TANZANIA BUREAU OF STANDARDS (TBS)

PRIVACY AND PERSONAL DATA PROTECTION POLICY

Document Status: Draft
Version: 1.0
Effective Date: [Insert Date]
Review Date: [Insert Date]
Policy Owner: Tanzania Bureau of Standards
Responsible Department: ICT / Legal / Administration
Approved By: [Insert Approving Authority]

---

1. INTRODUCTION

The Tanzania Bureau of Standards (TBS) is committed to protecting the privacy, confidentiality, integrity and security of personal data entrusted to the Bureau by customers, employees, suppliers, stakeholders, applicants, visitors and members of the public.

This Privacy and Personal Data Protection Policy establishes the principles, procedures and controls that govern the collection, processing, use, storage, disclosure, sharing, retention and disposal of personal data by TBS.

The Policy applies to personal data processed through:

- TBS official website;
- Online Application System (OAS);
- Integrated Standardisation, Quality Assurance, Metrology and Testing System (iSQMT);
- Content Management System (CMS);
- TBS email systems;
- Human Resource and employee management systems;
- Laboratory Information Management Systems;
- Certification and inspection systems;
- Customer and stakeholder databases;
- Financial and procurement systems;
- ICT infrastructure and databases;
- CCTV and physical security systems;
- Mobile applications and electronic platforms;
- Social media platforms operated by TBS;
- Electronic forms, surveys and feedback systems;
- TBS intranet;
- Cloud-based services approved by TBS;
- Third-party systems used to provide TBS services; and
- Any future information system operated or authorized by TBS.

2. PURPOSE OF THE POLICY

The purpose of this Policy is to:

1. Protect personal data held and processed by TBS.
2. Ensure compliance with applicable Tanzanian laws and regulations.
3. Establish clear responsibilities for employees and system users.
4. Ensure personal data is collected only for legitimate and specified purposes.
5. Protect personal data against unauthorized access, disclosure, alteration, loss or destruction.
6. Establish appropriate information-security controls for TBS systems.
7. Inform data subjects about how their personal information is handled.
8. Establish procedures for handling privacy complaints and data breaches.
9. Promote responsible use of personal data by TBS employees, contractors and service providers.
10. Ensure privacy is considered when developing, procuring or implementing new TBS systems.

---

3. LEGAL AND REGULATORY FRAMEWORK

This Policy shall be implemented in accordance with applicable laws, regulations, standards and Government directives, including:

- The Constitution of the United Republic of Tanzania;
- Personal Data Protection Act, 2022;
- Personal Data Collection and Processing Regulations, 2023;
- Applicable cybersecurity and electronic communications legislation;
- Standards Act and applicable TBS regulations;
- Government ICT policies and guidelines;
- Records management requirements;
- Applicable employment and public-service requirements;
- Applicable contractual and confidentiality obligations; and
- Other applicable laws and regulations of the United Republic of Tanzania.

The Personal Data Protection Act establishes requirements governing the collection, processing, storage, disclosure and transfer of personal data and provides rights to data subjects.

---

4. SCOPE

This Policy applies to:

4.1 Employees

All permanent and temporary employees, management, Board members, interns, volunteers and other personnel authorized to access TBS information.

4.2 Contractors and Consultants

All contractors, consultants, system developers, auditors and service providers who access TBS systems or personal data.

4.3 Customers and Stakeholders

Individuals and organizations interacting with TBS through physical or electronic channels.

4.4 Information Systems

All information systems, applications, databases, networks, servers, websites, cloud platforms and electronic devices owned, managed or authorized by TBS.

---

5. TYPES OF PERSONAL DATA COLLECTED

Depending on the service being provided, TBS may collect:

5.1 Identification Information

- Full name;
- National identification number where legally required;
- Passport information where applicable;
- Employee identification number;
- Company registration details;
- Signature;
- Photograph.

5.2 Contact Information

- Telephone number;
- Email address;
- Postal address;
- Physical address;
- Business address.

