UNIVERSAL TECHNOLOGY AND MANAGEMENT UNIVERSITY

UTAMU

For an Open Mind

UTAMU INFORMATION GOVERNANCE STATUTE AND CONTROL CODE

2026

Table of Contents

List of Accronyms

Acronym	Meaning
AI	Artificial Intelligence
AWS	Amazon Web Services
CMS	Content Management System
CSF	Cybersecurity Framework (NIST)
DPA	Data Protection and Privacy Act, 2019 (Cap 97)
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DSAR	Data Subject Access Request
ERP	Enterprise Resource Planning System
GDPR	General Data Protection Regulation (EU)
HR	Human Resources
HRIS	Human Resource Information System
HTTPS	Hypertext Transfer Protocol Secure
ICT	Information and Communication Technology
IGC	Information Governance Committee
ISO	International Organization for Standardisation
KPI	Key Performance Indicator
LMS	Learning Management System
NCHE	National Council for Higher Education
NIST	National Institute of Standards and Technology
PDPO	Personal Data Protection Office (Uganda)
PII	Personally Identifiable Information
RACI	Responsible, Accountable, Consulted, Informed
SaaS	Software as a Service
SIS	Student Information System
SSL	Secure Sockets Layer

Approval

This Information Governance Statute and Control Code is issued as a binding internal regulatory instrument of Universal Technology and Management University (UTAMU) and shall take effect upon approval by the Board of Directors following formulation and recommendation by the University Council.

Submitted By: _____**Date: 7th May, 2026**

Chairperson, Board of Directors

Signed By:……Date…**7th May 2026**

Secretary, Board of Directors

1.0 INTRODUCTION

1.1 Background

Universal Technology and Management University (UTAMU) was granted a provisional license by the National Council for Higher Education (NCHE) on 11th March 2013 (License No. UIPL022), and its name and particulars were published in the Uganda Gazette Vol. CVI No. 14 of 22nd March 2013 under Legal Notice No. 4 of 2013. UTAMU operates within the core mandate of Teaching and Learning, Research and Innovation, and Community Engagement. Governance of information assets is therefore integral to institutional credibility, regulatory compliance, academic integrity, and operational resilience.

This Statute is aligned with the requirements of the National Council for Higher Education (NCHE) and UTAMU's strategic direction.

1.2 Vision

The Vision of UTAMU is A global educational institution of excellence in management, science, technology and innovation.

1.3 Mission

The mission of UTAMU is to provide global quality education, research and innovation critical to economic and human development.

1.4 Core Values

The Core values of UTAMU are:

a) **Professionalism:** making sure that staff and students conduct themselves with the highest ethical standards and taking responsibility for all their actions

b) **Creativity:** committing to stimulating the culture of scientific and technological advancement, innovation and practical enrichment to UTAMU's stakeholders through a rich and flexible educational experience

c) **Integrity:** adhering to ethical and moral principles in all the educational, research and innovation processes

d) **Transparency:** seeking to provide accountability and value for money to UTAMU's stakeholders

e) **Empowerment:** offering unsurpassed practical opportunities to UTAMU's stakeholders through industry-oriented collaborations, research engagements and incubation clusters in order to transform the educational environment

f) **Community Engagement:** working with the community to solve real-world problems as a focal point towards economic development.

PART I: INFORMATION GOVERNANCE STATUTE

1. Authority

This Statute and Control Code constitute binding institutional governance authority for the protection, processing, management, security, and oversight of all University information assets.

It prevails over subordinate policies and procedures in the event of inconsistency and shall be binding upon all officers, staff, students, contractors, and third parties acting on behalf of the University.

This instrument shall be interpreted purposively to give effect to statutory compliance, enterprise risk mitigation, and institutional accountability.

This Statute shall be read together with Annex I (RACI Matrix), Annex II (Statutory Reconciliation), Annex III (Information Asset Domicile Register), Annex IV (Governance Templates & Control Instruments), Annex V (Domicile–Control–KPI Alignment Matrix), and Annex VI (International Alignment Matrix), which form an integral and binding part of this instrument.

The Annexes form an integral and binding part of this Statute. References to this Statute shall include its Annexes unless expressly stated otherwise.

2. Purpose

This Statute and Control Code establish the University's authoritative governance architecture for information assets. It operationalises statutory and regulatory obligations; codifies enforceable institutional control standards; embeds accountability, risk oversight, and audit traceability; protects institutional, academic, research, financial, and personal data assets; and safeguards institutional integrity, regulatory defensibility, and operational resilience.

The operationalisation of this purpose is structured through Annex III (Asset Register), Annex IV (Control Instruments), and Annex V (KPI Linkage Matrix).

