CLOUD4C

2021

CISO ITSA ROLES

Compliance Team

CLOUD4C SERVICES PVT LTD

DOCUMENT CONTROL

Preparation

Draft	Author	Date
1.0	Vineet Bulbule	4/01/2019
1.0	Vineet Bulbule	4/01/2020
1.0	Ashrith Karru	01/01/2021

Classification	Storage Location
Confidential	Shared folder

Review and Approval

Reviewer & Approver	Version	Date	Reviewed Draft Version
Binu Chacko	1.0	5/01/2019	1.0
Ashvin Parankusha	1.0	6/01/2020	1.0
Sreeram Chilakamarri	1.0	02/01/2021	1.0

Change Control

Version	Change Reason	Effective Date
1.0	New document created	5/01/2019
1.0	No updates in the document	6/01/2020
1.0	No updates in the document	02/01/2021

STATEMENT OF CONFIDENTIALITY

TABLE OF CONTENTS

Document Control 1
Preparation 1
Review and Approval 1
Change Control 1
1 CHIEF INFORMATION SECURITY OFFICER 3
1.1 Service Delivery 3
1.1.1 Supports System Security 3
1.1.2 Delivers Service Excellence 3
1.1.3 Leads and Develops People 3
1.1.4 Supports Shared Purpose and Direction 3
1.2 Information Security 3
1.2.1 Analyses and Evaluates 3
1.2.2 Applies Technical Proficiency 4
1.3 Technology Audit 4
1.4 Strategic and Emerging Level Technology Monitoring 4
2 INFORMATION TECHNOLOGY SECURITY ADVISOR (ITSA) 5
2.1 Service Delivery 5
2.1.1 Supports System Security 5
2.1.2 Delivers Service Excellence 5
2.1.3 Leads and Develops People 5
2.1.4 Supports Shared Purpose and Direction 5
2.2 Information Security 5
2.2.1 Analyses and Evaluates 5
2.2.2 Applies Technical Proficiency 6
2.3 Technology Audit 6
2.4 Emerging Technology Monitoring 6

1 CHIEF INFORMATION SECURITY OFFICER

1.1 Service Delivery

1.1.1 Supports System Security

- Reviews reports on, or analyses information on, security incidents and patterns to determine remedial actions to correct vulnerabilities

1.1.2 Delivers Service Excellence

- Develops and manages customer service performance requirements for information security
- Ensures information ownership responsibilities are established for each information system and implements a role-based access scheme
- Liaises with stakeholders to establish mutually acceptable contracts and service agreements

1.1.3 Leads and Develops People

- Performs project management duties where appropriate
- Directs the implementation of appropriate operational structures and processes to ensure an effective information security program
- Provides direction to system developers and architects
- Oversees and information security section
- Acts as a mentor
- Co-ordinates communication, awareness and training in information security for the agency

1.1.4 Supports Shared Purpose and Direction

- Develops strategies for ensuring the security of automated systems
- Ensures that the policy and standards for security are fit for purpose, current and are correctly implemented
- Reviews new business proposals and provide specialist advice on security issues and implications
- Advises the appropriate stakeholders of changes affecting the organisation's information technology security posture
- Works with system owners to determine appropriate information security policies for their systems and to respond to recommendations from audits
- Works with system owners to obtain and maintain the accreditation of their systems
- Provides technical advice to committees, including other agency and inter-agency committees as required
- Maintains security knowledge base

1.2 Information Security

1.2.1 Analyses and Evaluates

- Specifies organisational procedures for the assessment of an activity, process, product or service, against recognised criteria, such as ISO 27001

- Provides leadership and guidelines on information assurance security expertise for the organisation, working effectively with strategic organisational functions such as legal experts and technical support to provide authoritative advice and guidance on the requirements for security controls
- Reviews security plans and procedural documentation, including disaster recovery plans, to ensure that information security incidents are avoided during shutdown and long term protection of archived resources is achieved

1.2.2 Applies Technical Proficiency

- Evaluates and approves development efforts to ensure that baseline security safeguards are appropriately installed
- Provides for the restoration of information systems by ensuring that protection, detection, and reaction capabilities are incorporated
- Recommends and schedules information security-related repairs within the organisation's infrastructure and undertakes more complex repairs
- Validates the planning and scheduling of the installation of new or modified hardware, operating systems, and software applications ensuring integration with information security requirements for the infrastructure

