Draft Revised Cloud Policy and Procurement Guidelines for Interim Use

Draft

Version 0.2

Contributors

Sanjaya Karunasena
Samisa Abeysinghe
Dr Hans Wijayasuriya
Harsha Purasinghe

Draft

---

1. Objectives

The revised cloud policy aims to align national digital economy ambitions with global best practices while safeguarding national interests. The objectives are:

1. **Ensure Data Sovereignty and Compliance with Local Laws**
   Mandate that data generated by or on behalf of the government is managed in compliance with national data protection and security regulations.
2. **Promote Secure and Resilient National Digital Infrastructure**
   Foster cloud infrastructure that is secure, resilient, and capable of supporting the continuity of government operations and critical public services.
3. **Enable Participation of Hyperscalers While Safeguarding National Interests**
   Allow qualified global cloud providers to operate within a regulatory framework that ensures accountability, transparency, and adherence to sovereign controls while encouraging interoperability and future transition paths to local sovereign cloud infrastructure.
4. **Create an Investment-Friendly Ecosystem for Cloud and Digital Services**
   Attract local and international investments by providing clear regulatory guidance and predictable procurement practices.
5. **Support Innovation and Public Sector Modernization**
   Leverage cloud capabilities to accelerate digital transformation, enhance public service delivery, and enable agile innovation in government.

---

2. Data Classification Policy

All government and public sector data shall be classified into the following categories, aligned with the Sovereign Cloud Strategy:

- **Public**
  Data intended for unrestricted public access with minimal security requirements (e.g., open datasets, public reports).
- **Internal**
  Government operational data not meant for public access but not highly sensitive (e.g., internal communications, preliminary drafts).
- **Confidential**
  Data whose unauthorized disclosure could impact individual privacy, institutional confidentiality, or public trust (e.g., citizen service records, internal audits).
- **Restricted**
  Sensitive data that requires rigorous access controls due to potential implications for government operations or national interests (e.g., health records, government financial data).

Draft

- **Top Secret / National Security**
  Data that, if disclosed, would pose a grave threat to national security, public safety, or critical infrastructure. Hosting must occur in environments providing the highest level of sovereign control.

---

3. Data and Service Classification Framework for Cloud Deployments

Cloud deployments shall follow an integrated classification framework based on both data sensitivity and service criticality. Deployment recommendations are as follows:

Data Classification	Service Classification	Deployment Model
Public	Non-Critical	Sensitivity Level 1: Global Hosting with Local Oversight, Uptime Tier 1 or higher
Internal	Core Government	Sensitivity Level 2: Federated or Hybrid Cloud, Uptime Tier 2 or higher, may require Uptime Tier 3
Confidential	Core Government / Mission-Critical	Sensitivity Level 3: High Sovereignty + Conditional Localisation, Uptime Tier 3 or higher
Restricted	Mission-Critical	Sensitivity Level 3: High Sovereignty + Conditional Localisation or Sensitivity Level 4, Uptime Tier 3 or higher
Top Secret / National Security	Mission-Critical	Sensitivity Level 4: Full Sovereignty + Strict Localisation, Uptime Tier 3 or higher, may require Uptime Tier 4

This framework enables the participation of hyperscalers under defined conditions while allowing for migration to national sovereign cloud infrastructure as it matures.

---

4. Explanation of Sovereignty and Localisation Sensitivity Level

To guide cloud deployment decisions, the following tiers describe levels of sovereignty and localisation:

- **Sensitivity Level 4: Full Sovereignty + Strict Localisation**
  All data and service operations must be hosted and managed entirely within Sri Lanka

Draft

under the exclusive jurisdiction of the Sri Lankan government. Hosting must occur within a certified infrastructure that guarantees no foreign access—whether through physical, legal, or operational controls. Mandatory for Top Secret and highest-risk workloads. While Digital Sovereignty Zones are a preferred model for Sensitivity Level 4, other certified local sovereign environments may also be eligible.

