UNITED ARAB EMIRATES
MINISTRY OF CABINET AFFAIRS
PRIME MINISTER'S OFFICE

الإمـارات العـربـيـة المتـحـدة
وزارة شـــؤون مجـلـــس الـــوزراء
مكتب رئاسة مجلس الوزراء

NATIONAL CLOUD SECURITY POLICY

May 2023 Version 1.0

DISCLAIMER

This document is the sole property of UAE Cyber Security Council and is approved by the UAE Cabinet.

The UAE Cyber Security Council reserves the right to amend, add, or delete any section of this Policy.

Neither the whole nor part of this document shall be reproduced without the prior written consent of the UAE Cyber Security Council.

VERSION CONTROL

Version	0.1
Date:	21 February 2022
Prepared by:	CSC
Amendment Content:	Initial Draft

Version	0.2
Date:	08 March 2022
Prepared by:	CSC
Amendment Content:	Updates as per session held on 24 February 2022 with ADDA

Version	1.0
Date:	25 August 2022
Prepared by:	CSC
Amendment Content:	Updates as per review comments on the draft v0.2 of the document

	Reviewed by	Approved by
Designation:	xxxxxxxxx	xxxxxxxxx
Name:	xxxxxxxxx	xxxxxxxxx
Signature:	xxxxxxxxx	xxxxxxxxx
Date:	xxxxxxxxx	xxxxxxxxx

Table of Contents

Table of Contents

2. Cloud Consumers

Table of Contents

Table of Contents

SECTION 1

INTRODUCTION

INTRODUCTION

Cloud computing in recent times has brought in rapid advances in the delivery of digital services. It is also a key driving force in future technology breakthroughs, big data analytics, Artificial Intelligence (AI) and the Internet of Things (IoT). While its adoption has seen dramatic changes in providing cost-effective, agile, scalable, on-demand technology services to customers, like any emerging technology, cloud computing has also introduced unique complexities and cyber security challenges.

The increased adoption of cloud services locally and globally, naturally entails an increase in the threat landscape. Ensuring the security of the UAE’s digital transformation requires a holistic approach, which addresses risks and enables innovation.

The Council has established this policy to enhance cloud security, aligned with the UAE’s national priority to be a global leader in cyber security; and enhance the security posture of organizations and individuals within the UAE using cloud services.

1.1 Purpose

This policy aims to strengthen the cloud security posture of the UAE by outlining the principles for the adoption of secure cloud computing practices and addressing the challenges in the current cloud computing landscape. The policy will further provide guidance to the cloud ecosystem in the UAE, define requirements for cloud security and outline the oversight and enforcement of cloud security mandates.

The policy will help ensure Cloud Service Providers (CSP) achieve a set of security requirements and ensure all Cloud Service Consumers are well protected when procuring and using said services. The policy also aims to avoid the potential negative impacts of implementation, such as inhibiting investment and stunting the growth of the cloud computing sector due to overly stringent requirements.

1.2 Scope & Applicability

Achieving a resilient cloud security posture requires security responsibilities to be clearly defined and understood by the involved parties. The CSC understands that cloud computing is not unidimensional, and responsibilities vary according to service models. However, the implementation of security controls will be the ultimate responsibility of the entity using cloud services. A model outlining the applicability of the requirements based on the service model has been developed.

The services are defined as follows:

Software as a Service (SaaS)

The consumer is provided with the capability to use the provider’s applications running on a cloud infrastructure. The applications are remotely accessible from various client devices, such as a web or a program interface. The consumer is limited to application use and cannot manage or control the underlying cloud infrastructure employed.

Platform as a Service (PaaS)

The consumer is provided with the capability to deploy consumer-created or acquired applications onto the cloud infrastructure, utilizing programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure.

Infrastructure as a Service (IaaS)

The consumer is provided with the capability to provide essential computing resources, such as processing, storage, and networks, to deploy and run arbitrary software, including operating systems and applications.

1.2 Scope & Applicability

Cloud Consumers:

Critical Information Infrastructure (CII) Entities
The Cloud Security Policy is mandated on UAE government and critical infrastructure entities looking to procure and leverage cloud computing services in the UAE. Refer to the UAE Critical Information Infrastructure Policy for a detailed list of CII Sectors.

Commercial Entities (non-CII)
The Cloud Security Policy is NOT mandated on commercial consumers looking to procure cloud computing services in the UAE and will serve as an advisory guide only.

Cloud Service Providers (CSP):

This Cloud Security Policy is mandated on entities looking to provide cloud computing services in the UAE. All Cloud Service Providers must abide by the requirements set out within this policy.

1.3 Adoption Lifecycle

The National Cyber Security Governance Framework (NCSGF) outlines a common integrated approach for managing and adopting cyber security at the entity, sector, and national levels. The NCSGF introduces a lifecycle for Understanding, Assessing, Implementing, Monitoring and Collaborating cyber security within UAE. This lifecycle ensures continual improvement of the UAE's cyber security capabilities providing requirements for emerging technologies, such as cloud computing, are well defined, managed, and adopted.

Understanding the drivers for transitioning to cloud service, the skills required and how the business strategy aligns with the overall digital transformation objectives.

Assessing risk-benefit to identify the threats, determine the impact on business, identify relevant security controls to mitigate the risks and select the appropriate cloud deployment model.

Implementing the identified security controls on the selected cloud deployment model based on risk assessment.

Monitoring and reviewing the implemented controls and cloud service provider's performance and effectiveness in conformance to the National Cloud Security Policy.

Collaborating to realize the benefits of improved efficiency to increase customer value.

1.4 Cloud Security Principles

The following five cloud security principles are laid out to provide decision-makers with foundational elements to drive secure cloud adoption, implementation, and operations in the UAE. These principles assist cloud consumers, and cloud service providers to make policy, operational, and procurement decisions in line with the policies detailed in this document.

Risk-Based Approach

Potential risks to security and resilience are considered in the evaluation process for cloud adoption and expansion.

Data- Driven Cloud Security

Cloud security practices are in line with data sensitivity, its business impact and privacy expectations.

