Cloud4C GRC

Information Security Policy

Rev Number: 1.1

01/05/2018

Contents

1. Introduction

1.1. Process Overview

Cloud4C information security policies describe leadership's direction and position for protecting Company Confidential Information (CCI). These policies ensure practices, processes and controls are implemented to protect CCI created, used and maintained by Cloud4C. No part of any security related documentation is to be outsourced to a third party for document creation or for updating/modifying an existing policy or a process followed within Cloud4C.

1.2. Purpose

- Protect Cloud4C's business information and any client or customer information within its custody by establishing safeguards to protect CCI from theft, abuse, misuse and any form of damage
- Establish responsibility and accountability for information security in the organization Provide an appropriate level of awareness and knowledge to employees, in order to help minimize the occurrence and severity of information security incidents
- Comply with relevant laws, regulations and contractual obligations related to information security

1.3. Scope

This policy is applicable to Information Security and Risk Management (Information Security) functions with a responsibility of developing, maintaining and implementing Information Security Policies, Standards, Minimum Security Baselines (MSBs) and Guidelines.

1.4. Policy

GRC shall develop, maintain, and implement policies, standards, MSBs and guidelines to govern Cloud4C's information security program and requirements to ensure the confidentiality, integrity and availability of CCI as directed by Cloud4C management.

1.5. Actors

- Chief Information Security Officer
- Information Technology Security Advisor (also referred to as IT Security Manager or IT Security Officer)
- Information Owner
- Information Custodian
- Information User

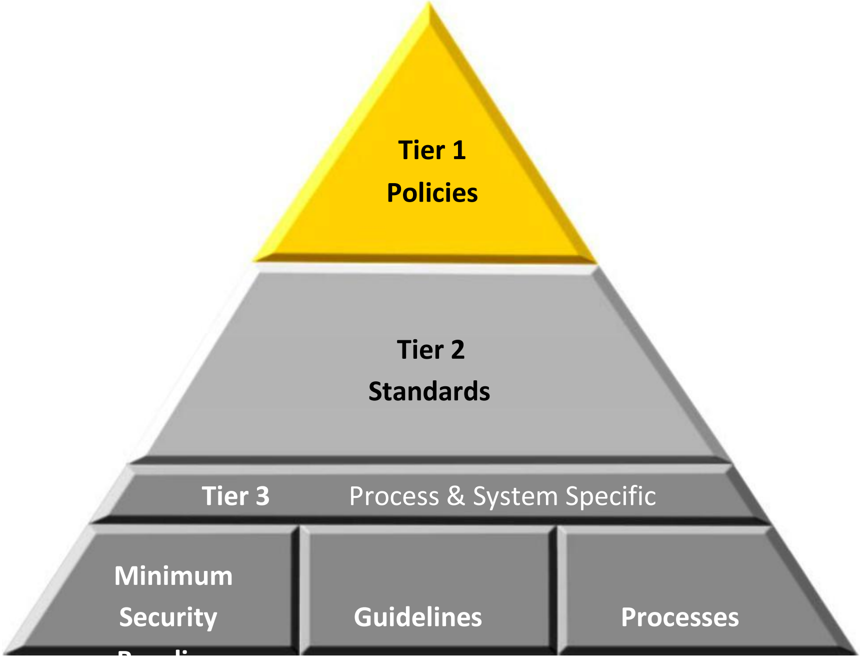
1.6. Applicable Documents

Information Security Policy

2. Process

2.1. Information Security Policy Framework

The Information Security Policy Framework serves as the foundation for all Cloud4C Information Security and Risk activities and as a guide for implementation of practices to minimize the risk to Cloud4C business operations as shown in diagram below.



2.2. Policy Framework Details

Policies, standards, MSBs, processes and guidelines play a key role in securing Company Confidential Information.

2.2.1. Policies

Policies are broad statements from Cloud4C management that guide behavior and set operational goals. Policies are intended to be long-term and guide the development of rules to address specific situations. Polices shall be concise and easily understood.

2.2.2. Standards

Standards are the identified requirements to address security risks, which provide a basis for common practices through-out Cloud4C.

2.2.3. Minimum Security Baselines

MSBs are a set of technical configurations used to ensure that a minimum level of security is provided across multiple implementations of systems, networks and products used through-out Cloud4C (e.g., Windows Server, Web Server, Oracle database, etc.).

2.2.4. Processes

Processes are the detailed business processes that carry out compliance with policies, standards and MSBs.

2.2.5. Guidelines

Guidelines are the statements that recommend conduct for a specific situation. Guidelines are recommendations to consider when assessing the particular level of security needed for each information system.

