CLOUD4C

01 January 2022

SYSTEM DEVELOPMENT & MAINTENANCE POLICY

Automation Team

CLOUD4C SERVICES PVT LTD

DOCUMENT CONTROL:

Preparation

Draft	Author	Date
1.0	Sudheer G	17/04/2013
1.1	Sudheer G	14/03/2014
1.2	Soudha Rahman	14/08/2015
1.3	Deepthi Naidu	2/01/2016
1.4	Deepthi Naidu	8/06/2016
1.5	M.Venkataniranjan	16/01/2017
1.6	M.Venkataniranjan	6/01/2018
1.7	M.Venkataniranjan	10/10/2018
1.7	M.Venkataniranjan	05/01/2019
1.7	P Dal Naidu	03/01/2020
1.7	Keerthana ravikanti	31/12/2020
1.7	Saikrishna.N	31/12/2021

Classification	Storage Location
Confidential	Shared folder

Review & Approval

Reviewer & Approver	Version	Date	Reviewed Draft Version
RS Prasad Rao	1.0	17/04/2013	1.0
RS Prasad Rao	1.1	14/03/2014	1.1
RS Prasad Rao	1.2	14/08/2015	1.2
RS Prasad Rao	1.3	2/01/2016	1.3
RS Prasad Rao	1.4	8/06/2016	1.4
RS Prasad Rao	1.5	16/01/2017	1.5
RS Prasad Rao	1.6	6/01/2018	1.6
RS Prasad Rao	1.7	10/10/2018	1.7
RS Prasad Rao	1.7	07/01/2019	1.7
RS Prasad Rao	1.7	03/01/2020	1.7
RS Prasad Rao	1.7	01/01/2021	1.7
Jeeth (Automation Team- VP)	1.7	01/01/2022	1.7

Release

Release Version	**Date Released**
1.0	17/04/2013
1.1	14/03/2014
1.2	14/08/2015
1.3	2/01/2016
1.4	8/06/2016
1.5	16/01/2017
1.6	6/01/2018
1.7	10/10/2018
1.7	07/01/2019
1.7	03/01/2020
1.7	01/01/2021
1.7	01/01/2022

Distribution List

Name	**Designation**	**Department**
COE Teams	COE Engineers	Service Delivery
BU Heads		

Change Control

Version	**Change Reason**	**Effective Date**
1.0	Baseline	17/04/2013
1.1	Added statement of Confidentiality & Reviewed	14/03/2014
1.2	Reviewed and no update	14/08/2015
1.3	Reviewed and no update	2/01/2016
1.4	Reviewed and updated version	8/06/2016
1.5	Reviewed and Updated version and scope	16/01/2017
1.6	Reviewed with no updates	6/01/2018
1.7	Reviewed and added Training section - 7 Review of the policy section -8	10/10/2018
1.7	No updates	05/01/2019
1.7	Reviewed and no updates	03/01/2020
1.7	Reviewed and no updates	31/12/2020
1.7	Reviewed and no updates	31/12/2021

STATEMENT OF CONFIDENTIALITY

This document contains proprietary trade secret and confidential information to be used solely for evaluating Cloud4C Services Private Ltd. The information contained herein is to be considered confidential. Customer, by receiving this document, agrees that neither this document nor the information disclosed herein, nor any part

CONTENTS

1 INTRODUCTION

This policy sets out the process that shall be followed during the system development stages. This will ensure that a standardized approach is followed that will require:

- Recording of all development requirements
- Recording as to whether those requirements are appropriate, taking into account of all interoperability / interfaces with other information systems
- Drafting a work plan to ensure that development is controlled
- System changes are tested prior to implementation
- System documentation is kept up-to-date

Building security into systems during their development is more cost-effective and secure than applying it afterwards. It requires a coherent approach to systems development as a whole, and sound disciplines to be observed throughout the development cycle. Ensuring that information security is addressed at each stage of the cycle is of key importance.

2 OBJECTIVE

The aim of this policy is to ensure that security is an integral part of information systems and also to ensure that process for all security requirements are identified at the requirements phase of a project and justified, agreed, and documented as part of the overall business requirements for information system.

3 SCOPE

This procedure shall be applicable to all employees of Cloud4C, its contractors, subcontractors, associated third parties who are users of Cloud4C services or who have access to Cloud4C facility..