Best Practice Guidelines

Global best practice frameworks are leveraged to provide security assurance and drive compliance efficiencies.

Collaborative & Transparent Ecosystem

Open sharing of information, good practices, incident reporting and intelligence is encouraged in the cloud ecosystem among cloud consumers, cloud service providers and regulators.

Continual improvement

Cloud security practices are improved continually for suitability, adequacy and effectiveness.

1.5 Exception Approval

A policy exception may be granted by the Cyber Security Council under special circumstances.

Exceptions will be reviewed on a case-by-case basis and their approval is not guaranteed.

SECTION 2

CLOUD CONSUMERS

The following section outlines the policy domains and sub-domains applicable to cloud consumers in the UAE. The policy sub-domains further elaborate on the objectives and policy statements.

2.1 Cloud Governance

2.1.1 Governance Framework

Version	1.0

Adoption Lifecycle

Understanding	Assessing	**Implementing**	Monitoring	Collaborating

Service Model Applicability

IaaS	PaaS	SaaS

Policy Objective

To establish leadership and governance to initiate and support the implementation of cloud security requirements.

Policy Statements

2.1.1.1 The senior leadership of the cloud consumer shall mandate the establishment of a cloud security program with apparent oversight and direction and assign resources (budget, people, and technology) for the successful implementation of the program.

2.1.1.2 Cloud consumers shall establish and document policies governing critical aspects of cloud security and a process to identify and ensure compliance with the cloud service's applicable legal and regulatory requirements.

2.1.1.3 When procuring cloud services, cloud consumers shall ensure its CSP has a suitable governance framework in place.

2.1 Cloud Governance

2.1.2 Risk Management

Version 1.0

Adoption Lifecycle

Understanding	**Assessing**	Implementing	Monitoring	Collaborating

Service Model Applicability

IaaS	PaaS	SaaS

Policy Objective

To proactively identify and remediate cloud security and privacy risks in a timely manner.

Policy Statements

2.1.2.1 A robust and continuous risk management program shall be established and implemented to include the cloud environment.

2.1.2.2 Security and privacy risk assessments shall be conducted to analyze the impact on data/assets hosted within the cloud environment.

2.1.2.3 Effective internal and external risk communication and consultation shall be undertaken at all stages of risk assessment.

2.1 Cloud Governance

2.1.3 Personnel Security

Version 1.0

Adoption Lifecycle

Understanding | Assessing | **Implementing** | Monitoring | Collaborating

Service Model Applicability

IaaS | PaaS | SaaS

Policy Objective

To ensure personnel accessing the cloud environment understand their responsibilities and receive regular security training.

Policy Statements

2.1.3.1 Cloud consumers shall follow security requirements stated in the National Cyber Security Policy for all personnel (employees, vendors and contractors) supporting cloud services.

2.1.3.2 Cloud consumers shall ensure contractual clauses with CSP's include (i) background screening of CSP personnel, (ii) clearly defined roles, and responsibilities matrix with segregation of duties in a shared responsibility model, (iii) regular user awareness and training program, (iv) a disciplinary process, and (v) orderly exit process, including contract termination.

2.1 Cloud Governance

2.1.4 Third Party and Supply Chain Security

Version 1.0

Adoption Lifecycle

Understanding	Assessing	Implementing	Monitoring	Collaborating

Service Model Applicability

IaaS	PaaS	SaaS

Policy Objective

To reduce the likelihood of supply chain compromise.

Policy Statements

2.1.4.1 Cloud consumers shall be aware of the information shared with or accessible by the CSP’s third party suppliers and their supply chain.

2.1.4.2 Cloud consumers shall identify the security risks of using supply chain resources.

2.1.4.3 Cloud consumers shall liaise with the CSP to understand third party suppliers’ compliance with the cloud security requirements.

2.1 Cloud Governance

2.1.5 Assurance and Independent Testing

Version	1.0

Adoption Lifecycle

Understanding	Assessing	Implementing	Monitoring	Collaborating

Service Model Applicability

IaaS	PaaS	SaaS

Policy Objective

To ascertain effective implementation of cloud security controls through independent testing and reduce reliance on supplier assertions.

Policy Statements

2.1.5.1 Cloud consumers shall engage a third party with adequate skills to conduct independent security control implementation testing.

2.1.5.2 Cloud consumers shall conduct independent assurance testing in service design and service components.

2.2 Contractual Agreements

2.2.1 Due Diligence

Version 1.0

Adoption Lifecycle

Understanding	Assessing	Implementing	Monitoring	Collaborating

Service Model Applicability

IaaS	PaaS	SaaS

Policy Objective

To protect the confidentiality of the cloud consumer’s data in the cloud environment.

Policy Statements

2.2.1.1 Cloud consumer shall perform legal due diligence and review all contractual obligations in detail prior to engaging any cloud services and/or CSPs to ensure that the use of any cloud services and/or CSPs will be commensurate with the organization’s risk profile.

2.2.1.2 As part of the contractual agreements, a non-disclosure agreement shall be drafted and formalized, and signed by both parties before cloud computing services are procured.

2.2 Contractual Agreements

2.2.2 Service Level Agreements

Version 1.0

Adoption Lifecycle

Understanding	Assessing	Implementing	Monitoring	Collaborating

Service Model Applicability

IaaS	PaaS	SaaS

Policy Objective

To pre-emptively protect the rights of the cloud consumer and CSP.

Policy Statements

2.2.2.1 As part of the contractual agreements, a Service Level Agreement detailing availability, quality of services provided, and actions in the case of a network outage, data loss, or security breach, etc. shall be drafted and formalized, and signed by both parties before cloud computing services are procured.

2.3 Data Security and Lifecycle Management

2.3.1 Data Governance

Version 1.0

Adoption Lifecycle

Understanding | Assessing | **Implementing** | Monitoring | Collaborating

Service Model Applicability

IaaS | PaaS | SaaS

Policy Objective

To ensure data classification and protection from unauthorized use, access, loss, destruction, and falsification.