5.3 Professional Information

- Employer;
- Job title;
- Professional qualifications;

- Professional registration information;
- Training records;
- Business information.

5.4 Transaction and Service Information

TBS may collect information relating to:

- Product registration;
- Premise registration;
- Certification;
- Inspection;
- Testing;
- Calibration;
- Import/export services;
- PVoC;
- Destination inspection;
- Management system certification;
- Applications and licences;
- Payments and invoices;
- Complaints and appeals.

TBS's OAS currently supports services including Destination Inspection, PVoC, Conditional Release, Premise Registration, Product Registration and Technical Assistance to Exporters.

5.5 Technical Information

Systems may automatically collect:

- IP address;
- Login information;
- User account information;
- Browser type;
- Device information;
- Operating system;
- Date and time of access;
- System activity logs;
- Authentication records;
- Audit trails;
- Error logs;
- Security logs.

---

6. SPECIAL CATEGORIES OF PERSONAL DATA

TBS shall only collect and process sensitive or special categories of personal data where there is a lawful basis and where such information is necessary for a legitimate TBS function.

Such information shall receive enhanced security and access controls.

Examples may include:

- Health information where required for employment or occupational purposes;
- Biometric information where lawfully implemented;
- Financial information;
- Identification documents;
- Other sensitive information protected under applicable law.

---

7. HOW TBS COLLECTS PERSONAL DATA

TBS may collect personal information through:

- TBS websites;
- Online application forms;
- iSQMT;
- OAS;
- Physical application forms;
- Email;
- Telephone;
- Customer service desks;
- Laboratory services;
- Inspection activities;
- Certification activities;
- Registration processes;
- Surveys;
- Complaints;
- Social media;
- CCTV;
- Recruitment processes;
- Procurement processes;
- Conferences and events;
- Correspondence;
- Authorized third-party systems.

---

8. PURPOSES OF PROCESSING PERSONAL DATA

TBS may process personal data for legitimate institutional purposes, including:

1. Provision of TBS services.
2. Processing applications.
3. Product registration.

4. Product certification.
5. Inspection and testing.
6. Laboratory services.
7. Calibration services.
8. Management system certification.
9. Processing payments.
10. Customer communication.
11. Handling complaints and appeals.
12. Enforcement of applicable standards and regulations.
13. Staff administration.
14. Recruitment.
15. Procurement.
16. Financial management.
17. ICT administration.
18. Security and access control.
19. Fraud prevention.
20. Cybersecurity monitoring.
21. Audit and accountability.
22. Statistical analysis and reporting.
23. Government reporting.
24. Legal and regulatory compliance.
25. Improving TBS services.

---

9. PRINCIPLES OF PERSONAL DATA PROTECTION

TBS shall apply the following principles:

9.1 Lawfulness

Personal data shall only be collected and processed on a lawful basis.

9.2 Fairness and Transparency

Individuals shall be informed about how their personal information is being processed.

9.3 Purpose Limitation

Personal data shall only be used for specified and legitimate purposes.

9.4 Data Minimisation

TBS shall collect only information reasonably necessary for the intended purpose.

9.5 Accuracy

Reasonable measures shall be taken to ensure that personal data is accurate and up to date.

9.6 Storage Limitation

Personal data shall not be retained longer than necessary, subject to legal, regulatory and records-management requirements.

9.7 Security

Appropriate technical and organizational safeguards shall be implemented to protect personal data.

9.8 Accountability

TBS shall maintain appropriate records and controls demonstrating compliance with applicable data-protection requirements.

---

10. TBS WEBSITE PRIVACY

The TBS website may collect information submitted by users through:

- Contact forms;
- Feedback forms;
- Application links;
- Subscription services;
- Complaints;
- Online enquiries;
- Downloads and requests;
- Other electronic services.

TBS shall clearly inform website visitors about:

- Information being collected;
- Purpose of collection;
- Use of cookies where applicable;
- Third-party services;
- Contact mechanisms;
- Data-security measures;
- Data-subject rights.