1.3 Technology Audit

- Develops plans for risk-based audit coverage of technology systems for inclusion in audit planning and uses experience to ensure audit coverage is sufficient to provide the business with the assurance of adequacy and integrity
- Leads and manages complex technical audits, managing specialists contracted to contribute highly specialised technical knowledge and experience
- Identifies areas of risk and specifies interrogation programs. Recommends changes in processes and control procedures based on audit findings, including, where appropriate, the assessment of safety-related software systems to determine compliance with standards and required levels of safety integrity
- Provides general and specific advice, and authorises the issue of formal reports to management on the effectiveness and efficiency of control mechanisms
- Reviews or develops effective vulnerability countermeasures
- Reviews the report of, or participates in, an information security risk assessment or review. Oversees the development of the audit planning process
- Reports to senior managers on technical aspects of information security management, and compliance with and enforcement of policies across the agency

1.4 Strategic and Emerging Level Technology Monitoring

- Co-ordinates the identification and assessment of new and emerging hardware, software and communication technologies, products, methods and techniques
- Evaluates likely relevance of these for the organisation. Provides regular briefings to staff and management
- Works with the Chairman and Managing Director (CMD) to formulate the organisation's information security budget
- Interprets and/or approves security requirements as they relate to the capabilities of new information technologies, taking into account organisational policies and government guidelines and legislation

- Ensures that protection and detection capabilities are acquired or developed using an engineering approach and are consistent with the organisation's information technology security architecture
- Identifies security program implications of new technologies or technology upgrades

2 INFORMATION TECHNOLOGY SECURITY ADVISOR (ITSA)

2.1 Service Delivery

2.1.1 Supports System Security

- Reviews information systems for actual or potential breaches in security and ensures that all identified breaches in security are promptly and thoroughly investigated
- Ensures that security records are accurate and complete including certification documentation
- Validates and authorises user and access administration on systems under the defined policies, standards and procedures of the agency
- Ensures patches are applied and removes known system weaknesses under information security policies and standards

2.1.2 Delivers Service Excellence

- Develops and manages customer service performance requirements for information security
- Assists operational staff to locate and repair information security problems and failures

2.1.3 Leads and Develops People

- Provides direction to system developers regarding the correction of security problems identified during testing
- Provides on the job training and coaching for team members

2.1.4 Supports Shared Purpose and Direction

- Drafts and maintains the policy, standards, procedures and documentation for security
- Interprets security policy and contributes to the development of standards and guidelines that comply with this
- Monitors contract performance and reviews deliverables and contract requirements related to organisational information technology security and privacy
- Communicates with system owners and personnel to increase their awareness of applicable information security policies and standards

2.2 Information Security

2.2.1 Analyses and Evaluates

- Conducts security risk assessments for business applications and computer installations; provides authoritative advice and guidance on security strategies to manage the identified risk
- Investigates major breaches of security, and recommends appropriate control improvements

- Writes and publishes reports on incident outcomes and distributes to appropriate stakeholders
- Analyses information security incidents and patterns to determine remedial actions to correct vulnerabilities
- Monitors and evaluates the effectiveness of the organisation's information security procedures and safeguards for the infrastructure
- Develops and implements the necessary security plans and procedural documentation, including disaster recovery plans, to ensure that information security incidents are avoided during shutdown and long term protection of archived resources is achieved
- Reports unresolved network security exposures, misuse of resources or noncompliance situations to an ITSM

2.2.2 Applies Technical Proficiency

- Ensures that any system changes required to maintain security are implemented
- Recommends and schedules information security-related repairs, upgrades or project tasks within the organisation's environment
- Writes and maintains scripts required to ensure the security of the infrastructure's environment
- Plans and schedules the installation of new or modified hardware, operating systems, and software applications ensuring integration with information security requirements for the infrastructure
- Schedules and performs regular and special backups on all infrastructure systems

2.3 Technology Audit

- Evaluates functional operation and performance in light of test results and makes recommendations regarding certification or accreditation
- Examines vulnerabilities and determines actions to mitigate them. Develops and applies effective vulnerability countermeasures
- Analyses information security vulnerability bulletins for their potential impact on the computing or network environment, and takes or recommends appropriate action
- Performs risk assessment, business impact analysis and accreditation for all major information systems within the organisation
- Interprets patterns of non-compliance to determine their impact on levels of risk and/or overall effectiveness of the organisation's information technology security program
- Oversees the development of organisational logging standards to comply with audit requirements.
- Manages and audits system event logs

2.4 Emerging Technology Monitoring

- Monitors, the market to gain knowledge and understanding of currently emerging technologies
- Identifies new and emerging hardware and software technologies and products based on own area of expertise, assesses their relevance and potential value to the organisation, contributes to briefings of staff and management
- Formulates or provides input to the organisation's information security budget
- Develops network security requirements specific to acquisition for inclusion in procurement documents