Policy Statements

2.3.1.1 Policies and procedures shall be established and implemented for data classification, labelling and handling throughout its' lifecycle to secure the data that is resident (permanently or temporarily) within the service's geographically distributed (physical and virtual) applications, infrastructure, network and systems components and shared with other third parties to ascertain any regulatory, statutory, or supply chain agreement (SLA) compliance impact.

2.3.1.2 Data and objects containing data shall be assigned a classification by the data owner based on data type, value, sensitivity, and criticality.

2.3 Data Security and Lifecycle Management

2.3.2 Encryption and Cryptography

Version 1.0

Adoption Lifecycle

Understanding | Assessing | [✓ Implementing] | Monitoring | Collaborating

Service Model Applicability

[✓ IaaS] | [✓ PaaS] | SaaS

Policy Objective

To protect data at rest, in transit and during processing within the cloud environment.

Policy Statements

2.3.2.1 Policies and procedures shall be established and implemented, for the use of encryption protocols for the protection of sensitive data at rest (may include but not limited to: file servers, databases, and end-user devices), data in use (memory), and data in transmission (may include but not limited to: system interfaces, over public networks, and electronic messaging) as per applicable legal, statutory, and regulatory compliance obligations.

2.3.2.2 Keys shall be maintained by the cloud consumer or trusted key management provider. Key management and key usage shall be separate duties.

2.4 Data Location and Sovereignty

2.4.1 Data Location Awareness

Version	1.0

Adoption Lifecycle

Understanding | Assessing | **Implementing** | Monitoring | Collaborating

Service Model Applicability

IaaS | PaaS | SaaS

Policy Objective

To ensure the cloud consumer is aware of the location at which data is stored, processed, and managed from.

Policy Statements

2.4.1.1 Location of data shall be known at all stages and handled as per applicable laws, regulations, standards, and frameworks published within the UAE pertaining to data location and sovereignty.

2.4.1.2 During the selection of cloud service providers, cloud consumers shall ensure that they operate within acceptable legal jurisdiction(s).

2.4.1.3 Cloud consumers shall verify whether any agreements with the cloud service provider relating to the use of their data by the service provider are acceptable to them and not contrary to relevant local legislation.

2.4.1.4 Cloud consumers shall determine, depending on classification of the data to be hosted, the requirements for data localization and relevant security requirements to be implemented.

2.5 Interoperability and Portability

2.5.1 Interoperability

Version 1.0

Adoption Lifecycle

[✓ Understanding] Assessing [✓ Implementing] Monitoring Collaborating

Service Model Applicability

IaaS PaaS SaaS

Policy Objective

To ensure the cloud consumer can select various diverse CSPs that can cooperate and interoperate with each other.

Policy Statements

2.5.1.1 Cloud consumers planning to or using multiple cloud services shall perform a comprehensive assessment on their needs and requirements for interoperability of their services and respective CSPs.

2.5.1.2 Cloud consumers shall ensure that industry standards and available APIs are consistently utilized and applied across their data and cloud services to support interoperability.

2.5.1.3 Cloud consumers shall document appropriate policies and procedures defining the requirements for interoperability and clearly communicate it to all parties.

2.5 Interoperability and Portability

2.5.2 Portability

Version 1.0

Adoption Lifecycle

Understanding	Assessing	**Implementing**	Monitoring	Collaborating

Service Model Applicability

IaaS	PaaS	SaaS

Policy Objective

To protect the cloud consumers from vendor lock-in and ensure the ease of mobility between different CSPs.

Policy Statements

2.5.2.1 Contractual agreements shall include provisions specifying the cloud consumer’s access to all structured and unstructured data in an industry-standard format upon contract termination.

2.5.2.2 Cloud consumers, when procuring cloud services, shall ensure the CSP has demonstrated its commitment to portability (may include but not limited to, upon contract termination, the length of time for which data will be stored, the controls implemented by CSP for protection of such data and data deletion process)

2.5.2.3 Cloud consumers shall document appropriate policies and procedures defining the requirements for portability and clearly communicate it to all parties.

2.6 Cloud Architecture, Infrastructure & Virtualization

2.6.1 Change Control and Configuration

Version	1.0

Adoption Lifecycle

Understanding	Assessing	**Implementing**	Monitoring	Collaborating

Service Model Applicability

IaaS	PaaS	SaaS

Policy Objective

To ensure that changes to the cloud infrastructure are identified and managed, and any unauthorized changes are detected.

Policy Statements

2.6.1.1 Cloud consumers, when procuring cloud services, shall ensure the CSP has adequate change management controls in place such that the status, location and configuration of service components are tracked throughout their lifetime within the service.

2.6.1.2 Cloud consumers shall be made available the results of a change or move of an image and the subsequent validation of the image's integrity through electronic methods.

2.6 Cloud Architecture, Infrastructure & Virtualization

2.6.2 Data Centre Security

Version	1.0

Adoption Lifecycle

Understanding	Assessing	Implementing	**Monitoring**	Collaborating

Service Model Applicability

IaaS	PaaS	SaaS

Policy Objective

To ensure physical protection against unauthorized access, tampering, theft or reconfiguration of systems.

Policy Statements

2.6.2.1 Cloud consumers shall validate the effectiveness of the physical security controls at the CSP data centres before hosting data or procuring any services (the level of security controls applied should take into consideration the classification of data to be hosted).

2.6 Cloud Architecture, Infrastructure & Virtualization

2.6.3 Asset and Endpoint Management

Version	1.0

Adoption Lifecycle

Understanding	Assessing	**Implementing**	Monitoring	Collaborating

Service Model Applicability

IaaS	**PaaS**	SaaS

Policy Objective

To strengthen the cloud consumer’s cyber security posture by understanding its cloud assets and endpoints and the risks associated with them.

Policy Statements

2.6.3.1 Policies shall be developed and implemented to ensure all cloud assets and endpoints are catalogued, tracked, and managed securely based on organizational business risk.

2.6 Cloud Architecture, Infrastructure & Virtualization

2.6.4 Application Security

Version	1.0

Adoption Lifecycle

Understanding	Assessing	**Implementing**	Monitoring	Collaborating

Service Model Applicability

IaaS	**PaaS**	**SaaS**

Policy Objective

To protect the confidentiality, integrity, and availability of the data within the CSP’s applications, as well as the CSP’s environment.