2.3. Structure of this Policy

There are a total of 16 Information Security policies that govern Cloud4C's information security posture and requirement. The 16 areas are:

Policy #	Policy Name	Policy Contents
1	Information Security Policy Management	Information Security Responsibilities Information Security Policy Lifecycle Information Security Policy Framework
2	Information Management Policy	Information Categorization Information Protection
3	IS Risk Management Policy	Oversight IS Risk Assessment Model Risk Level Matrices IS Risk Acceptance and Tolerance IS Residual Risk Remediation
4	Threat Management Policy	Identifying Threats Threat Analysis Developing Attack Scenarios Implementing Controls and Counter Measures Monitoring and Reporting Threats
5	Vulnerability and Patch Management Policy	Identifying Vulnerabilities Communicating Vulnerabilities Remediating Vulnerabilities Vulnerabilities Metrics
6	Personnel Security Management (HR) Policy	Prior to Employment During Employment Terminations
7	Physical Security Management Policy	Facility Controls and Secure Areas Equipment and Other Media Security
8	Mobile Device Security Management Policy	Mobile Device Management Physical Security Logical Security

		Disposal

Policy #	Policy Name	Policy Contents
		Compliance
9	Infrastructure Security Management Policy	Network Security Management Remote Access Security Management Management of Third Party Network Security Endpoint Protection
10	Access Management Policy	User Access Management Password Management Systems Network Access Control Operating System Access Controls Third Party Access
11	System & Software Lifecycle Management Policy	Security in System and Software Lifecycle Security in Development and Support Processes Third Party Software Developers Minimum Security Baseline Standards (MSBs)
12	Security Monitoring and Event Management Policy	Monitoring and Logging Review and Reporting Log Protection
13	Security Incident and Investigations Management Policy	Incident Identification, Investigation and Analysis Incident Escalation and Reporting Security Incident Response and Investigation
14	Compliance Management Policy	Compliance with Legal, Regulatory and Contractual Requirements Compliance with Information Security Policies, Standards and Minimum Security Baselines Reporting Security Incidents and Violations
15	Cryptographic Key Management Policy	Key Management Approved Cryptography Techniques
16	Off-Premise Policy	Contractual Risk Identification Contractual Security Provisions Vendor Management

2.4. Information Security Responsibilities

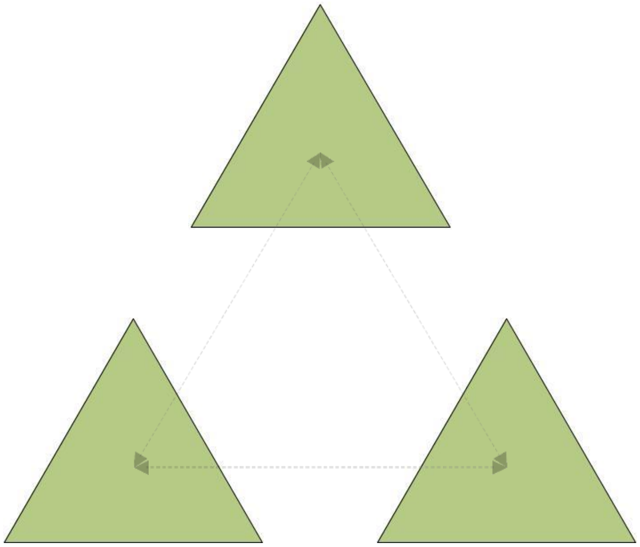
Information Security roles and responsibilities must be clearly defined and communicated to Cloud4C employees and third parties.

2.4.1. Governance Structure

Cloud4C must establish a governance structure to support the Information Security policies and organization within the Cloud4C enterprise.

2.4.1.1. Information Security Triad

The Information Security Triad comprises the three pillars of the Information Security organization including Information Security Governance, Information Security Architecture and Information Security Compliance. The goal of the Information Security Triad is to identify, evaluate and manage risks to Cloud4C and to provide solutions or controls to help eliminate or mitigate those risks. These risks may be internal or external to Cloud4C, and may be discovered through various methods ranging from formal risk assessments to informal audits.



2.4.1.2. Information Security Governance

Information Security Governance oversees the overarching risk management process and handles submission of projects for review (input), risk communication and risk acceptance (output). Information Security Governance represents the management processes within the Information Security Triad.

2.4.1.3. Information Security Architecture

Information Security Architecture performs risk assessments and internal audits, primarily focusing on information technology architecture, application security, and system configuration. Information Security Architecture represents the technology risk review organization within the Information Security Triad.

2.4.1.4. Information Security Compliance

Information Security Compliance evaluates risks as they pertain to legal, regulatory and contractual obligations. Information Security Compliance represents the regulatory risk organization within the Information Security Triad and defines Information Security policy for the Cloud4C enterprise.

