our services are restored as quickly as possible in the event of a disaster.
- Data integrity: Protect and recover data to prevent loss or corruption.
- Compliance: Meet regulatory requirements for data recovery and business continuity.

Disaster Recovery Team

- **DR Manager**: Oversees the DR process and ensures all procedures are followed.
- **DevOps**: Responsible for the recovery.

DR Plan

RDS (Relational Database Service)

Multi-AZ Deployment:

- Use Multi-AZ deployments for high availability and automatic failover.
- Multi-AZ deployment (near DR) is an AWS managed near-DR solution that provides synchronous replication of your RDS database to a standby instance in a different Availability Zone within the same Region.
- If the primary database becomes unavailable because of an outage at the Availability Zone level, AWS automatically promotes the standby database to the primary role.
- This ensures minimal data loss and downtime.
- Note: Multi-AZ deployment does not protect against Region-level outages.

Metrics:

- RPO: 0
- RTO: 1-2 minutes

AWS Backup:

- Enable automated snapshots and set a 90 days retention period.
- Take manual snapshots before major changes.
- Regularly test backup restoration twice per year to ensure data integrity.

Metrics:

- RPO: 1 hour
- RTO: 30 minutes

S3 (Simple Storage Service)

Versioning:

- Enable versioning on critical S3 buckets to protect against accidental deletions and overwrites.

Lifecycle Policies:

- Implement lifecycle policies to transition data to different storage classes and delete outdated versions.

Cross-Region Replication:

- Enable cross-region replication for critical data to ensure availability in case of a regional disaster.

Recovery Steps:

- In the event of data loss, use S3 versioning to restore the previous versions of the objects.
- If a regional outage occurs, access the replicated data in the alternate region.

Data Encryption

Data Encryption Introduction

Papaya's infrastructure is built on AWS, a highly reliable and secure cloud service platform. AWS provides a suite of security features, including encryption, which Papaya uses to safeguard data. AWS's compliance with various global standards ensures that our encryption practices meet stringent security requirements.

Encryption at Rest

File Storage with Amazon S3

Papaya uses Amazon S3 for scalable file storage solutions. To protect data at rest, we utilize server-side encryption with AES-256. This ensures that all files stored in S3 buckets are encrypted using one of the most secure encryption standards available.

Reference: Amazon S3 Encryption Documentation

Database Management with Amazon RDS

Papaya employs Amazon RDS for database management, ensuring data at rest is protected using AES-256 encryption.

Reference: Amazon RDS Encryption Documentation

Encryption in Transit

To ensure data is secure during transfer, Papaya uses Transport Layer Security (TLS) to encrypt data in transit.

- **TLS Protocol**: Establishes a secure connection by encrypting data before it is sent and decrypting it upon arrival, preventing interception or eavesdropping.
- **Data Encryption Standard**: AES-256

AES-256 Encryption

AES-256 is a symmetric encryption algorithm widely regarded for its security and efficiency. By using a 256-bit key length, it provides a high level of security, making it resistant to various cryptographic attacks.

Key Features of AES-256:

- **Strong Security**: 256-bit key length provides a robust level of security against brute-force attacks.
- **Performance**: Optimized for high performance, ensuring minimal impact on system performance.
- **Compliance**: Meets regulatory requirements for data protection, including GDPR, HIPAA, and more.

Data Encryption Conclusion

Papaya's commitment to data security is demonstrated through the comprehensive application of AES-256 encryption across its AWS cloud infrastructure. By securing data both at rest and in transit, Papaya ensures that customer data remains confidential and protected from unauthorized access.

Data Deletion Policy

Data Deletion Policy Introduction

This document provides an overview of the data deletion process in the system. There are two types of data deletion: soft deletion and hard deletion. Soft deletion is performed first, and if the customer requests it, hard deletion can be performed.

Soft Deletion Data

Stage 1 - Deletion Request

The deletion of Customer Data begins when the customer initiates a deletion request. Generally, a deletion request is directed to a specific resource, Policy/Claim/Claim Document. Deletion requests may be handled in different ways depending on the scope of the customer's request:

Resource Deletion:

- Individual resources containing Customer Data, such as claim documents, can be deleted in a number of ways from the Care Portal or via API.
- Customers may issue a remove of claim document or make a DELETE API request command to delete a document through the API.
- Customers may select a file and delete it from the Insurer Portal.

Account Deletion:

- Customers can request to deactivate the accounts.
- Deactivated accounts cannot log in or perform any action in the system.
- Deactivated accounts can be reactivated later.
- Customers can also request to delete the accounts, which will delete all the data associated with the account.