Policy Statements

2.6.4.1 Policies and procedures shall be developed and implemented to establish security as a key focus across the application/software development lifecycle such as SecDevOps/DevSecOps.

2.6.4.2 Cloud consumers, when procuring cloud services, shall ensure CSP has adequate change application security controls in place.

2.6 Cloud Architecture, Infrastructure & Virtualization

2.6.5 Device Hardening

Version 1.0

Adoption Lifecycle

Understanding | Assessing | **Implementing** | Monitoring | Collaborating

Service Model Applicability

IaaS | PaaS | SaaS

Policy Objective

To only enable necessary ports, protocols and services that are required to meet business needs.

Policy Statements

2.6.5.1 Cloud consumers shall ensure adequate hardening guidelines are developed and implemented for all cloud systems (physical and virtual), including but not limited to operating systems, virtual machines, hypervisors, Internet of Things sensors and network and security devices.

2.7 Identity and Access Management

2.7.1 Cloud Identities

Version 1.0

Adoption Lifecycle

Understanding | Assessing | Implementing | Monitoring | Collaborating

Service Model Applicability

IaaS | PaaS | SaaS

Policy Objective

To manage user identities in the cloud securely.

Policy Statements

2.7.1.1 User authentication environment and ability to manage identities shall be restricted to authorized consumer staff.

2.7.1.2 Cloud consumers shall implement centralized processes for privileged account (root accounts) creation and strictly control & limit the activities that can be performed through the account.

2.7.1.3 Multi-factor authentication should be considered for all accounts within the cloud.

2.7 Identity and Access Management

2.7.2 Cloud Authentication & Authorization

Version 1.0

Adoption Lifecycle

Understanding	Assessing	Implementing	Monitoring	Collaborating

Service Model Applicability

IaaS	PaaS	SaaS

Policy Objective

To prevent unauthorized access and alteration of organizational resources, applications, and data while consuming cloud services.

Policy Statements

2.7.2.1 Cloud consumers shall establish processes and procedures for authenticating access to systems, applications, and data assets by integrating authentication on the cloud with an internal directory service.

2.7.2.2 Role Based Access Controls (RBAC) shall be implemented within management interfaces.

2.7.2.3 Cloud consumers shall implement processes and procedures to verify authorized access to data and system functions.

2.7.2.4 Multi-factor authentication shall be implemented for accounts with elevated privileges within the cloud.

2.7 Identity and Access Management

2.7.3 Access Governance

Version	1.0

Adoption Lifecycle

Understanding	Assessing	Implementing	Monitoring	Collaborating

Service Model Applicability

IaaS	PaaS	SaaS

Policy Objective

To de-risk the processes used to request, approve, grant, manage and audit access.

Policy Statements

2.7.3.1 Cloud consumers shall define and implement formal requests and approvals as part of the user access provisioning process.

2.7.3.2 Cloud consumers shall ensure timely de-provisioning or modification of access of movers/leavers or system identity changes.

2.7.3.3 Cloud consumers shall periodically review and recertify access rights and entitlements.

2.8 Security Incident Management, E-Discovery, and Cloud Forensics

2.8.1 Incident Management Process

Version 1.0

Adoption Lifecycle

Understanding | Assessing | **Implementing** | Monitoring | Collaborating

Service Model Applicability

IaaS | PaaS | SaaS

Policy Objective

To minimize the impact of environmental, security and reliability issues with the cloud service.

Policy Statements

2.8.1.1 Cloud consumers shall establish incident management processes for the cloud services, which shall be regularly tested and enacted in response to security incidents.

2.8.1.2 Incident management shall include pre-defined processes for responding to common types of incidents and attacks on the cloud environment.

2.8 Security Incident Management, E-Discovery, and Cloud Forensics

2.8.2 Incident Reporting

Version 1.0

Adoption Lifecycle

Understanding | Assessing | **Implementing** | Monitoring | Collaborating

Service Model Applicability

IaaS | PaaS | SaaS

Policy Objective

To ensure security incidents are reported in acceptable timescales and formats.

Policy Statements

2.8.2.1 A defined process and contact route shall be implemented for reporting security incidents by cloud consumers.

2.8.2.2 Cloud consumers shall be responsible for notifying relevant external entities within acceptable timeframe.

2.8.2.3 Points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities shall be maintained and regularly updated.

2.8 Security Incident Management, E-Discovery, and Cloud Forensics

2.8.3 Incident Response

Version 1.0

Adoption Lifecycle

Understanding | Assessing | **Implementing** | Monitoring | Collaborating

Service Model Applicability

IaaS | PaaS | SaaS

Policy Objective

To effectively contain and minimize the impacts of security incidents.

Policy Statements

2.8.3.1 Cloud consumers shall set up clear procedures to activate security incident management, establish the incident response plan in line with the Cyber Security Incident Response Plan issued by CSC and define a relevant protocol to appraise the management on the development of the incident, containment, and communication to appropriate entities.

2.8.3.2 Cloud consumers shall conduct regular incident simulations to stress-test security incident response plans.

2.8 Security Incident Management, E-Discovery, and Cloud Forensics

2.8.4 E-discovery and Cloud Forensics

Version 1.0

Adoption Lifecycle

Understanding	Assessing	Implementing	Monitoring	Collaborating

Service Model Applicability

IaaS	PaaS	SaaS

Policy Objective

To support incident investigation and fulfil e-Discovery requests for Legal proceedings.

Policy Statements

2.8.4.1 The cloud consumers shall identify suitable personnel to oversee the setup and ongoing supervision of e-Discovery/Cloud Forensic capabilities with clear and measurable metrics.

2.8.4.2 The cloud consumers shall establish e-Forensic protocols coherent with UAE law enforcement procedures in digital evidence handling and ensure CSPs comply with such protocols.