3. Scope

This instrument applies to:

a) All academic and administrative units;

b) All physical, digital, and cloud-based systems;

c) All personal data and institutional data processed by the University;

d) All third-party processors and service providers handling University information.

e) All cross-border data transfers and international collaborations involving University information assets

All systems within scope must be declared in Annex III prior to operation.

Third parties processing University information assets shall be contractually bound to comply with this Statute through enforceable data processing agreements and vendor control instruments (Annex IV F-10 and F-11).

4. Definitions

a. **Information Asset**: Any data, system, record, database, document, repository or digital platform owned, controlled or processed by the University.
b. **Personal Data**: Information relating to an identified or identifiable natural person.
c. **Data Controller**: The entity that determines the purposes and means of processing personal data.
d. **Data Processor**: An entity that processes personal data on behalf of the Data Controller.
e. **High-Risk Processing**: Processing activities presenting elevated legal, reputational, operational or ethical risk requiring documented assessment.
f. **Control Owner**: Officer accountable for implementation, monitoring and effectiveness of specific governance controls.
g. **Incident:** Any event compromising the confidentiality, integrity or availability of information assets.
h. **AI System**: Any automated or semi-automated system that processes data to generate decisions, recommendations, classifications or predictive outputs.
i. **Information Asset Domicile**: A formally declared system, repository, platform or physical archive recorded in Annex III and subject to governance controls.

5. Governance Structure

a. **University Council** — Formulation and Oversight Authority
b. **Board of Directors** — Final Approval and Strategic Oversight
c. **Vice Chancellor** — Executive Accountability
d. **Information Governance Committee (IGC)** - Operational Oversight and KPI Monitoring.
e. **Data Protection Officer (DPO)** — Statutory Privacy Compliance
f. **Head ICT Services**— Information Security Accountability
g. **Registrar** — Records Lifecycle Governance
h. **Legal Counsel** — Regulatory Interpretation and Contractual Safeguards.

Oversight authority shall not dilute executive accountability. Delegation of operational duties does not transfer constitutional or statutory responsibility.

Role accountability and instrument ownership are detailed in Annex I (RACI Matrix)

6. Accountability and Reporting

a. Quarterly information governance review meetings shall be conducted.
b. An Annual Information Governance Report shall be submitted within 90 days of the financial year end.
c. Incidents classified as High or Critical under Section 15 shall be escalated to executive leadership within forty-eight (48) hours of identification.

d. Corrective actions shall be documented and tracked to verified closure.

e. KPI variance exceeding defined thresholds shall trigger formal review and documented corrective action.

f. Performance reporting shall utilise the Quarterly Governance Review Template (Annex IV F-15) and shall be evaluated against the indicators defined in Part III and Annex V.

7. Institutional Positioning Statement

The UTAMU Information Governance Statute and Control Code is:

a. Statutorily compliant with Uganda's Data Protection and Privacy Act (Cap 97);

b. Structurally aligned with GDPR principles of accountability and risk-based governance;

c. Operationally consistent with ISO 27001 information security control families;

d. Privacy-extended in alignment with ISO 27701;

e. Cybersecurity-informed using the NIST Identify–Protect–Detect–Respond–Recover model.

f. While UTAMU does not claim formal ISO certification unless independently verified, this Statute adopts control architectures consistent with internationally recognised best practice.

PART II: CONTROL DOMAINS

Each Control Domain constitutes a mandatory institutional control layer. Controls are cumulative and shall be interpreted together to ensure comprehensive governance coverage.

8. Data Protection

The University shall ensure lawful processing of personal data in accordance with applicable data protection law and this Statute.

The Data Protection Governance Domain shall include:

a. Maintenance of an up-to-date Data Processing Register (Annex IV F-01).

b. Determination and documentation of lawful basis for processing.
c. Performance of Data Protection Impact Assessments (DPIA) for high-risk processing (F-02).
d. Management of Data Subject Access Requests (F-03).
e. Personal data breach notification procedures (F-04).
f. Oversight of cross-border data transfers (F-12).
g. Maintenance of regulatory registration and liaison records (F-16).

Where consent is relied upon as the lawful basis for processing, such consent shall be demonstrable, specific, informed, freely given, and capable of withdrawal at any time. Consent shall not be presumed where another lawful basis applies.

9. Information Security

Technical safeguards, including encryption at rest and in transit, access control, authentication protocols, patch management, backup integrity, and incident response, shall be governed under this domain.