TBS's current website identifies Privacy Policy, Terms & Conditions, Copyright Statement and Disclaimer among its website resources.

---

11. PRIVACY IN TBS ONLINE SYSTEMS

All TBS systems processing personal data shall implement appropriate privacy and security controls.

These include:

11.1 User Authentication

Users shall have unique accounts where required.

Shared user accounts shall be prohibited unless specifically authorized for technical or operational reasons.

11.2 Password Management

Systems shall enforce appropriate password requirements and, where technically feasible, multi-factor authentication.

11.3 Role-Based Access

Users shall only access information necessary for their assigned responsibilities.

11.4 User Access Review

System administrators shall periodically review user accounts and privileges.

Access shall be removed or modified promptly when:

- An employee leaves TBS;
- An employee changes department;
- A contract expires;
- A user's role changes;
- Access is no longer required.

11.5 Audit Trails

Critical systems shall maintain logs showing:

- User login;
- User logout;
- Records accessed;
- Records created;
- Records modified;
- Records deleted;
- Administrative activities;
- Security events.

---

12. iSQMT PRIVACY REQUIREMENTS

The iSQMT system shall protect personal and business information processed through TBS services.

Access to customer information shall be based on official responsibilities.

The system should maintain:

- User identification;
- Access controls;
- Audit trails;
- Application history;
- Data modification history;
- System logs;
- Backup records;
- Security monitoring.

Users shall not download, copy, disclose or distribute customer information unless authorized.

---

13. ONLINE APPLICATION SYSTEM (OAS)

Personal data submitted through OAS shall only be used for purposes related to the service for which the information was provided or other lawful TBS functions.

OAS shall implement appropriate controls including:

- Secure authentication;
- Encryption in transit;
- Access control;
- Application audit trails;
- Secure database management;
- Backup;
- Monitoring;
- Vulnerability management;
- Data retention controls.

---

14. EMAIL PRIVACY

TBS official email systems may contain confidential and personal information.

Employees shall:

- Use official email for official business;
- Avoid sending personal data to unauthorized recipients;
- Verify recipients before sending sensitive information;
- Avoid unnecessary forwarding of confidential information;
- Use approved secure methods for sensitive documents;
- Report suspected phishing or unauthorized disclosure immediately.

---

15. CCTV AND PHYSICAL SECURITY

TBS may use CCTV and other security technologies for:

- Protection of employees;
- Protection of visitors;
- Protection of TBS property;
- Prevention and investigation of security incidents;
- Access control;
- Workplace security.

CCTV footage shall only be accessed by authorized personnel and shall be retained in accordance with applicable law, security requirements and TBS records-management procedures.

---

16. COOKIES AND WEBSITE TECHNOLOGIES

TBS websites may use cookies or similar technologies to:

- Improve website functionality;
- Understand website usage;
- Maintain user sessions;
- Improve security;
- Improve user experience.

Where required, users shall be provided with appropriate information and choices concerning cookies.

---

17. DATA SHARING AND DISCLOSURE

TBS shall not disclose personal data indiscriminately.

Personal data may be disclosed where:

1. Required by law;
2. Required by a court or competent authority;
3. Necessary to provide a TBS service;
4. Required for regulatory functions;
5. Necessary for auditing;
6. Required for legitimate Government functions;
7. Necessary for investigation of fraud or security incidents;
8. Authorized by the data subject where consent is the applicable legal basis;
9. Required by an authorized service provider under a lawful contractual arrangement.

---

18. THIRD-PARTY SERVICE PROVIDERS

Where TBS engages third parties to process personal data, appropriate contractual and technical controls shall be established.

Service providers may include:

- ICT system developers;
- Hosting providers;
- Cloud service providers;
- Payment service providers;
- ICT support providers;
- Security service providers;
- Auditors;
- Consultants.