2.9 Cloud Resilience

2.9.1 Secure Backup

Version 1.0

Adoption Lifecycle

Understanding | Assessing | Implementing | Monitoring | Collaborating

Service Model Applicability

IaaS | **PaaS** | **SaaS**

Policy Objective

To ensure high availability of information to minimize the impact of regulatory non-compliance or data loss incidents.

Policy Statements

2.9.1.1 Cloud consumers shall establish the requirements for regular backups of information within the cloud environments and the backup restoration testing schedule.

2.9.1.2 Cloud consumers shall establish minimum encryption requirements for backups while ensuring that restoration efforts are successful for such data.

2.9 Cloud Resilience

2.9.2 Business Continuity and Disaster Recovery

Version 1.0

Adoption Lifecycle

Understanding	**Assessing**	Implementing	Monitoring	Collaborating

Service Model Applicability

IaaS	PaaS	SaaS

Policy Objective

To ensure high availability of resources and information as part of continuous efforts and minimize the impact of outages and incidents.

Policy Statements

2.9.2.1 Requirements for operational continuity, including uptime, redundancy, high availability and recovery priorities, shall be communicated as part of cloud service contracts, and tested for cloud services.

2.9.2.2 Business continuity and disaster recovery plans shall be formalized and communicated to all relevant parties (including but not limited to consumer and third party)

2.9.2.3 Recovery plans shall at a minimum define Maximum Tolerable Period of Disruption (MTPD), Recovery Time Objective (RTO), Recovery Point Objective (RPO) and roles and responsibilities of all relevant parties.

SECTION 3

CLOUD SERVICE PROVIDERS

The following section outlines the policy domains and sub-domains applicable to cloud service providers in the UAE. The policy sub-domains further elaborate on the objectives and policy statements.

3.1 Cloud Governance

3.1.1 Governance Framework

Version 1.0

Adoption Lifecycle

Understanding	Assessing	Implementing	Monitoring	Collaborating

Service Model Applicability

IaaS	PaaS	SaaS

Policy Objective

To coordinate and direct an overall approach to CSP’s managing the service and the security of information within it.

Policy Statements

3.1.1.1 A security governance framework shall be established to ensure procedure, personnel, and physical and technical controls remain effective through the lifetime of the service, in response to changes in the service, changes in threat and technology development.

3.1 Cloud Governance

3.1.2 Risk Management

Version	1.0

Adoption Lifecycle

Understanding	Assessing	Implementing	Monitoring	Collaborating

Service Model Applicability

IaaS	PaaS	SaaS

Policy Objective

To ensure security and privacy are part of CSP's operational risk process and reporting mechanisms.

Policy Statements

3.1.2.1 Security and privacy risks impacting consumer services provided by CSP's shall be continuously monitored and reported on in alignment with a formally documented risk management process.

3.1 Cloud Governance

3.1.3 Personnel Security

Version 1.0

Adoption Lifecycle

Understanding	Assessing	Implementing	Monitoring	Collaborating

Service Model Applicability

IaaS	PaaS	SaaS

Policy Objective

To reduce the likelihood of accidental or malicious compromise of consumer data by CSP personnel, ensure thorough screening and adequate training is undertaken.

Policy Statements

3.1.3.1 Personnel with access to consumer data and systems shall be subject to security screening and background verification checks.

3.1.3.2 Continual security education and training shall be provided to personnel based on their role within the CSP and in compliance with consumers requirements (as applicable).

3.1.3.3 A formal exit process for CSP personnel shall be followed as per contractual obligations with cloud consumers.

3.1 Cloud Governance

3.1.4 Third Party and Supply Chain Security

Version	1.0

Adoption Lifecycle

Understanding	Assessing	Implementing	Monitoring	Collaborating

Service Model Applicability

IaaS	PaaS	SaaS

Policy Objective

To reduce the likelihood of supply chain compromise and ensure that the supply chain supports all cloud policy requirements that the CSP must implement.

Policy Statements

3.1.4.1 CSP shall manage security risks from third party suppliers and delivery partners.

3.1.4.2 CSP shall mandate cloud security requirements on suppliers in line with this policy and consumer requirements (as applicable).

3.1.4.3 CSP shall manage the conformance of supplier’s security requirements, conduct regular audits and report to consumers on a need-to-know basis.

3.1 Cloud Governance

3.1.5 Assurance and Independent Testing

Version	1.0

Adoption Lifecycle

Understanding | Assessing | Implementing | **Monitoring** | **Collaborating**

Service Model Applicability

IaaS | PaaS | SaaS

Policy Objective

To ensure that all cloud security requirements and controls are implemented, and objectives are met in practice.

Policy Statements

3.1.5.1 CSP shall hold certificates of compliance with recognized industry standards for Cloud Security for the scope of cloud services and products being provided to cloud consumers.

3.1.5.2 CSP shall provide flexibility to cloud consumers for conducting independent assurance testing of services and components.

3.2 Contractual Agreements

3.2.1 Due Diligence

Version	1.0

Adoption Lifecycle

Understanding	Assessing	Implementing	Monitoring	Collaborating

Service Model Applicability

IaaS	PaaS	SaaS

Policy Objective

To protect the confidentiality of the cloud consumer’s data in the cloud environment.

Policy Statements

3.2.1.1 CSPs shall be subjected to legal review and due diligence to ensure that terms and conditions are not detrimental to the cloud consumers.

3.2.1.2 As part of the contractual agreements, a Non-Disclosure Agreement shall be drafted and formalized, and signed by both parties before cloud computing services are procured.

3.2 Contractual Agreements

3.2.2 Service Level Agreements

Version 1.0

Adoption Lifecycle

Understanding	Assessing	Implementing	Monitoring	Collaborating

Service Model Applicability

IaaS	PaaS	SaaS

Policy Objective

To pre-emptively protect the rights of the cloud consumer and CSP.

Policy Statements

3.2.2.1 As part of the contractual agreements, a Service Level Agreement detailing availability, data ownership, division of responsibility, etc. shall be drafted, formalized, and signed by both parties before cloud computing services are procured.

3.2.2.2 Risks associated with third party suppliers and delivery partners shall be addressed in SLAs between the CSP and the third-party supplier.