The University shall:

a. Maintain an inventory of information assets with assigned asset owners.
b. Conduct annual information security risk assessments.
c. Enforce role-based access controls with a quarterly review.
d. Apply multi-factor authentication to critical systems.
e. Conduct regular backup and restoration testing.
f. Maintain documented incident response procedures.
g. Test business continuity and disaster recovery arrangements annually.
h. Conduct periodic penetration testing for externally facing systems.
i. Maintain documented patch management procedures.

Information security controls shall apply to all digital and physical domiciles listed in Annex III and shall be implemented using Annex IV instruments F-05, F-06, F-14 and related controls. Monitoring and escalation thresholds are defined in Annex V. The University shall implement appropriate technical and organisational measures proportionate to the nature, scope, context, and risk of processing activities.

Appropriate technical safeguards, including encryption where proportionate to the level of risk, shall be implemented to protect information assets.

10. Digital Platform and Website Governance

The University shall maintain governance controls over institutional digital platforms, websites, public portals, and online service interfaces to ensure accuracy, integrity, lawful publication, and secure operation.

This Domain shall include:

a. Assignment of accountable content owners.
b. Version control and review cycles for published material.
c. Oversight of hosting providers and cloud infrastructure.

d. Secure configuration and vulnerability management.
e. Documentation of website data capture mechanisms (Annex IV F-17).
f. Suspension of non-compliant digital processing pending remediation.

All personal data collected via digital platforms shall additionally comply with Section 8 (Data Protection Governance).

11. Records and Lifecycle Management

The University shall:

a. Classify records at creation.
b. Maintain approved retention schedules.
c. Require dual authorisation for record disposal.
d. Maintain a Disposal Register.
e. Implement Legal Hold procedures where litigation or investigation risk exists.
f. Preserve archival integrity and prevent unauthorised destruction.
g. Destruction of records outside approved retention schedules constitutes a disciplinary breach.

Records lifecycle controls apply to all physical and digital repositories declared in Annex III and shall be implemented through Annex IV instrument F-07 and monitored under the Retention Compliance KPI defined in Part III and Annex V. Where litigation, investigation, or regulatory inquiry is anticipated, relevant records shall be preserved under formal Legal Hold until written clearance is issued by Legal Counsel.

Records retention schedules shall be approved by the Registrar in consultation with Legal Counsel and reviewed periodically.

12. Artificial Intelligence Governance

The University shall:

a. Maintain an AI Systems Register.
b. Classify AI tools as Low, Medium, or High Risk.
c. Conduct documented impact assessments for High-Risk AI.
d. Require human oversight in admissions, grading, employment, and disciplinary decisions.
e. AI systems shall not be deployed to make fully autonomous decisions in consequential academic, employment, or disciplinary matters unless demonstrable human oversight, review, and override capability is maintained.
f. Conduct annual AI performance and fairness review.

g. AI deployments shall comply with principles of fairness, transparency, accountability, and proportionality.

AI tools shall not be deployed in a manner that replaces human decision-making in consequential academic, employment, or disciplinary determinations without documented oversight and review. All AI systems must be registered in Annex III (D-10) and governed using Annex IV instruments F-08 and F-09. Performance and risk thresholds are defined in Annex V.

High-risk AI systems shall not be deployed without documented approval by the Information Governance Committee (IGC) and recorded entry in the AI Systems Register (Annex III D-10).

PART III: OPERATIONAL GOVERNANCE

All University information assets shall be formally declared in Annex III (Information Asset Domicile Register). Information systems, repositories, cloud services, AI tools, and physical archives shall be formally declared in Annex III as part of their operational onboarding and governance lifecycle. Deployment of undeclared domiciles constitutes a governance breach and may trigger escalation under Section 15.

13. Information Assets Domicile

Information Asset Domiciles are formally defined in Annex III. All controls, KPIs, and oversight mechanisms shall map to these domiciles. All Information Asset Domiciles shall be governed in accordance with Annex V (Domicile–Control–KPI Alignment Matrix), which provides mandatory linkage between asset category, applicable control domains, required governance instruments, performance indicators, and escalation thresholds. No control instrument listed in Annex IV may be deployed without corresponding domicile registration under Annex III.

No information asset shall process institutional or personal data unless declared in Annex III and mapped to applicable control instruments under Annex IV and performance indicators under Annex V.

14. Key Performance Indicators

KPIs defined in this section are operationalised and mapped to specific domiciles and control instruments through Annex V (Domicile–Control–KPI Alignment Matrix).