Third parties shall only process personal data for authorized purposes and shall be required to maintain appropriate confidentiality and security controls.

---

19. CROSS-BORDER DATA TRANSFERS

Where personal data is transferred outside Tanzania, TBS shall ensure that the transfer is undertaken in accordance with applicable Tanzanian data-protection requirements.

Appropriate safeguards, approvals, contractual arrangements or other lawful mechanisms shall be applied where required.

The Personal Data Collection and Processing Regulations specifically address procedures for transferring personal data outside the country.

---

20. INFORMATION SECURITY

TBS shall implement reasonable technical and organizational measures including:

- Firewalls;
- Antivirus and endpoint protection;
- Encryption;
- Secure authentication;
- Access controls;
- Network segmentation where appropriate;
- Backup systems;
- Disaster recovery;
- Security monitoring;
- Vulnerability assessments;
- Patch management;
- Penetration testing where appropriate;
- Physical security;
- Secure configuration;
- Incident management.

---

21. DATA BACKUP AND RECOVERY

Critical TBS systems shall have appropriate backup arrangements.

Backups shall:

- Be performed according to approved schedules;
- Be protected from unauthorized access;
- Be tested periodically;
- Have appropriate retention periods;
- Support disaster recovery;
- Be protected against accidental deletion and corruption.

Backup copies containing personal data shall receive the same level of protection as the original information.

---

22. DATA BREACH MANAGEMENT

A personal data breach may include:

- Unauthorized access;
- Unauthorized disclosure;

- Loss of personal data;
- Theft of equipment containing personal data;
- Hacking;
- Malware or ransomware;
- Accidental disclosure;
- Unauthorized modification;
- Destruction of personal data;
- Sending information to the wrong recipient.

Employees must immediately report suspected breaches to the designated TBS ICT/Data Protection authorities.

TBS shall:

1. Identify and contain the incident.
2. Assess the nature and extent of the breach.
3. Determine affected systems and individuals.
4. Preserve relevant evidence and logs.
5. Take corrective measures.
6. Notify relevant authorities where required by law.
7. Notify affected individuals where legally required.
8. Document the incident.
9. Conduct a post-incident review.

---

23. DATA RETENTION

TBS shall establish retention periods for different categories of information.

Retention shall consider:

- Legal requirements;
- Regulatory requirements;
- Public-sector records requirements;
- Operational requirements;
- Contractual obligations;
- Audit requirements;
- Historical and archival requirements.

When personal data is no longer required, it shall be securely:

- Deleted;
- Destroyed;
- Anonymised; or
- Archived where legally required.

---

24. DATA SUBJECT RIGHTS

Subject to applicable law and lawful limitations, individuals may have rights relating to their personal data, including rights to:

- Be informed about processing;
- Access their personal data;
- Request correction of inaccurate information;
- Request appropriate restriction of processing;
- Object to certain processing;
- Request deletion where legally applicable;
- Exercise other rights provided under applicable data-protection legislation.

Requests shall be handled through an established TBS procedure.

---

25. EMPLOYEE PRIVACY

TBS shall protect employee information processed for:

- Recruitment;
- Employment administration;
- Payroll;
- Leave;
- Performance management;
- Training;
- Disciplinary processes;
- Pension and benefits;
- Occupational requirements;
- Security;
- Legal compliance.

Employees shall only access personnel information where authorized.

---

26. LABORATORY AND TESTING INFORMATION

Personal information associated with laboratory customers, applicants, test requests, sample submissions and reports shall be protected against unauthorized access.

Laboratory personnel shall maintain confidentiality regarding customer information and test results in accordance with applicable TBS procedures and relevant standards.

---

27. INSPECTION AND CERTIFICATION INFORMATION

Information obtained during:

- Product inspections;
- Premise inspections;
- Certification audits;
- Laboratory testing;
- Management-system certification;
- Market surveillance;
- Verification activities;

shall be treated as confidential where required by law, contract, policy or applicable standards.