3.3 Data Security and Lifecycle Management

3.3.1 Data Governance

Version	1.0

Adoption Lifecycle

Understanding	**Assessing**	**Implementing**	Monitoring	Collaborating

Service Model Applicability

IaaS	PaaS	SaaS

Policy Objective

To ensure the security of data in cloud environments, such that access is strictly limited to authorized personnel.

Policy Statements

3.3.1.1 Policies and procedures shall be developed for the classification, protection, and handling of data throughout its lifecycle, in line with all applicable laws in the UAE and regulations, standards, and risk levels.

3.3 Data Security and Lifecycle Management

3.3.2 Encryption and Cryptography

Version 1.0

Adoption Lifecycle

Understanding | Assessing | **Implementing** | Monitoring | Collaborating

Service Model Applicability

IaaS | PaaS | SaaS

Policy Objective

To protect data through industry-standard encryption and key management best practices.

Policy Statements

3.3.2.1 Policies for cryptography, encryption, and key management, shall be developed and implemented to ensure that data at rest and in transit is securely encrypted.

3.4 Data Location and Sovereignty

3.4.1 Data Location Transparency

Version	1.0

Adoption Lifecycle

Understanding	Assessing	Implementing	Monitoring	Collaborating

Service Model Applicability

IaaS	PaaS	SaaS

Policy Objective

To ensure the CSP is transparent with the cloud consumers regarding the location of data processing, transit and storage.

Policy Statements

3.4.1.1 Location of the processing, storage, transfer, and backup of data shall be clearly communicated to the consumer and compliance with applicable contractual obligations, laws, and regulations in the UAE regarding data location and sovereignty shall be maintained at all stages.

3.5 Interoperability and Portability

3.5.1 Interoperability

Version	1.0

Adoption Lifecycle

Understanding	Assessing	Implementing	Monitoring	Collaborating

Service Model Applicability

IaaS	PaaS	SaaS

Policy Objective

To ensure CSPs maximize interoperability to the degree that it is possible, allowing the cloud consumers the freedom to simultaneously procure different cloud services from different CSPs.

Policy Statements

3.5.1.1 CSPs shall ensure the freedom of its cloud consumers to select their preferred provider for related services, allowing interoperability across cloud consumers and CSP environments and across different CSPs.

3.5.1.2 CSPs shall use open and published Application Programming Interfaces (API's) to ensure support for interoperability between components and to facilitate application migration.

3.5.1.3 CSP shall use an industry-recognized virtualization platform and standard virtualization formats to help ensure interoperability.

3.5.1.4 CSPs shall follow any policies and procedures defined by consumers in line with consumer's interoperability requirements.

3.5 Interoperability and Portability

3.5.2 Portability

Version 1.0

Adoption Lifecycle

Understanding	Assessing	Implementing	Monitoring	Collaborating

Service Model Applicability

IaaS	PaaS	SaaS

Policy Objective

To allow the cloud consumers the ease of mobility between CSPs.

Policy Statements

3.5.2.1 CSPs shall enable portability using defined policies, standards or documented formats to ensure that cloud consumers are able to get their data into or out of cloud services in a reasonably easy and cost-effective manner.

3.5.2.2 CSPs shall use secure, standardized network protocols to import and export data and manage the service.

3.5.2.3 CSPs shall follow any policies and procedures defined by consumers in line with consumer’s portability requirements.

3.6 Cloud Architecture, Infrastructure & Virtualization

3.6.1 Change Control and Configuration

Version 1.0

Adoption Lifecycle

Understanding | Assessing | **Implementing** | Monitoring | Collaborating

Service Model Applicability

IaaS | PaaS | SaaS

Policy Objective

To ensure that changes to CSP infrastructure does not result in significant downtime and disruption to cloud services.

Policy Statements

3.6.1.1 Changes to the CSP's cloud infrastructure shall be preemptively planned and coordinated efficiently, ensuring compliance with applicable uptime requirements.

3.6.1.2 CSPs shall always ensure the integrity of all virtual machine images. Any changes made to virtual machine images must be logged, and an alert raised regardless of their running state.

3.6 Cloud Architecture, Infrastructure & Virtualization

3.6.2 Data Centre Security

Version	1.0

Adoption Lifecycle

Understanding	Assessing	**Implementing**	Monitoring	Collaborating

Service Model Applicability

IaaS	PaaS	SaaS

Policy Objective

To protect the CSP's assets and facilities from physical security risks and environmental factors.

Policy Statements

3.6.2.1 The physical security of the CSP's facilities and assets shall be maintained by restricting access to authorized personnel, monitoring visitor access and data center surveillance systems, and preemptively protecting its facilities from environmental factors.

3.6 Cloud Architecture, Infrastructure & Virtualization

3.6.3 Asset and Endpoint Management

Version 1.0

Adoption Lifecycle

Understanding	Assessing	**Implementing**	Monitoring	Collaborating

Service Model Applicability

IaaS	**PaaS**	SaaS

Policy Objective

To strengthen the CSP's cyber security posture by understanding its assets, endpoints, and associated risks.

Policy Statements

3.6.3.1 Policies and procedures shall be developed and implemented to ensure all assets and endpoints are catalogued, tracked, and managed securely based on organizational business risk.

3.6 Cloud Architecture, Infrastructure & Virtualization

3.6.4 Application Security

Version	1.0

Adoption Lifecycle

Understanding	Assessing	Implementing	Monitoring	Collaborating
		●		

Service Model Applicability

IaaS	PaaS	SaaS
	●	●

Policy Objective

To protect the confidentiality, integrity, and availability of the data within cloud applications and the CSP’s development environment.

Policy Statements

3.6.4.1 CSPs shall ensure that applications and programming interfaces are designed, developed, deployed, and tested in accordance with leading industry standards and adhere to consumer’s security requirements as well as applicable legal, statutory, or regulatory compliance obligations in the UAE.

3.6 Cloud Architecture, Infrastructure & Virtualization

3.6.5 Device Hardening

Version 1.0

Adoption Lifecycle

Understanding | Assessing | **Implementing** | Monitoring | Collaborating

Service Model Applicability

IaaS | PaaS | SaaS

Policy Objective

To only enable necessary ports, protocols and services that are required to meet business needs.