Table 1: Performance Key Indicators

Information governance performance shall be monitored through measurable indicators, including:

Domain	Indicator	Target	Related Domicile Category	Owner
Data Protection	Processing Register Coverage	100%	All Personal Data Domiciles	DPO

Data Protection	Breach Logging Timeliness	100% within 24 hrs	All Digital & Physical Systems	DPO / ICT
Information Security	System Uptime	≥ 95%	Core Systems / Cloud / Website	Head of ICT Services
Records Management	Retention Compliance	≥ 95%	Physical Archives / Digital Records	Academic Registrar
AI Governance	AI Register Coverage	Full documented coverage (subject to periodic validation)	AI Systems	IGC
Vendor Governance	Contract Documentation Completeness		AI Systems	Legal
Procurement & Vendor Records	Financial Documentation Completeness		Financial	Finance
Human Resource Records	Staff files completeness		HR Records	HR Office

Quarterly dashboard reporting is mandatory. KPI monitoring shall be conducted using the Quarterly Governance Review Template (Annex IV F-15).

Failure to achieve KPI thresholds for two consecutive reporting cycles, or any material deviation exceeding 10% from target levels, shall trigger a formal review by the Information Governance Committee and escalation to Executive Leadership or the University Council where risk exposure warrants.

15. Risk Management and Escalation

Risk registers shall reference specific domiciles (Annex III) and control instruments (Annex IV), with escalation triggers defined in Annex V.

a. Each control domain shall maintain a Risk Register.

b. Risks shall be categorised as Low, Moderate, High, or Critical. Risk classifications shall be determined using documented criteria considering impact severity, likelihood, regulatory exposure, financial exposure, reputational harm, and operational disruption.

c. Critical risks require executive review.

d. Repeated control failures shall trigger a formal corrective action plan.

e. Escalation pathways shall be documented and auditable.

Risk classification criteria shall be documented and applied consistently across all domains. All risk assessments shall be documented, dated, signed by the responsible officer, and retained as auditable records.

Risk classifications shall be determined using documented criteria considering impact severity, likelihood, regulatory exposure, financial exposure, reputational harm, and operational disruption. Classification methodology shall be approved by the Information Governance Committee and reviewed annually.

16. Audit and Assurance

Audit testing shall verify (i) domicile completeness under Annex III, (ii) instrument utilisation under Annex IV, and (iii) KPI adherence under Annex V.

a. An annual documented internal audit shall be conducted and retained as a formal assurance artefact available for regulatory inspection.
b. Findings shall be formally documented with management response.
c. Corrective actions shall be tracked to verified closure.
d. Documentary evidence shall be maintained for regulatory inspection.
e. Periodic control effectiveness testing shall be conducted.
f. Audit findings rated High or Critical shall be reported to executive leadership within 30 days

Internal audit findings shall not be modified, suppressed, or reclassified without documented justification and a retained audit trail.

17. Review and Amendment

Amendments shall require formulation and recommendation by the University Council and approval by the Board of Directors. Operational updates to Annexes that do not alter constitutional authority may be approved by the Information Governance Committee and shall be reported to Council. No amendment shall dilute statutory compliance obligations without documented legal review.

18. Enforcement and Disciplinary Measures

Breach of this Statute and Control Code may constitute misconduct and may result in disciplinary action in accordance with University regulations, contractual obligations, or applicable law. Failure to utilise mandatory instruments listed in Annex IV or to declare assets under Annex III constitutes a control breach.

Enforcement actions shall be proportionate to the severity of the breach and may include written warning, suspension of system access, disciplinary proceedings, contract termination, or regulatory referral where legally required or appropriate.

19. Training and Awareness

The University shall conduct mandatory annual information governance awareness training for all staff and relevant contractors. Completion rates shall be monitored and reported through the governance dashboard. Training programmes shall incorporate domicile responsibilities (Annex III), instrument usage (Annex IV), and KPI awareness (Annex V).

Failure to complete mandatory training without reasonable cause may result in temporary suspension of system access until compliance is achieved.

20. Interpretation

20.1 Composition of the Information Governance Committee

The Information Governance Committee shall be comprised of the following:

i. The University Secretary (Chairperson)
ii. Director, Quality Assurance
iii. The Academic Registrar
iv. The Head ICT
v. The Head Human Resources (Secretary)

The Committee may co-opt the Guild President or a student representative where matters affecting student information governance arise

Quorum

The quorum for meetings of the Committee shall be 40% of the members

Frequency of meetings

The Information Governance Committee shall meet at least once during the academic year or when an urgent need arises.

20.2 Supremacy

In the event of conflict between this Statute and subordinate policies or procedures, this Statute shall prevail to the extent of inconsistency

20.2 Review Cycle

This Statute shall be reviewed at least once every five (5) years or earlier where required by regulatory change, risk exposure, or Board directive.