TBS already recognizes confidentiality as an important element of its Management Systems Certification activities.

---

28. SOCIAL MEDIA

TBS social media platforms may collect or receive information when individuals:

- Comment;
- Send messages;
- Participate in campaigns;
- Submit questions;
- Participate in surveys;
- Interact with TBS posts.

TBS shall avoid publishing personal information without an appropriate lawful basis or authorization.

Photographs and videos taken during TBS events shall be managed in accordance with applicable privacy, communications and records-management requirements.

---

29. PUBLICATION OF INFORMATION

TBS may publish information necessary to fulfil its statutory and public-information functions.

Where personal information is published, TBS shall consider:

- Legal authority;

- Necessity;
- Public interest;
- Privacy risks;
- Accuracy;
- Security implications.

Personal information that is not necessary for public disclosure shall not be published unnecessarily.

---

30. INFORMATION CLASSIFICATION

TBS should classify information into appropriate categories, such as:

Public

Information approved for public release.

Internal

Information intended for TBS employees and authorized users.

Confidential

Information that could cause harm if disclosed without authorization.

Restricted/Highly Confidential

Highly sensitive information requiring strict access controls.

Personal data shall be classified according to its sensitivity and associated risks.

---

31. PRIVACY BY DESIGN

Privacy and data protection shall be considered when TBS:

- Develops new systems;
- Procures software;
- Implements new databases;
- Introduces mobile applications;
- Integrates systems;
- Migrates data;
- Introduces cloud services;
- Changes ICT infrastructure.

Before implementing systems that significantly process personal data, TBS should conduct appropriate privacy and security risk assessments.

---

32. SYSTEM INTEGRATION

Where TBS systems exchange information, integrations shall be controlled through:

- Authorized APIs;
- Secure data-transfer mechanisms;
- Authentication;
- Encryption;
- Access controls;
- Audit logs;
- Data minimisation;
- Data validation.

Unauthorized extraction or transfer of information between systems is prohibited.

---

33. REMOTE ACCESS

Remote access to TBS systems containing personal data shall only be permitted through approved mechanisms.

Where applicable, TBS shall implement:

- VPN;
- Multi-factor authentication;
- Device security;
- Session controls;
- Access logging;
- Encryption.

---

34. MOBILE DEVICES AND LAPTOPS

Employees handling personal data on laptops, tablets or mobile devices shall ensure that devices are:

- Password protected;
- Encrypted where appropriate;
- Updated;
- Protected against malware;
- Configured with automatic screen locking;

- Secured against unauthorized access.

Loss or theft of a device containing TBS personal data must be reported immediately.

---

35. USB AND REMOVABLE STORAGE

The use of USB drives and other removable storage devices containing personal or confidential information shall be controlled.

Where possible, sensitive information should be transferred using approved secure systems rather than unmanaged removable media.

---

36. CLOUD SERVICES

TBS shall only use cloud services that have been properly assessed and authorized.

Before approving a cloud service, TBS should consider:

- Data location;
- Security controls;
- Encryption;
- Access controls;
- Backup;
- Disaster recovery;
- Vendor obligations;
- Data-transfer requirements;
- Data retention;
- Exit arrangements.

---

37. DATA ACCURACY

TBS shall take reasonable measures to ensure that personal information is:

- Accurate;
- Complete where necessary;
- Current;
- Relevant to the purpose for which it is processed.

Data subjects should be provided with appropriate mechanisms to request correction of inaccurate information.

---

38. EMPLOYEE RESPONSIBILITIES

Every TBS employee shall:

- Protect personal information;
- Use systems only for authorized purposes;
- Keep passwords confidential;
- Follow ICT security procedures;
- Avoid unauthorized disclosure;
- Report security incidents;
- Respect confidentiality;
- Complete required privacy and cybersecurity training.

Failure to comply may result in disciplinary or other appropriate action.