4 POLICY STATEMENT

4.1 System Development and Maintenance General Guidelines

- Security requirements for new systems or enhancements to existing systems shall be analyzed and necessary controls shall be introduced.
- Appropriate validation checks shall be applied to validate input and output data to ensure that it is correct and appropriate. In the case of sensitive data, additional controls shall be incorporated as required.
- Changes to documents/sources of application input data and implementation changes shall be done by using a change control procedure.
- Responsibilities of all personnel involved in data input or output process shall be defined.
- Validation checks shall be performed to detect any processing errors that may lead to incorrect results/output in the data processed.
- Message authentication such as PKI (Public Key Infrastructure) shall be implemented for critical applications as deemed appropriate from the perspective of protecting the data integrity.
- Capacity demands shall be monitored before planning for the introduction of new business and system requirements to ensure the availability of processing power and storage.

- The risk assessment shall be done before the introduction of new applications/systems and care shall be exercised not to disrupt existing application/system.
- Application systems shall be reviewed and tested when the changes occur.
- Acceptance criteria shall be clearly defined for upgrades of systems and new versions.
- Acceptance tests shall be planned and carried out as per the plan.
- Installation of the additional software other than the standard software build on the operational systems shall be controlled.
- The purchase, use, and modification of software shall be controlled and checked to protect against any virus/worms / Trojans etc.
- Provision shall be made to restore the original system, in case the new introduction does not function after going ‘live’.
- Test data used for system or acceptance testing shall be as close to the operational data and care shall be taken to avoid personal data, where possible and adequate controls shall be implemented to protect the test data and test results.
- Strict controls shall be implemented to secure the source code and related libraries.
- The operational data shall be used in testing with due authorization and shall be erased from the test system on completion of testing. A log shall be maintained for use of operational data and information logged shall be audited.
- Operating procedures for systems shall be documented and an activity log as appropriate detailing the activity shall be maintained. This activity log shall be monitored periodically for compliance with the procedures.
- There shall be a mechanism for fault logging and clear rules for handling the reported faults. The environment shall be constantly monitored for any adverse event.
- The fault logs shall be reviewed periodically. Any corrective action shall be within the prescribed controls and shall be duly authorized by the respective supervisors.

5 SECURITY IN APPLICATION DEVELOPMENT AND MAINTENANCE

A formal methodology shall be defined and documented for application development and maintenance process.

- All applications developed internally shall follow the defined application development and maintenance process.
- Security requirements in an information system shall be identified and documented during the requirements gathering and analysis phase of development/change of application software. They shall be justified and agreed with business process owners.
- Systems security requirements shall reflect the business value of the information assets involved *(Refer: ISMS - Asset Classification Policy and Procedures)* and the potential damage that may be caused due to the absence of sufficient security.
- Appropriate security controls including audit trails and activity logs shall be designed into application systems, including user-written applications. These shall include controls for validation of input data, internal processing and output data.
- All changes to applications shall follow a defined change control *procedure (Refer: ISMS – Change Management Policy and Procedure)*. All proposed system changes shall be authorized and reviewed to verify that they do not compromise the security of either the system or the operating environment.
- Applications shall be reviewed and tested prior to installation of OS patches or updates in a test environment in order to ensure that there is no adverse impact on security due to the changes in the operating system.

- Cloud4C shall ensure that notifications of changes to the operating system are provided in time to allow appropriate tests and reviews to take place before implementation.
- Cloud4C shall ensure that technical vulnerabilities of information systems being used shall be evaluated at the right time and measures shall take to address the associated risk. Roles and responsibilities for vulnerability management (which includes vulnerability monitoring, vulnerability risk assessment, asset tracking, patch testing and management) should be clearly defined.
- In case of patches not available for the identified vulnerabilities, Cloud4C shall ensure that the following shall be implemented:
    - turning off services or capabilities related to the vulnerability
    - adapting or adding access controls
    - increased monitoring to detect or prevent actual attacks
    - raising awareness of the vulnerability
- Cloud4C shall maintain an audit log for all the technical vulnerability management procedures performed and it should regularly monitor the effectiveness and efficiency of the vulnerability management process.
- Specific procedures shall be defined for controlling access and management of the following to minimize the risk of corruption and unauthorized access and changes to software programs:
    - Production software
    - Test data and test applications
    - Program source library
- If the software is developed by a third party the following process shall be followed:
    - Cloud4C shall ensure that software development processes comply with Cloud4C application development and maintenance methodology.
    - Cloud4C shall have appropriate licensing agreements and contractual requirements to ensure appropriate software necessary for the development are used.
    - Cloud4C shall obtain assurance from the third party for the quality and accuracy of the work carried out.
    - Cloud4C shall be the owner of the source code of the software developed. In the case of Cloud4C being not the owner of the source code then the source code shall be maintained under escrow arrangement, mutually agreed with the third party.
    - Cloud4C shall obtain the rights of access for an audit of the quality and accuracy of the work carried out.
    - Cloud4C shall perform testing processes as per Cloud4C application development and maintenance methodology.
    - Cloud4C shall ensure scanning of outbound media, periodic monitoring of system activities shall be carried out to ensure no information leakage shall occur.