- **Sensitivity Level 3: High Sovereignty + Conditional Localisation**
  Data and services must meet high sovereignty requirements (e.g., encrypted, auditable, accessible only under Sri Lankan legal authority). Hosting may include certified private or foreign cloud providers operating locally or internationally, provided they operate under arrangements that recognize and enforce Sri Lankan jurisdiction—such as through legal constructs comparable to extraterritorial embassies or international agreements—subject to compliance with defined sovereign conditions.
- **Sensitivity Level 2: Federated or Hybrid Cloud**
  Mixed deployment models allowing interoperability between local and international cloud environments. Data flows must be auditable, with control points retained locally. Suitable for moderate-sensitivity workloads.
- **Sensitivity Level 1: Global Hosting with Local Oversight**
  Public or non-critical data may be hosted internationally, provided oversight mechanisms are in place. Contracts must ensure exit strategies, transparency, and compliance with basic national safeguards.

---

5. Procurement Guidelines

- All cloud procurement must align with the data classification and sovereignty tiers.
- Preference shall be given to providers that demonstrate compliance with Sri Lankan laws, support sovereign control mechanisms, and enable integration with local or sovereign cloud infrastructure where applicable.
- Procurement processes must encourage competition, innovation, and value for money.
- Contracts must include clauses for data residency, portability, service continuity, auditability, and exit mechanisms.
- Strategic partnerships (e.g., with hyperscalers) must undergo prior technical and legal review by designated authorities.
- All procurements should provide for future migration to national sovereign cloud infrastructure, including through modular designs and flexible contract terms.
- Systems deployed under Sensitivity Level 3 and Sensitivity Level 2 must be capable of operating in hybrid conditions, supporting interoperability between sovereign, local, and international environments while maintaining compliance with data classification and sovereignty requirements.

End of Draft

Draft

Definition: Digital Sovereignty Zones (DSZs)

Digital Sovereignty Zones are secure, government-certified hosting environments physically located within Sri Lanka that operate entirely under Sri Lankan jurisdiction. They are designed to host the country's most sensitive digital assets, including Top Secret and national security-related data.

Key features include:

- **Exclusive legal and operational control** by Sri Lankan authorities.
- **Physical and logical isolation** from foreign access or influence.
- **Use of certified infrastructure** and compliance with strict data protection and cybersecurity protocols.
- **Eligibility for Sensitivity Level 4 deployments**, and in some cases, Sensitivity Level 3 workloads depending on the required level of control and assurance.

DSZs form a foundational element of Sri Lanka's sovereign cloud framework, enabling the country to maintain digital independence while securely managing critical workloads.

Draft

Annexe A: Data Classification & Cloud Deployment Mapping

Classification	Data Security Controls	Data Sovereignty Requirements	Data Residency Requirements	Deployment Sensitivity Level	Cloud Model
Public	- Basic encryption (TLS in transit, AES-256 at rest)- Integrity checks and routine backups- Standard IAM (RBAC, MFA optional)	- No special restrictions- Governed by standard public‑data policies	- Flexible placement- Any certified region/provider is acceptable, provided basic legal safeguards are met	**Sensitivity Level 1**	Global Hosting with Local Oversight
Internal	- Stronger encryption (in transit & at rest)- RBAC with MFA- Detailed logging & audit trails	- Managed by accredited government or vetted partners only- Sharing limited to "need-to-know" groups	- Must reside in jurisdictions compliant with local laws- Provider must support data-localization options	**Sensitivity Level 2**	Federated or Hybrid Cloud
Confidential	- Advanced encryption (HSM-backed keys)- MFA + least-privilege RBAC- IDS/IPS, vulnerability scans, incident response plan	- High-sovereignty legal/contractual controls- Data access only under Sri Lankan jurisdiction- Auditable under national law	- Geo-fenced to approved data centres- No replication outside designated zones without approval	**Sensitivity Level 3**	High Sovereignty + Conditional Localization
Restricted	- Dedicated compute/network isolation- Air-gapped or virtually isolated environments- Continuous monitoring & third-party audits	- Strict government control- Only certified entities may host or process- Regular legal attestation of sovereign controls	- Must remain in certified local sovereign environments (DSZs) or equivalent- Any foreign hosting requires equivalent legal guarantees (e.g., embassy-style status)	**Sensitivity Level 3 or Sensitivity Level 4**	High Sovereignty + Conditional Localization or Full Sovereignty + Strict Localization
Top Secret / National Security	- State-of-the-art cryptography- Physically air-gapped networks- 24/7	- Exclusive Sri Lankan government ownership & control- No foreign	- Absolute localization in Digital Sovereignty Zones (DSZs)- Certified	**Sensitivity Level 4**	Full Sovereignty + Strict Localization (Digital