---

39. ICT DEPARTMENT RESPONSIBILITIES

The ICT Department shall:

1. Implement appropriate technical safeguards.
2. Manage system access.
3. Maintain security logs.
4. Monitor systems.
5. Manage backups.
6. Coordinate vulnerability assessments.
7. Support incident response.
8. Maintain system documentation.
9. Ensure secure system configuration.
10. Support privacy impact assessments.
11. Coordinate system security reviews.
12. Ensure secure disposal of ICT equipment.

---

40. DATA PROTECTION / PRIVACY OFFICER

TBS shall designate an appropriate officer or function responsible for coordinating data-protection matters.

The responsible officer shall:

- Coordinate privacy compliance;
- Advise management;
- Support privacy assessments;
- Coordinate data-subject requests;

- Support breach management;
- Maintain privacy documentation;
- Coordinate awareness programmes;
- Liaise with relevant regulatory authorities;
- Monitor implementation of this Policy.

---

41. TRAINING AND AWARENESS

TBS shall provide regular training to employees on:

- Personal data protection;
- Cybersecurity;
- Phishing;
- Password security;
- Confidentiality;
- Data handling;
- Social engineering;
- Incident reporting;
- Secure use of TBS systems.

New employees should receive privacy and information-security awareness as part of induction.

---

42. PRIVACY COMPLAINTS

Individuals who believe their personal information has been improperly processed may submit a complaint to TBS through the designated complaints channels.

TBS shall investigate complaints and take appropriate corrective measures.

Where appropriate, complaints may also be directed to the Personal Data Protection Commission (PDPC), which is responsible for overseeing implementation of Tanzania's personal-data protection framework.

---

43. CONTACT DETAILS

For privacy-related enquiries, requests or complaints:

Tanzania Bureau of Standards (TBS)
Headquarters
Sam Nujoma Road / Morogoro Road
Ubungo

P.O. Box 9524
Dar es Salaam, Tanzania

Telephone: +255 22 245 0206
Toll Free: 0800110827
Email: info@tbs.go.tz
Complaints: complaints@tbs.go.tz

TBS currently publishes these general contact and complaints channels on its website.

Privacy/Data Protection Contact:
[Insert designated Data Protection Officer/Privacy Officer]
[Insert official privacy email]

---

44. POLICY VIOLATIONS

Unauthorized:

- Access;
- Collection;
- Copying;
- Disclosure;
- Modification;
- Downloading;
- Sharing;
- Sale;
- Transfer;
- Destruction;

of personal data may constitute a violation of TBS policy and applicable law.

Appropriate administrative, disciplinary, contractual or legal action may be taken.

---

45. POLICY REVIEW

This Policy shall be reviewed periodically and whenever there are significant changes to:

- Applicable legislation;
- TBS functions;
- ICT systems;
- Data-processing activities;
- Cybersecurity threats;
- Organizational structure;

• Government ICT requirements.

---

46. APPROVAL

This Policy shall take effect upon approval by the authorized TBS approving authority.

Prepared by: ___
Name: ___
Position: ____
Date: _____

Reviewed by: ___
Name: ___
Position: ___
Date: _____

Approved by: ___
Name: ___
Position: ___
Date: _____

ANNEX 1: TBS SYSTEMS AND PRIVACY CONTROL MATRIX

TBS System/ Platform	Information Processed	Main Privacy Risk	Required Controls
TBS Website	Names, emails, enquiries, IP/log data	Unauthorized disclosure	Privacy notice, HTTPS, access controls, secure hosting
OAS	Customer/application information	Unauthorized access	Authentication, encryption, audit logs, backups
iSQMT	Customer, certification, inspection and service data	Excessive access	Role-based access, audit trails, encryption
CMS	Website administrator information	Unauthorized publication	User roles, MFA, logs, approval workflow
HR System	Employee information	Unauthorized disclosure	Restricted access, encryption, audit trails
Laboratory Systems	Customer/sample/testing information	Confidentiality breach	Role-based access, secure storage, audit logs