20.3 Amendment Authority

Amendments shall require formulation and recommendation by the University Council and approval by the Board of Directors. Operational updates to Annexes that do not alter constitutional authority may be approved by the Information Governance Committee and shall be reported to Council.

20.4 Effective Date

This Statute shall take effect upon approval by the Board of Directors.

ANNEXES

The Annexes form an integral and binding part of this Statute. References to this Statute shall include its Annexes unless expressly stated otherwise.

Annex I – Control Domains & Instruments RACI matrix

Table 1: RACI Matrix

Control Area / Instrument	Responsible (R)	Accountable (A)	Consulted (C)	Informed (I)
Data Processing Register (Annex IV F-01)	Unit Heads	DPO	ICT, Legal	VC, IGC
DPIA (Annex IV F-02)	Unit Heads	DPO	Legal, ICT	IGC, VC
DSAR Handling (F-03)	DPO Office	DPO	Legal, Registrar	VC, IGC
Breach Notification (F-04)	ICT	DPO	Legal	VC, IGC
Security Incident Response (F-05)	ICT	ICT Director	DPO	VC, IGC
Access Control Authorisation (F-06)	ICT	ICT Director	Unit Heads	IGC
Records Disposal (F-07)	Unit Custodian	Registrar	Legal	VC, IGC
AI Register & Risk Assessment (F-08/F-09)	Unit Heads	IGC Chair	ICT, Legal	VC
Vendor Risk Assessment (F-10/F-11)	Procurement/ICT	Legal Counsel	DPO	VC, IGC
Cross-Border Transfer Assessment (F-12)	DPO/Legal	Legal Counsel	ICT	VC, IGC
Asset Domicile Declaration (F-13)	Unit Heads	IGC	ICT	VC
Annual Information Risk Assessment (F-14)	IGC Secretariat	IGC Chair	DPO, ICT, Legal	VC, University Council (where applicable)
Quarterly Governance Review (F-15)	IGC Secretariat	IGC Chair	DPO, ICT, Registrar	VC

Annex II: Data Protection and Privacy Act, Cap 97)

This Annex provides structured reconciliation between the obligations imposed under the Data Protection and Privacy Act, ~~2019~~ (Cap 97) and the controls established under the UTAMU Information Governance Statute and Control Code. It demonstrates statutory traceability, institutional accountability, and control alignment.

Table 2: Statutory Clause Matching

DPA Section	Legal Requirement	Statute Reference	Control Instrument	Evidence Artefact	Responsible Officer
s.7	Lawful and fair processing	Part II – Data Protection	F-01 Processing Register	Processing Activity Log	DPO
s.8	Personal data must be accurate and kept up to date	Data Protection Domain	F-03 DSAR Form	Correction Log	DPO
s.9	Purpose limitation	Processing Controls	F-01 Register	Purpose Declaration	DPO
s.10	Data minimization	Data Classification Controls	F-01 Register	Data Inventory	DPO
s.11	Retention limitation	Records Lifecycle Domain	F-07 Disposal Authorization	Retention Schedule	Registrar
s.12	Security safeguards	Information Security Domain	F-05 Incident Report; F-06 Access Authorization	Security Audit Log	Head of ICT Services
s.13	Data subject rights	Data Subject Rights Controls	F-03 DSAR	DSAR Log	DPO
s.14	Accountability of the data collector	Governance & Reporting	F-15 Quarterly Review	Annual Governance Report	VC / DPO
s.19	Cross-border data transfer	Vendor Governance	F-12 Transfer Assessment	Transfer Assessment Record	Legal / DPO
s.21	Data breach notification	Incident Response	F-04 Breach Notification	Breach Register	DPO
s.22	Registration of the data collector	Governance Structure	F-16 Regulatory Liaison Log	PDPO Registration Certificate	DPO
s.24–26	Access and rectification rights	Data Subject Rights Section	F-03 DSAR	Rights Request Log	DPO
s.28	Security measures	Information Security	F-05 Incident Report; F-14 Risk Assessment	Risk Assessment Report	Head of ICT Services
s.29	Registration compliance	Governance & Accountability	F-16 Regulatory Log	Registration Renewal Record	DPO
s.30–33	Enforcement cooperation	Governance & Escalation	F-16 Regulatory Liaison Log	Inspection Readiness File	DPO

s.34–38	Offences and penalties	Enforcement Section	Disciplinary Record	Misconduct Register	University Secretary

Annex III: Information Asset Domicile Register

All information assets shall be recorded in and governed through this register. Each domicile shall have an assigned Custodian and Control Owner. Failure to declare a domicile constitutes a governance breach.