Draft

Classification	Data Security Controls	Data Sovereignty Requirements	Data Residency Requirements	Deployment Sensitivity Level	Cloud Model
	SOC monitoring, red-team exercises, and stringent incident-response	legal or operational access permitted-Frequent reassessment of access privileges	infrastructure under direct government jurisdiction		Sovereignty Zones)

Annexe B: Data Classification Checklist

1. Top Secret / National Security:

Check the boxes if the data meets **ANY** of the following criteria:

- [ ] Unauthorized exposure could directly compromise national defence capabilities.
- [ ] Unauthorized exposure could lead to significant loss of life or critical infrastructure failure.
- [ ] The data is specifically designated as "Top Secret" by a relevant authority.
- [ ] Access to the data is strictly limited to individuals with specific national security clearances.
- [ ] The data resides only in fully sovereign, certified environments (DSZs) as a mandatory requirement.

Decision: If **ANY** of the above are checked, classify the data element as **Top Secret / National Security**. **Stop Evaluation.** Otherwise, proceed to Restricted.

2. Restricted:

Check the boxes if the data meets **ANY** of the following criteria:

- [ ] Unauthorized disclosure could lead to significant financial loss or operational disruption.
- [ ] Unauthorized disclosure could severely impact the privacy of a large number of individuals (e.g., extensive health records).
- [ ] The data is subject to strict regulatory requirements demanding rigorous protection (e.g., specific clauses within HIPAA or financial regulations).
- [ ] The data requires strong isolation and dedicated monitoring due to its sensitivity.
- [ ] Compromise of the data could significantly undermine public trust in government services.

Decision: If **ANY** of the above are checked, classify the data element as **Restricted**. **Stop Evaluation.** Otherwise, proceed to Confidential.

3. Confidential:

Check the boxes if the data meets **ANY** of the following criteria:

- [ ] Unauthorized disclosure could lead to reputational damage or loss of public trust.
- [ ] Unauthorized disclosure could violate the privacy of individuals (e.g., individual service records).
- [ ] The data requires strong encryption both in transit and at rest.
- [ ] Access to the data should be controlled based on the principle of least privilege.
- [ ] The data contains sensitive internal information not intended for public release.

Decision: If **ANY** of the above are checked, classify the data element as **Confidential**. **Stop Evaluation.** Otherwise, proceed to Internal.

4. Internal:

Check the boxes if the data meets **ANY** of the following criteria:

- [ ] The data is intended for internal use within the government or approved partners.
- [ ] Unauthorized public disclosure would be undesirable but would likely not cause significant harm.
- [ ] The data includes routine operational information.
- [ ] Access to this data is generally granted to a broad range of internal users.
- [ ] Examples include draft policies, internal memos, and routine system logs.

Decision: If **ANY** of the above are checked, classify the data element as **Internal**. **Stop Evaluation.** Otherwise, the data is likely Public.

5. Public:

If the data does not meet the criteria for any of the above levels, it is classified as **Public**. This category includes data intended for unrestricted release with no confidentiality requirements (e.g., open datasets, public reports, published statistics).

How to Apply This Checklist Scheme:

For each data element, start with the "Top Secret / National Security" checklist. If any of the criteria are met, classify it accordingly and stop. If none are met, move to the "Restricted" checklist, and so on.

Annexe C: Controls Selection Checklist by Classification

Check the boxes for the controls required by your data's classification.

Control Category	Public	Internal	Confidential	Restricted	Top Secret
Encryption (in transit/at rest)	☐ Basic	☐ Standard	☐ Advanced	☐ Dedicated	☐ State-of-the-Art

Control Category	Public	Internal	Confidential	Restricted	Top Secret
IAM & Access Controls	☐ RBAC	☐ RBAC+MFA	☐ Least-Privilege+MFA	☐ Dedicated	☐ Strict, Re-certified
Network Isolation	☐ N/A	☐ Virtual	☐ Isolated	☐ Air-gapped	☐ Air-gapped & Physically
Monitoring & Audit	☐ Basic	☐ Detailed	☐ Continuous	☐ 24/7 SOC	☐ 24/7 SOC + Red-Team
Legal / Contractual Sovereignty Guarantees	☐ Standard	☐ Accredited	☐ High-Sov.	☐ Strict	☐ Exclusive
Data Residency Enforcement	☐ Flexible	☐ Jurisdiction-Bound	☐ Geo-Fenced	☐ Local DSZs	☐ Local DSZs