Policy Statements

3.6.5.1 The CSP shall ensure adequate hardening standards and/or procedures are developed and implemented for cloud systems (physical and virtual), as applicable, including but not limited to: operating systems, virtual machines, hypervisors, and network and security devices.

3.7 Identity and Access Management

3.7.1 Cloud Identity and Access Management

Version 1.0

Adoption Lifecycle

Understanding | Assessing | **Implementing** | Monitoring | Collaborating

Service Model Applicability

IaaS | PaaS | SaaS

Policy Objective

To meet cloud consumer expectations and any compliance requirements to prevent unauthorized access to CSP hosted infrastructure, applications and data.

Policy Statements

3.7.1.1 Authentication processes, access control, accountability, and logging (format, retention, and access) shall meet the cloud consumer specification aligned with regulatory and legal requirements in the UAE.

3.8 Security Incident Management, E-Discovery, and Cloud Forensics

3.8.1 Incident Management Process

Version 1.0

Adoption Lifecycle

Understanding	Assessing	Implementing	Monitoring	Collaborating

Service Model Applicability

IaaS	PaaS	SaaS

Policy Objective

To minimize impact of environmental, security and reliability issues with CSP cloud services.

Policy Statements

3.8.1.1 CSP shall follow defined incident management processes for the cloud services, regularly tested and enacted in response to security incidents.

3.8 Security Incident Management, E-Discovery, and Cloud Forensics

3.8.2 Incident Reporting

Version 1.0

Adoption Lifecycle

Understanding | Assessing | Implementing | Monitoring | **Collaborating**

Service Model Applicability

IaaS | PaaS | SaaS

Policy Objective

To ensure CSP security incidents are reported in acceptable timescales and format.

Policy Statements

3.8.2.1 Security incidents shall be notified to impacted cloud consumers and UAE authorities within the applicable response framework and timeframes.

3.8.2.2 Regular threat and vulnerability scanning shall be carried out to prioritize remediation and response capabilities to create quality insights.

3.8.2.3 CSPs shall communicate emerging threats to the broader cloud community, as applicable.

3.8 Security Incident Management, E-Discovery, and Cloud Forensics

3.8.3 Incident Response

Version	1.0

Adoption Lifecycle

Understanding	Assessing	Implementing	Monitoring	Collaborating

Service Model Applicability

IaaS	PaaS	SaaS

Policy Objective

To effectively contain and minimize the impacts of security incidents.

Policy Statements

3.8.3.1 Incident response capabilities to effectively contain and minimize security incidents impacts shall be established through formal incident response plans in line with the Cyber security Incident Response Framework and Plan issued by CSC

3.8 Security Incident Management, E-Discovery, and Cloud Forensics

3.8.4 E-discovery and Cloud Forensics

Version 1.0

Adoption Lifecycle

Understanding	Assessing	**Implementing**	Monitoring	Collaborating

Service Model Applicability

IaaS	PaaS	SaaS

Policy Objective

To support CSP incident investigation and fulfil e-Discovery requests for Legal proceedings.

Policy Statements

3.8.4.1 Appropriate systems and processes shall be deployed to enable logging and monitoring controls to establish and retain audit trails and allow necessary reviews and retention.

3.8.4.2 Forensic capabilities should be provided in a timely manner to legal or regulatory requests, including response to e-discovery information requests.

3.9 Cloud Resilience

3.9.1 Secure Backup, Business Continuity and Disaster Recovery

Version	1.0

Adoption Lifecycle

Understanding	Assessing	Implementing	Monitoring	Collaborating

Service Model Applicability

IaaS	PaaS	SaaS

Policy Objective

To meet cloud consumer expectations for availability and continuity of CSP cloud services.

Policy Statements

3.9.1.1 CSP shall ensure provisions are made to meet consumers' uptime, backup, and business continuity objectives.

3.9.1.2 CSP shall establish a detailed disaster recovery plan which must be tested at regular intervals.

SECTION 4

IMPLEMENTATION

IMPLEMENTATION

This policy should be read in conduction with the cloud security controls framework attached in the appendix 6.6 which provides control statements supporting the policy requirements.

The Cyber Security Council will work with sector regulators and Emirate lead entities to ensure compliance to the requirements of this policy.

Cloud service consumers and CSP’s are expected to conduct compliance self-assessments against these policy requirements and report back to relevant authorities annually and/or as required.

To bring about the change required to successfully promote cloud security, education, awareness, and communications are needed. The CSC will engage participants to promote cloud security as a national and organizational priority. As processes, procedures, and solutions are built to support the collection, analysis, dissemination, and use of information across organizational boundaries, the CSC will educate and raise awareness to provide a foundational understanding and trust among participants. Furthermore, the CSC will work with participating stakeholders to acknowledge stakeholder organizations that contribute information that leads to innovative cyber solutions and connections among disparate sources of information that enhances the resilience of the UAE’s cyberspace.

SECTION 5

PERFORMANCE MONITORING

PERFORMANCE MONITORING

The National Cloud Security Policy outlines measures for monitoring and evaluating progress towards the following objectives:

- Promote transparency and effective management of the Cloud Services
- Provide guidance for improvement and taking necessary intervention steps when appropriate.
- Measure the successful implementation of Cloud Security requirements by CSPs and Consumers

SECTION 6

APPENDICES

6.1 Reference Documents

UAE Policies and Standards

The following UAE policies and standards were referenced when defining these policy statements.

Authority/Body	Document
TDRA	National Policy for the Regulation of Cloud Services (Draft)
CSC	UAE IA Regulation
TDRA	Cloud First Policy (Draft)
DESC	CSP Security Standard
DESC	Information Security Regulation v2
UAE Smart Government	UAE Smart Data Framework

6.1 Reference Documents

International Standards

The following table outlines the international sources referenced in this document.