Table 3: Institutional Asset Domicile Register

Ref	Domicile Category	System / Repository	Physical / Logical Location	Data Classification	Primary Custodian	Control Domain(s)	Linked KPI (Part III)	Risk Rating
D-01	Student Information	Student Information System (SIS)	On-premise / Cloud	Confidential – Personal Data	Academic Registrar	Data Protection; Information Security	Processing Register Coverage; Breach Logging	High
D-02	Teaching & Learning	Learning Management System (LMS)	Cloud-hosted	Confidential / Academic Records	Academic Affairs	Information Security; AI Governance (if automated tools used)	System Uptime ≥95%	High
D-03	Finance	ERP / Finance System	On-premise / Cloud	Confidential – Financial Data	Finance Director	Information Security; Records Management	Financial Documentation Completeness	High
D-04	Human Resources	HR Information System	On-premise	Confidential – Personal & Employment Data	HR Director	Data Protection; Records Lifecycle	Retention Compliance	High
D-05	Research	Research Data Repository	Local Server / Cloud	Sensitive Personal / Research Data	Director Research	Data Protection; Vendor Governance	High-Risk Processing Control	High
D-06	Website & Public Platforms	Website CMS	Cloud	Public + Limited Personal Data	ICT Director / Communications	Digital Governance; Information Security	Processing Register Coverage	Medium
D-07	Email & Collaboration	Institutional Email	Cloud	Confidential / Institutional	ICT Director	Information Security	Incident Closure Rate	High
D-08	Cloud Storage	Cloud Repositories (AWS/Azure/Google)	Cross-border Cloud	Confidential	ICT Director	Vendor Governance; Security	Vendor Compliance KPI	High
D-09	Physical Archives	Records Room / Storage	Physical Campus	Confidential / Historical Records	Registrar	Records Lifecycle Management	Retention Compliance ≥95%	Medium
D-10	AI Systems	AI-enabled systems (Admissions, Analytics)	Cloud / SaaS	Confidential / Derived Data	Information Governance Committee	AI Governance	AI Register Coverage	High

D-11	Vendor Platforms	Payment Gateway / Admissions Portal	Vendor Hosted	Confidential Financial / Personal	Legal + ICT	Vendor Governance	Contract Documentation Completeness	High
D-12	Backup & Recovery	Backup Infrastructure	Offsite / Cloud	All classifications	ICT Director	Information Security	Recovery Test Compliance	Critical
D-13	Procurement & Contracts	Procurement Records	ERP / Physical	Confidential	Procurement Head	Records Management; Vendor Governance	Financial Completeness	Medium
D-14	Governance Records	Council Minutes, Committee Reports	Physical + Digital	Restricted	University Secretary	Governance Oversight	KPI Achievement ≥85%	Medium
D-15	Compliance & Regulatory	PDPO Registration Records	Legal Office	Restricted	DPO	Data Protection	Compliance KPI	Medium

Annex IV: Governance Templates & Control Instruments

All instruments listed in Annex IV are controlled governance documents. Failure to utilise mandatory instruments where required constitutes a control breach under Section 18 (Enforcement).

Table 4: Governance Templates and Instruments Register

Ref	Template / Instrument	Primary Asset Domicile	Control Domain	Purpose	Linked KPI (Part III)	Mandatory / Conditional	Approval Authority	Record Retention
F-01	Data Processing Register	All Personal Data Systems (SIS, LMS, HR, ERP, Website, Research)	Data Protection	Record all processing activities	Processing Register Coverage (100%)	Mandatory	DPO	Permanent
F-02	Data Protection Impact Assessment (DPIA)	High-Risk Digital & Research Systems	Data Protection	Assess risk prior to high-risk processing	Risk Register Review: High-Risk Control	Mandatory (High Risk)	DPO + Approval Authority	Permanent
F-03	Data Subject Access Request (DSAR) Form	All Personal Data Repositories	Data Protection	Facilitate access, rectification, and erasure	Response Timeliness KPI	Mandatory	DPO	6 Years
F-04	Personal Data Breach Notification Form	All Digital & Physical Systems	Data Protection / Security	Log and escalate personal data breaches	Breach Logging Timeliness	Mandatory (If Breach)	DPO	6 Years
F-05	Information Security Incident Report	Core Systems, Cloud, Website, ERP	Information Security	Record security incidents	System Uptime; Incident Rate	Mandatory	ICT Director	6 Years
F-06	Access Control Authorisation Form	Core Systems & Cloud Infrastructure	Information Security	Approve and review system access	Access Review Compliance	Mandatory	ICT Director	6 Years
F-07	Records Disposal Authorisation Form	Physical Archives & Digital Repositories	Records Management	Authorise lawful record disposal	Retention Compliance ≥95%	Mandatory	Registrar	Permanent Disposal Log
F-08	AI Risk Assessment Template	AI Systems	AI Governance	Assess AI risk & fairness	AI Register Coverage (100%)	Mandatory (AI Use)	IGC	Permanent
F-09	AI Systems Register	AI Tools & Automated Systems	AI Governance	Maintain inventory of AI deployments	AI Register Coverage	Mandatory	IGC	Permanent

