# Cromulent Innovations Cloud Compliance Documentation

(Prepared exclusively for Cromulent Innovations by InterSlice, Inc.)

## 1. Introduction

The objective of this document is to establish a clear and consistent process for documenting compliance with cybersecurity regulations and standards, including CIS benchmarks, to ensure a secure and compliant environment. This Standard Operating Procedure (SOP) applies to all employees, contractors, and third-party vendors involved in managing and securing the organization's information systems.

## 2. Purpose

The purpose of this SOP is to ensure that Cromulent Innovations meets or exceeds cybersecurity regulations and standards, mitigating potential risks and safeguarding sensitive information.

## 3. Scope

This SOP applies to all employees, contractors, and third-party vendors involved in managing and securing the organization's information systems.

## 4. Responsibilities

Cybersecurity compliance documentation is a critical component of the organization's security posture. Compliance analysts are responsible for:

- Planning and leading security audits to ensure compliance with SOX, PCI DSS, HIPAA, and other mandates.
- Coordinating audits with IT departments, both internally and externally.
- Developing and reviewing compliance-related documents.
- Performing vulnerability tests and developing mitigation strategies.
- Designing remediation efforts for security deficiencies.
- Ensuring timely disclosure of cybersecurity incidents to the SEC.
- Planning and maintaining compliance activities according to policies, standards, and industry regulations.
- Identifying and addressing shortcomings in existing security and compliance processes.
- Working with third parties and consultants for independent security audits.

## 5. Prerequisites

Organizations must adhere to various local and international regulations regarding data storage and processing. This includes HIPAA, FISMA, PCI-DSS, GDPR, and ISO/IEC 27001 standards.

#### 5.1 Key Regulations:

- **HIPAA**: Ensures the privacy and security of health information.
- **FISMA**: Governs the security of federal information systems in the U.S.
- **PCI-DSS**: Protects cardholder data for merchants handling payment information.
- **GDPR**: Protects personal data of individuals in the EU and EEA.
- **ISO/IEC 27001**: Provides a framework for managing an Information Security Management System (ISMS).

## 6. Implementation Steps

#### 6.1 Identify Major Security Vulnerabilities

- Conduct a thorough gap assessment of the existing security environment.
- Evaluate alignment with CIS controls and other relevant frameworks.

#### 6.2 Complete Data Classification

- Define and categorize data based on sensitivity and criticality.
- Implement appropriate access controls for each data classification level.

#### 6.3 Conduct a Risk Assessment

- Evaluate and rank risks based on likelihood and potential impact.
- Identify and prioritize security gaps using established risk assessment frameworks (e.g., NIST, CIS).

#### 6.4 Map Security Framework to Compliance Frameworks

- Map the security framework to specific compliance regulations and laws.
- Identify assets and data protected by each regulation.
- Consider jurisdiction-specific requirements and regulations.

### 6.5 AWS Account Security

- Enforce least privilege for IAM roles and policies.
- Enable MFA for all users and the root account.
- Restrict root account usage and secure its credentials.

### 6.6 Logging and Monitoring

- Enable and configure CloudTrail in all regions.
- Set up CloudWatch for monitoring and alerting.
- Enable GuardDuty for continuous threat detection.
- Centralize logs and ensure they are encrypted.

### 6.7 Network Security

- Implement VPC flow logs and restrict traffic with security groups and network ACLs.
- Regularly review and update security group rules.

### 6.8 Data Protection

- Encrypt data at rest and in transit using AWS KMS and TLS/SSL.
- Regularly rotate encryption keys and perform data backups.
- Test backup and restore procedures periodically.

### 6.9 Incident Response

- Develop and maintain an incident response plan.
- Conduct regular incident response simulations.
- Configure automated responses using AWS Lambda and other services.

### 6.10 Compliance and Audit

- Use AWS Config rules to enforce CIS compliance.
- Perform regular security assessments and audits.
- Generate compliance reports for auditing purposes.

## 7. Employee Guidelines

### 7.1 Security Awareness Training

- Conduct regular training sessions on AWS security best practices and incident response.

### 7.2 Access Management

- Ensure individual IAM accounts with MFA enabled.
- Prohibit sharing of IAM credentials and regularly review access permissions.

### 7.3 Data Handling

- Enforce policies for secure data handling and storage.
- Educate employees on data encryption and backup procedures.

### 7.4 Incident Reporting

- Establish clear procedures for reporting security incidents.
- Provide a secure channel for incident reporting.

## 8. Documentation and Record Keeping

- Maintain detailed records of all security policies, procedures, and changes.
- Document all compliance efforts and audit results.
- Keep records of employee training sessions and attendance.

## 9. Review and Improvement

- Conduct regular reviews of the compliance plan.
- Update policies and procedures based on new benchmarks and services.
- Continuously improve security measures based on incident and audit findings.

By adhering to this integrated CIS compliance and SOP document, Cromulent Innovations can ensure a robust and secure AWS environment, meeting or exceeding regulatory requirements and safeguarding sensitive information.

## References:

I have developed this SOP based on these references and the success of each of them. These references provided a comprehensive understanding of how cybersecurity compliance documentation should function and be configured for maximum security.

https://complianceforge.com/example-cybersecurity-documentation/

https://www.comptia.org/content/articles/what-is-cybersecurity-compliance

https://online.utulsa.edu/blog/what-does-a-security-compliance-analyst-do/

https://nordlayer.com/learn/regulatory-compliance/cybersecurity-compliance/

https://arcticwolf.com/resources/blog/10-steps-navigate-cybersecurity-compliance/

| Date | Employee | Change |
|---|---|---|
| 05/29/24 | Julian Pena | “SOP: Compliance Documentation (Cybersecurity Compliance)” |