Authority/Body	Document
NIST	SP 800-145 - The NIST Definition of Cloud Computing
NIST	SP 500-322 - Evaluation of Cloud Computing Services Based on NIST SP 800-145
ISO/IEC	17788 - Cloud Computing Overview and Vocabulary
ISO/IEC	27001 - Information Security Management
ISO/IEC	27002 - Information Security, Cybersecurity, And Privacy Protection — Information Security Controls
ISO/IEC	27017 - Code of practice for information security controls based on ISO/IEC 27002 for cloud services
ISO/IEC	27018 - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
ISO/IEC	19086 – Cloud Computing Service Level Agreements (SLA) Framework
ISO/IEC	19941 – Cloud Computing Interoperability and portability
CSA	CSA CCM - Cloud Controls Matrix

6.2 Abbreviations

Usage	Description
API	Application Programming Interface
CSP	Cloud Service Provider: An entity (Private or Public) that provides cloud-based platforms, infrastructure, application, security or storage services to another entity/organization. Usually for a fee.
IaaS	Infrastructure as a Service: A service model where backend IT infrastructure for running applications is cloud-hosted on a subscription basis.
PaaS	Platform as a Service: A service model where a cloud-hosted platform is provided for developing, running, and managing applications.
SaaS	Software as a Service: A service model where cloud-hosted software is licensed and delivered on a subscription basis.
SLA	Service Level Agreement (): a contractual agreement between a service provider and a consumer (A state Agency), where the consumer requirements are specified, and the service provider states the level of service responsibilities and guarantees regarding availability, performance and support levels.
VM	Virtual Machine: file type (called an Image) that appears to the user as an actual machine when executed. The VM can be started or stopped as needed, and changes made to the VM while it is running can be stored on disk to make them persistent (definition source: NIST).

6.3 Definitions

Usage	Description
Classification labels	Open Data: • Data that is publicly shared and published online with minimal restrictions Non-Open Data: • Confidential • Sensitive • Secret
Federation	The act of combining data or identities across multiple platforms, federation can be managed by a cloud service provider or by a cloud broker.
Governance	The controls and practices, and processes that make sure policies are enforced.
Hosted Application	An internet based or web-based application that runs remotely.
Internal Cloud	A type of private cloud whose services are provided by an IT department to those in its organization.
Vendor Lock-in	Dependency on a particular vendor (cloud service provider) and the difficulty moving from one cloud service provider to another.
Virtualization	The simulation of the software and or hardware upon which other software can run.

6.4 Roles and Responsibilities

The below table defines the key stakeholders and their respective roles and responsibilities with regards to this policy.

Stakeholder	Roles and Responsibilities
UAE Cyber Security Council (CSC)	As the custodian of this document, CSC shall: • Issue the National Cloud Security Policy and review the document periodically to ensure its relevance. • Coordinate with relevant stakeholders to disseminate the policy to critical sectors and entities. • Oversee the implementation of the provisions of the regulation to ensure compliance with the policy.
Government Entities and National Critical Infrastructure Sectors	• Comply with the requirements outlined in the National Cloud Security Policy. • Implement the Policy’s provisions on applicable services. • Exercise due diligence and conduct the appropriate risk assessments outlined in this policy.
Cloud Service Providers	• Cloud Service Providers are required to comply with and meet the security requirements outlined in the policy.
Non-Government/ CII Cloud Consumers	• To improve their security posture, consumers may choose to adhere to the policy's security requirements.

6.5 Compendium

Cloud Computing Overview

As defined by the National Institute of Standards and Technology, Cloud Computing is a model that leverages a shared pool of configurable computing resources, such as networks, servers, storage, applications, and services, to achieve ubiquitous, convenient, on-demand network access that can be rapidly provisioned and released with minimal management effort or service provider interaction. The cloud computing model comprises five essential characteristics, three service models, and four deployment models.

Cloud Characteristics

- **On-demand self-service:** A consumer can unilaterally provision computing capabilities as needed automatically without requiring human interaction.
- **Broad network access:** Capabilities are available over the network and accessed through standard mechanisms such as mobile phones, tablets, laptops, and workstations.
- **Resource pooling:** The cloud service provider’s computing resources are pooled to serve multiple consumers, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. Typically, the customer has little to no information regarding the location of data storage.
- **Rapid elasticity:** According to demand, capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward, to a seemingly unlimited degree.
- **Measured service:** Monitoring, controlling, and reporting resource usage to provide transparency for providers and consumers. Cloud systems automatically control and optimize resource use by leveraging a metering capability.

6.5 Compendium

Cloud Service Models

- **Software as a Service (SaaS):** The consumer is provided with the capability to use the provider’s applications running on a cloud infrastructure. The applications are remotely accessible from various client devices, such as a web or a program interface. The consumer is limited to application use and cannot manage or control the underlying cloud infrastructure employed.
- **Platform as a Service (PaaS):** The consumer is provided with the capability to deploy consumer-created or acquired applications onto the cloud infrastructure, so long as they are developed using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure.
- **Infrastructure as a Service (IaaS):** The consumer is provided with the capability to provision fundamental computing resources such as processing, storage, and networks, to deploy and run arbitrary software, which can include operating systems and applications.

6.5 Compendium

Cloud Deployment Models

- **Private cloud:** The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.
- **Community cloud:** The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations with shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.
- **Public cloud:** The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, government organization, or some combination of them. It exists on the premises of the cloud provider.
- **Hybrid cloud:** The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability.

6.5 Compendium

Cloud Innovation

With most entities migrating to cloud computing and adopting at least one of the three service models, the cloud computing sector has seen significant growth and is expected to grow further. Naturally, the rise in adoption also drives the technological growth around cloud computing; Cloud Edge, Software Defined Networks, and the shift to Omni cloud are major emerging trends in cloud computing. However, novel technologies do not come without novel security threats, and these technologies must be wholly understood.

- **Cloud Edge** – Building a distributed network of “micro” data centres to keep computing, storage, and network requirements at the “edge” of the network, reducing latency.
- **Software Defined Network (SDN)** – Novel approach to networking that allows on-the-go dynamic configuration of networks through programming.
- **Multicloud/Omni cloud** – Eliminating barriers between various cloud infrastructures that lead to vendor lock-in and enabling collaboration
  across all platforms.