F-10	Vendor Risk Assessment Template	Third-Party Vendors	Vendor Governance	Assess vendor compliance risk	Contract Documentation Completeness	Mandatory (Vendor Use)	Legal + ICT	Contract Duration + 6 Years
F-11	Vendor Data Processing Agreement (DPA) Template	Third-Party Data Processors	Vendor Governance	Enforce contractual safeguards	Contract Documentation Completeness	Mandatory	Legal	Contract + 6 Years
F-12	Cross-Border Transfer Assessment Form	Cloud & International Transfers	Vendor Governance	Evaluate transfer adequacy	Vendor Compliance KPI	Conditional	Legal / DPO	6 Years
F-13	Information Asset Domicile Declaration Form	All Units	Governance Oversight	Identify asset location & custodian	Asset Register Completeness (100%)	Mandatory	Unit Heads	Permanent
F-14	Annual Information Risk Assessment Template	All Domiciles	Risk Management	Assess institutional exposure	Annual Risk Review	Mandatory	IGC	7 Years
F-15	Quarterly Governance Review Template	All Domiciles	Governance Oversight	Consolidated KPI & risk reporting	KPI Achievement ≥85%	Mandatory (Quarterly)	IGC	Governance Record
F-16	Regulatory Liaison Log	All Regulatory Interactions	Governance	Record regulator communications	Compliance KPI	Mandatory	DPO	Permanent
F-17	Website Data Capture Declaration	Website & Public Platforms	Digital Governance	Document cookies & online data capture	Processing Register Coverage	Mandatory	ICT / Communications	6 Years
F-18	Incident Escalation Record	All Domiciles	Risk Management	Track corrective action pathway	Incident Closure Rate	Mandatory	University Secretary	6 Years

Special Control Conditions

Instrument	Governance Condition
DPIA	-High-risk processing shall not commence without documented approval.
AI Risk Assessment	-High-risk AI systems require formal IGC approval and BOARD authorisation before deployment.
Breach Notification	-Logged breaches must be reviewed at the next Quarterly Governance Meeting.
Records Disposal	-Requires dual authorisation and legal hold clearance.
Vendor Assessment	-No vendor onboarding without a completed assessment and contract safeguards.
Risk Assessment	-Annual institutional risk review is mandatory and reportable.

4. Template Governance Lifecycle

1. Templates shall carry version numbers.
2. Version history shall be maintained by the IGC Secretariat.
3. Superseded templates shall be archived.
4. Template utilisation shall be reviewed during quarterly governance meetings.
5. Failure to use mandatory templates constitutes a control breach.