6 SECURITY IN DEVELOPMENT AND SUPPORT PROCESSES

- Change control processes *(Refer: ISMS – Change Management Policy and Procedure)*
    - Cloud4C change control procedures shall be compliant with or based on accepted systems development and maintenance methodology.
    - The change control processes must be used for all changes (including configuration changes) to software, hardware, and communications links.
    - System documentation must be updated to reflect changes.

    - An audit trail and version control must be maintained for all the changes made.
- Technical review of operating system changes
    - Cloud4C change control procedure shall address all changes, enhancements, installations of new software patches and version updates.
    - Before application of the updates in the production ('live') environment, Cloud4C shall test the operation and compatibility of the proposed updates with existing application.
    - All updates, patches, version changes, etc. must be tested and reviewed for security controls before implementation.
- Restrictions on changes to software packages
    - Modifications to software packages should be discouraged. As far as possible, and practicable, vendor-supplied software packages shall be used without modification.
    - All modifications (including configuration changes, changes to reports, etc.) to software packages must be made under Cloud4C program change control procedures.
- Covert channels and Trojan code
    - Cloud4C program change control procedures shall include procedures for the inspection of software source code for possible 'Trojan' code or 'covert' channels.
    - Cloud4C shall request that the vendor guarantees that the software is free of 'Covert channels' and 'Trojan' code when purchasing the software from third parties.
- Information leakage: Opportunities for information leakage shall be prevented. The following should be considered to limit the risk of information leakage, e.g. through the use and exploitation of covert channels:
    - Scanning of outbound media and communications for hidden information.
    - Masking and modulating system and communications behaviour to reduce the likelihood of a third party being able to deduce information from such behaviour.
    - Making use of systems and software that are considered to be of high integrity, e.g. using evaluated products *(Refer: ISMS – Systems Planning and Acceptance Policy and Procedure).*
    - Regular monitoring of personnel and system activities.
    - Monitor resource usage in computer systems.
- Outsourced software development
    - Cloud4C requirements for outsourced software development shall include compliance with Cloud4C program change control procedures or equivalent program change control procedures.
    - Cloud4C requirements for outsourced software development shall include compliance with acceptable systems development and maintenance methodology.
    - A process shall be implemented to verify the vendor's compliance with Cloud4C requirements.
    - All outsourced developments shall adhere to the Compliance Policy of GISMO.
    - If third party software is being considered for critical business activity, Cloud4C shall license the source code from the third party.
    - The third-party shall provide source code to an outside party who will hold the source code in escrow each time the source code is revised.
    - All documentation, which describes systems or systems procedures, shall be reviewed by the Head - Information security to ensure that confidential

information is not being inadvertently disclosed, before being released to third parties.

7 TRAINING

Cloud4C shall ensure all team members undergo periodical training outlined in this policy.

8 REVIEW OF THE POLICY

- This document will be reviewed and updated on an annual basis or when significant changes occur to the organization systems and information security standards.

9 COMPLIANCE WITH THE POLICY

Compliance with the System Development and Maintenance Policy and Procedure shall be mandatory. Head Information security–Cloud4C, assisted by information security forum shall ensure continuous compliance to this policy and procedure within Cloud4C. The periodic review shall be conducted by Departmental Heads and shall be reported to Head – Information security to verify compliance to this policy and procedure. All employees shall be responsible to inform the Head– Information security if any policy breach is discovered or identified.

10 VIOLATION WITH THE POLICY

Any user found to have violated this System Development and Maintenance Policy and Procedure may be subjected to disciplinary action, up to and including termination of employment.

10.1 Consequences of violation of the Policy

Disciplinary action shall be consistent with the severity of the incident, as determined by an investigation, and may include, but not be limited to:

- Loss of access privileges to information assets, and
- Other actions as deemed appropriate by Management, Human Resources, and the Legal Department.

11 CONTACT ROLE FOR CLARIFICATION REGARDING THE POLICY

The sponsor of this policy is the Head – Information security – Cloud4C. Head – Information security – Cloud4C shall be responsible for the maintenance and accuracy of the policy. Any questions regarding this policy shall be directed to the Head – Information security.

12 WAIVER CRITERIA

This Policy and Procedure is intended to address information security requirements. Requested waivers shall be formally submitted to the Head - Information security including justification and benefits attributed to the waiver for approval. The waiver shall only be used in exceptional situations for communicating non-compliance with the policy for a specific period (subject to a maximum period of 30 days). After the time period the need for the waiver shall be reassessed and re-approved, if necessary. The waiver shall not be provided for more than three consecutive terms. The waiver shall be monitored to help ensure its concurrence with the specified period and exception.