Stage 2 - Soft Deletion

- Soft deletion is the natural point in the process to provide a brief internal staging and recovery period.
- Ensures time to recover any data that has been marked for deletion by accident or error.
- Data remains in the system until the customer requests hard deletion.
- Audit logs are maintained for all deletion actions.

Hard Deletion Data

Stage 3 - Logical Deletion from Active System

After the data is marked for deletion and any recovery period has expired, the data is deleted successively from Papaya's active and backup storage systems.

For all types of Customer Data except Claim Documents:

- Copies of the deleted data are marked as available storage and overwritten over time.
- In an active storage system, deleted data is stored as entries within a massive structured table.
- Compacting existing tables to overwrite deleted data can be expensive.
- Mark-and-sweep garbage collection and major compaction events are scheduled at regular intervals.

For Claim Documents:

- Customer Data is deleted through cryptographic erasure.
- This is an industry standard technique that renders data unreadable by deleting the encryption keys.
- Logical deletion can be completed even before all deleted blocks are overwritten.

Stage 4 - Expiration from Backup System

- Deleted data is eliminated from backup systems using both overwriting and cryptographic techniques.
- Customer Data is stored within large aggregate snapshots of active systems.
- Full and incremental snapshots are made on daily, weekly, and monthly cycles.
- Backups are retired after a predefined period.
- Cryptographic erasure may occur before backup expiration.

Cloud Provider Data Deletion

The Papaya System is hosted on AWS Cloud. For more information on compliance on AWS, refer to the following documentation:

- Amazon EC2 Compliance
- Amazon RDS Compliance
- Amazon EBS Compliance
- Amazon S3 Compliance

Access Control Guideline

Granting Access Right

An Administrator verifies user identities before they open accounts. The IT Admin is responsible for user registration and de-registration that formally addresses establishing, activating, modifying, reviewing, disabling, and removing accounts. The Admin also removes, disables, or secures default and unnecessary system accounts.

Papaya Insurtech maintains a current listing of all workforce members with access to our claim portal.

Papaya Insurtech implements Role-based access control capable of mapping each user to one or more roles and each role to one or more system functions. The system administrator sets the access control for the storing, processing, or transmitting covered information components with a default 'deny-all' setting for emergency execution.

Role	Level 1: Read Individual Case	Level 2: Download Individual Case	Level 3: Read All Cases	Level 4: Download All Cases	Level 5: Manage Access Control
System Administrator	✓	✓	✓	✓	✓
Head of Claim	✓	✓	✓	-	-
Head of CS	✓	✓	-	-	-
Claim Assessor	✓	-	-	-	-
CS Executive	✓	-	-	-	-

Role	Level 1: Read Individual Case	Level 2: Download Individual Case	Level 3: Read All Cases	Level 4: Download All Cases	Level 5: Manage Access Control
Head of Operations	✓	✓	✓	✓	-
Operations Executive	✓	-	-	-	-

Changing Access Right

When users' access rights change, the company notifies the account managers, who then modify each user's account accordingly. User registration and de-registration, at a minimum, communicate relevant policies to users and require acknowledgment.

Process includes:

- Checking authorization is necessary
- Ensuring minimum level of access is appropriate
- Addressing termination and transfer
- Removing/renaming default accounts
- Removing/blocking critical access rights
- Automatic removal of inactive accounts

Privileged Account

Privileges are methodically authorized, controlled, and allocated to users based on need-to-use and event-by-event.

Key Practices:

- Document access for each system product/element
- Explicitly authorize access to security-relevant functions
- Limit authorization to privileged accounts
- Audit execution of privileged functions
- Prevent non-privileged users from executing privileged functions
- Assign elevated privileges to different user IDs
- Restrict access to privileged functions
- Enable authorized users to determine business partner's access

Data Handling

File System Access:

- Disable access not explicitly required
- Permit access to authorized users for job duties
- Review user access rights after changes
- Maintain documented list of authorized users
- Review critical system accounts every 60 days

- Review all other accounts every 180 days

Physical Security:

- Do not leave covered information unattended
- Protect information during mail services
- Control access to diagnostic and configuration ports
- Disable unnecessary ports and services
- Ensure unique user identification
- Configure BYOD and company devices with automatic lockout

Data Protection:

- Limit access rights to minimum necessary
- Control inter-application access rights
- Specify minimum required outputs
- Encrypt covered information in non-secure areas
- Prohibit unauthorized copying/moving/printing
- Restrict database access

Termination

Process Requirements:

- Remove/modify access rights within 24 hours
- Close old accounts after 90 days
- Reduce/remove access rights before termination
- Require signed Acceptable Use Agreements
- Monitor unauthorized remote connections quarterly
- Review system components and storage logs daily
- Implement process for security control failures