TBS System/ Platform	Information Processed	Main Privacy Risk	Required Controls
Certification Systems	Company/client information	Unauthorized disclosure	Confidentiality controls and access restrictions
Email	Personal and official correspondence	Phishing/data leakage	MFA, spam filtering, encryption where appropriate
CCTV	Images/video	Unauthorized viewing	Restricted access and retention controls
TBS Intranet	Internal information	Unauthorized access	Authentication, authorization, monitoring
Financial Systems	Payment/accounting information	Fraud/data theft	Segregation of duties, access control, audit logs
Procurement Systems	Supplier information	Unauthorized disclosure	Role-based access and secure records
Social Media	Names, comments, photographs	Unlawful publication	Moderation and privacy controls
Backup Systems	Copies of system databases	Data leakage	Encryption, restricted access, secure backup storage

ANNEX 2: MINIMUM SECURITY CONTROLS FOR TBS SYSTEMS

Every critical TBS information system should, where applicable, implement:

- Unique user accounts;
- Strong passwords;
- Multi-factor authentication;
- Role-based access control;
- Encryption;
- Secure backups;
- Audit logs;
- Security monitoring;
- Antivirus/endpoint protection;
- Vulnerability management;
- Patch management;
- Disaster recovery;
- Business continuity;
- Secure system development;
- Data retention controls;
- Secure disposal;

- Incident response procedures.

ANNEX 3: PRIVACY CHECKLIST FOR NEW TBS SYSTEMS

Before a new system is deployed, TBS should confirm:

- [ ] The purpose of collecting personal data has been identified.
- [ ] The categories of personal data have been identified.
- [ ] The lawful basis for processing has been established.
- [ ] Only necessary data is collected.
- [ ] Data retention requirements have been established.
- [ ] User access levels have been defined.
- [ ] Security requirements have been documented.
- [ ] Audit logging has been implemented.
- [ ] Backup and recovery requirements have been established.
- [ ] Data-sharing arrangements have been documented.
- [ ] Third-party processor requirements have been assessed.
- [ ] Cross-border data-transfer implications have been assessed where applicable.
- [ ] Privacy risks have been assessed.
- [ ] Appropriate privacy notices have been prepared.
- [ ] Incident-response arrangements are available.
- [ ] Data protection responsibilities have been assigned.
- [ ] The system has undergone appropriate security testing before production use.

ANNEX 4: IMPORTANT IMPLEMENTATION ACTIONS FOR TBS

To operationalize this Policy, TBS should establish:

1. **TBS Data Protection Register** – showing all categories of personal data collected and processed.
2. **System Data Inventory** – covering OAS, iSQMT, CMS, HR, laboratory, certification, financial and other systems.
3. **Data Retention Schedule** – specifying how long different categories of information should be retained.
4. **User Access Review Procedure** – periodic review of all system accounts.
5. **Data Breach Response Procedure** – clear escalation and reporting process.
6. **Privacy Impact Assessment Procedure** – for new or substantially changed systems.
7. **Third-Party Data Processing Agreements** – for vendors handling TBS personal data.
8. **Employee Privacy and Cybersecurity Training Programme**.
9. **Website Privacy Notice** – clearly displayed on the TBS website.
10. **Data Subject Request Procedure** – for access, correction and other applicable rights.
11. **Information Classification Procedure**.
12. **Secure Data Disposal Procedure**.
13. **ICT Backup and Restoration Procedure**.
14. **System Audit and Logging Procedure**.

15. **Periodic Privacy Compliance Audit**.

---

47. DISCLAIMER

This Policy is intended as an institutional policy framework for TBS and should be reviewed and validated by TBS Legal, ICT, Records Management and the designated data-protection function before formal approval and publication.

It should also be aligned with the latest requirements and guidance issued by the Personal Data Protection Commission (PDPC). The PDPC itself provides a website privacy-notice template intended to be customized according to an organization's actual processing activities and legal obligations.