2.5. Information Security Policy Lifecycle

Information Security serves as the governing body for Cloud4C Information Security Policies, Standards and MSBs throughout their lifecycle to provide continuous protection of Cloud4C's E-media infrastructure. Business units may create subsidiary-specific information security policies, procedures and standards to meet specific business needs as long as those they do not weaken or conflict with Information Security's policies, standards and MSBs.

2.5.1.1. Implementation and Compliance Monitoring

Information Security is responsible for implementing procedures for monitoring compliance with Information Security Policies, Standards and MSBs. Information Security shall provide self-assessment tools, guidance and oversight to assist Information Owners and Information Custodians with measuring compliance.

2.5.1.2. Exceptions to Policies

Cloud4C employees and third parties are expected to comply with Information Security Policies, Standards and MSBs. In the event that a policy, standard or MSB cannot be adhered to, an exception shall be submitted via email to Information Security (ITSA@Cloud4C.com).

An exception may be granted only if the benefits of the exception outweigh the increased risks, as determined by the Chief Information Security Officer (CISO). Compliance progress shall be validated at the exception expiration date. Exceptions may be closed if the agreed upon solution has been implemented and the exception has been resolved.

An extension may be requested if more time is required to implement the long term solution by completing an extension request. These extensions shall require approval from the next level of management (e.g., Director to Vice President).

2.5.1.3. Additions, Changes, and Deletions

Alterations to established Information Security Policies, Standards, MSBs and Guidelines are made as necessary. Cloud4C business unit leaders may request a new or modification to a policy, or standard by submitting a change request to Information Security. Each request must include the business justification for requesting such a change. Information Security shall review each request and provide recommendations for CIO approval/denial.

Information Security is responsible for ensuring all approved changes or additions to Information Security Policies and Standards are communicated to Cloud4C employees in a timely manner.

2.5.1.4. Review Process

Information Security Policies, Standards and MSBs shall be reviewed based on Section 2.5 Review Intervals below to ensure they are consistent and properly address the following:

- Business needs and business environment – controls remain effective from both a cost and process perspective and support the business without causing unreasonable disruption on the timely execution of those processes
- External technology environment – opportunities and threats created by changes, trends, and new developments
- Internal technology environment – strengths and weaknesses resulting from Cloud4C's use of technology

- Legal, regulatory, and contractual requirements
- Other requirements specific to new or unique circumstances
- Information Security Policies, Standards and MSBs shall be approved by the CISO or designee.

2.5.1.5. Review Intervals

A review of Information Security Policies, Standards and MSBs shall be performed periodically by Information Security. In addition to the annual review, relevant Information Security Policies, Standards and MSBs shall be considered for review and update:

- When a significant change is identified in the technology, business, or regulatory environment that may have a substantial impact on Cloud4C's risk posture
- After the resolution of a significant security incident
- After the performance of an internal or external review that identifies a need for change

2.5.1.6. Dissemination

Information Security Policies, Standards and MSBs shall be published and made accessible to relevant Cloud4C employees and third parties.

Disclosure of Information Security Policies, Standards and MSBs outside of Cloud4C or contracted third parties is not permitted without the approval of Information Security. Appropriate logical and physical security controls must be used to protect electronic and hardcopy Information Security Policies, Standards and MSBs.

2.5.1.7. Disciplinary Action

Cloud4C shall take disciplinary action, as defined by Cloud4C Human Resources, in response to violations of Information Security Policies, Standards and MSBs.

3. RACI Matrix

Responsible	Approver	Consulted	Informed

(R)esponsible – The individual or group who completes the task

(A)ccountable – The individual or group who is responsible for the activity or decision

(C)onsulted – The individual or group to be consulted prior to final decision or action

(I)nformed – The individual or group to be informed after a decision or action is taken

	Roles				
Policy Sections	**Chief Information Officer**	**Information Security & Risk Management**	**Information Owner**	**Information Custodian**	**Information Users**
Information Security Responsibilities	**A**	**R**	**I**	**I**	**I**
Information Security Policy Lifecycle	**A**	**R**	**C**	**I**	**I**
Information Security Policy Framework	**A**	**R**	**I**	**I**	**I**

4. Document Revision History

Revision	Date	Changes
1.0	27/11/2017	New Document
1.1	01/05/2018	Made updates to the Structure and Compliance scope of the policy.

4.1.1.1. Change History

This policy is a living document that will be reviewed and updated annually, or more often if the need arises, based on changes in technology, applications, procedures, business needs, or threats.

Version:	Changed By:	Change Date:
1.0	Krishna Rohit Joysula	25/10/2017
1.1	Vineet Bulbule	01/05/2018

4.1.1.2. Approved By

Approved By:	Approval Date:
Binu Chacko – CISO	27/11/2017
Binu Chacko – CISO	08/05/2018