Annexe D: Service Classification Checklist

1. Mission-Critical Services:

Check the boxes if the service meets **ANY** of the following criteria:

[ ] Failure or disruption would result in **loss of life, national security risk, or critical infrastructure failure**.
[ ] The service is essential for **emergency response, defence operations, or national-level crisis management**.
[ ] The service must be **operational 24/7** with no acceptable downtime (e.g., national emergency systems, border control).
[ ] The service directly supports **vital national interests or constitutional functions** (e.g., elections, national security communications).
[ ] Service failure would cause **irreversible damage to the country's sovereignty or governance**.

Decision:
If **ANY** of the above are checked, classify the service as **Mission-Critical**. Stop evaluation. Otherwise, proceed to **Core Government**.

2. Core Government Services:

Check the boxes if the service meets **ANY** of the following criteria:

[ ] The service is **mandated by law or regulation** for the delivery of essential government functions (e.g., taxation, identity issuance).
[ ] Disruption could cause **major operational paralysis**, legal violations, or **public unrest**.

Draft

[ ] The service supports **inter-ministerial operations or high-priority citizen services** (e.g., pensions, land registration).
[ ] The service handles **regulated personal data or sensitive transactions** involving the public.
[ ] The service has **defined performance and security SLAs** due to its importance in government continuity.

Decision:
If **ANY** of the above are checked, classify the service as **Core Government**. Stop evaluation. Otherwise, proceed to **Non-Critical**.

3. Non-Critical Services:

Check the boxes if the service meets **ANY** of the following criteria:

[ ] The service supports **internal productivity or administrative functions** (e.g., HR systems, time tracking).
[ ] Disruption would be **inconvenient but not severely disruptive** to public service delivery.
[ ] The service is primarily for **supporting analysis, planning, or reporting**, with no direct citizen impact.
[ ] The service can **tolerate planned or short-term downtime** without major consequences.
[ ] The service is used by **a limited set of internal users** with no public interface or regulatory requirement.

Decision:
If **ANY** of the above are checked, classify the service as **Non-Critical**. Otherwise, further assessment may be required to determine if the service is obsolete or outside current classification needs.

How to Apply This Checklist Scheme:

For each **service**, start with the **Mission-Critical** checklist. If any of the criteria are met, classify it accordingly and **stop**. If none are met, continue to the **Core Government** checklist, and so on. The **first applicable category** determines the classification.

Annexe E: Cloud Model Selection Checklist

Match your data classification to the recommended cloud deployment.

Classification	Public Cloud Only	Hybrid Cloud	Private Cloud / DSZ
Public	☐ OK	☐ Optional	☐ Optional
Internal	☐ Not Recommended	☐ Preferred	☐ Optional
Confidential	☐ Not Recommended	☐ Allowed	☐ Preferred

Draft

Classification	Public Cloud Only	Hybrid Cloud	Private Cloud / DSZ
Restricted	☐ Not Allowed	☐ Conditional	☐ Preferred / DSZ
Top Secret / National Security	☐ Not Allowed	☐ Not Allowed	☐ Required (DSZ)

Match your service classification to the recommended data centre (uptime) tier deployment.

Classification	Uptime Tier I	Uptime Tier II	Uptime Tier III	Uptime Tier IV
Non-Critical	☐ OK	☐ Preferred	☐ Optional	☐ Optional
Core Government	☐ Not Allowed	☐ Conditional	☐ Preferred	☐ Preferred
Mission-Critical	☐ Not Allowed	☐ Not Allowed	☐ Required	☐ Preferred

Note: Additionally, mission-critical services may require local DSZ even if required connectivity guarantees are met (e.g. response time, geopolitical tensions).

Usage:

1. **Use** the Data Classification Checklist in Annexe B to determine its classification.
2. **Select controls** in Annexe C according to that classification.
3. **Use** the Service Classification Checklist in Annexe D to determine its classification.
4. **Choose your cloud model** and **data centre tier** via Annexe D, ensuring alignment with deployment tiers and sovereignty tiers in the main policy.

This annexe and these checklists will help ensure that every piece of government data is handled in full compliance with your revised Cloud Policy—meeting security, residency, and sovereignty requirements end-to-end.

Draft