Annex V: Domicile–Control–KPI Alignment Matrix

Table 5: Domicile, Control and KPI Matrix

Information Asset Domicile	Primary Risk Exposure	Applicable Control Domain	Mandatory Control Instrument (Annex IV Ref)	Linked KPI (Part III)	Reporting Frequency	Escalation Trigger
Student Information System (SIS)	Personal data breach; unauthorised access; data accuracy errors	Data Protection; Information Security	F-01 Processing Register; F-03 DSAR; F-04 Breach Notification; F-06 Access Authorisation	Processing Register Coverage (100%); Breach Logging Timeliness; Access Review Compliance	Quarterly	Breach not logged within 24 hrs; Access review <95%
Learning Management System (LMS)	Data leakage; grading manipulation; system downtime	Information Security; AI Governance (if automated grading used)	F-06 Access Authorisation; F-05 Incident Report; F-08 AI Risk Assessment (if applicable)	System Uptime ≥95%; AI Register Coverage	Quarterly	Uptime <95%; High-risk AI deployed without approval
ERP / Finance System	Financial fraud, record manipulation, loss of audit trail	Information Security; Records Management	F-06 Access Authorisation; F-07 Disposal Register; F-14 Risk Assessment	Financial Documentation Completeness (100%); Retention Compliance ≥95%	Quarterly	Audit exception; retention breach
HR Information System	Exposure of staff personal data; unlawful processing	Data Protection; Records Management	F-01 Processing Register; F-03 DSAR; F-07 Disposal Authorisation	Processing Register Coverage; Retention Compliance	Quarterly	Failure to log processing; disposal without authorisation
Research Data Repository	Sensitive personal data; cross-border transfer risk	Data Protection; Vendor Governance	F-02 DPIA; F-12 Cross-Border Transfer Assessment; F-10 Vendor Assessment	High-Risk Processing Control; Vendor Compliance KPI	Quarterly	High-risk processing without DPIA
University Website & CMS	Unlawful cookie tracking; reputational risk; cyber intrusion	Digital Governance; Information Security	F-17 Website Data Capture Declaration; F-06 Access Authorisation; F-05 Incident Report	Processing Register Coverage; System Uptime	Quarterly	Non-compliant cookie deployment; public data breach
Email & Collaboration Platforms	Phishing; data exfiltration; misdirected communications	Information Security	F-05 Incident Report; F-06 Access Authorisation	Incident Closure Rate; Access Review Compliance	Quarterly	Critical incident unresolved >30 days
Cloud Storage (AWS/Azure/Google)	Cross-border data risk; vendor dependency	Vendor Governance; Information Security	F-10 Vendor Risk Assessment; F-11 DPA; F-12 Cross-Border Assessment	Contract Documentation Completeness (100%)	Annual + Quarterly Review	Vendor contract lapse; inadequate safeguards
Physical Archives	Unauthorised destruction; retention non-compliance	Records Lifecycle Management	F-07 Records Disposal Authorisation	Retention Compliance ≥95%	Quarterly	Disposal without dual authorisation
AI Systems (Admissions, Analytics, Automation)	Algorithmic bias; unlawful automated decision-making	AI Governance; Data Protection	F-08 AI Risk Assessment; F-09 AI Register	AI Register Coverage (100%)	Quarterly	AI deployed without registration
Vendor-Hosted Platforms (Admissions Portal, Payment Gateway)	Third-party breach; contractual gaps	Vendor Governance	F-10 Vendor Assessment; F-11 DPA; F-04 Breach Form	Contract Documentation Completeness; Breach Logging Timeliness	Quarterly	Vendor onboarded without risk assessment
Backup & Disaster Recovery Systems	Data loss; failure to restore	Information Security	F-14 Risk Assessment; F-05 Incident Report	Backup Test Compliance; System Recovery Time	Annual + Incident-Based	Failed recovery test

Annex VI: Global Framework Alignment Matrix

This Annex demonstrates alignment between the UTAMU Information Governance Statute and internationally recognised data protection, privacy, and information security standards. It provides evidence of institutional maturity beyond minimum statutory compliance.

Table 6: Global Framework Alignment Matrix

Governance Domain	Statute Control Area	GDPR Principle	ISO 27001 / 27701	OECD Privacy Principle	NIST CSF Function
Lawful Processing	Lawful Basis & Consent Controls	Lawfulness, Fairness, Transparency	ISO 27701 Clause 7	Collection Limitation	Identify
Purpose Limitation	Processing Register & Purpose Controls	Purpose Limitation	ISO 27701 7.2	Purpose Specification	Identify
Data Minimisation	Data Collection Controls	Data Minimisation	ISO 27701 7.3	Data Quality	Protect
Accuracy	Data Rectification Mechanism	Accuracy	ISO 27701 7.4	Data Quality	Protect
Storage Limitation	Retention Schedule	Storage Limitation	ISO 27001 A.8.3	Use Limitation	Protect
Integrity & Confidentiality	Information Security Controls	Integrity & Confidentiality	ISO 27001 Annex A	Security Safeguards	Protect
Accountability	Governance Oversight & Reporting	Accountability	ISO 27701 Governance Controls	Accountability	Govern
Data Subject Rights	DSAR Procedure	Articles 12–23 (GDPR)	ISO 27701 7.3	Individual Participation	Respond
Breach Management	Incident Response Protocol	Articles 33–34	ISO 27001 A.16	Security Safeguards	Detect / Respond
Vendor Governance	Third-Party Due Diligence	Processor Obligations	ISO 27001 A.15	Accountability	Govern
Cross-Border Transfers	Transfer Safeguards	Chapter V (GDPR)	ISO 27701 7.5	Use Limitation	Govern
Risk Management	Risk Register & Annual Review	Risk-Based Approach	ISO 27001 Clause 6	Accountability	Identify
AI Governance	Automated Processing Oversight	Article 22 (GDPR)	ISO 27701 Extension	Transparency	Govern

Sources: GDPR (EU General Data Protection Regulation) – global benchmark for privacy, ISO/IEC 27001 – Information Security Management, ISO/IEC 27701 – Privacy Information Management, OECD Privacy Guidelines, NIST Cybersecurity Framework (CSF)