CONSTITUTION

ICT Innovation Lab

Department of Information and Communication Technology
Faculty of Engineering and Technology
Islamic University, Kushtia-7003, Bangladesh

Version: 1.0
Adopted on: 18 September 2026
Custodian: Coordinator, ICT Innovation Lab
Review cycle: Annual

A governance framework for responsible innovation, collaborative research, practical skill development, and ethical use of laboratory resources.

Document Status and Interpretation

This Constitution establishes the governance and operating rules of the ICT Innovation Lab (the "Lab"). It becomes effective after approval by the competent authority of Department of Information and Communication Technology and Islamic University, Kushtia-7003, Bangladesh. Where any provision conflicts with an institutional policy, law, regulation, ethics requirement, or safety rule, the higher authority shall prevail and the remaining provisions shall continue in force.

In this document, "shall" indicates a mandatory requirement; "may" grants discretion; "Coordinator" means the faculty member formally appointed to lead the Lab; and "member" includes student, faculty, staff, and approved external members unless a provision states otherwise.

Contents

Document Status and Interpretation i

1 Name, Status, Vision, and Mission 1
- 1.1 Name and institutional status . . . 1
- 1.2 Vision . . . 1
- 1.3 Mission . . . 1

2 Objectives and Scope 1
- 2.1 Core objectives . . . 1
- 2.2 Technical sections . . . 1

3 Governance and Chain of Command 2
- 3.1 Governance bodies . . . 2
- 3.2 Order of authority . . . 2
- 3.3 Institutional Authority . . . 3
- 3.4 Faculty Advisory Committee . . . 3
- 3.5 Lab Coordinator . . . 3
- 3.6 Student Executive Committee . . . 3
- 3.7 Role accountability . . . 3

4 Membership and Admission 4
- 4.1 Membership categories . . . 4
- 4.2 Eligibility . . . 4
- 4.3 Application through a project or research proposal . . . 4
- 4.4 Review and decision . . . 4
- 4.5 Induction and activation . . . 5
- 4.6 Continuation, inactivity, and exit . . . 5

5 Project Governance and Progress Review 5
- 5.1 Project registration . . . 5
- 5.2 Project Lead duties . . . 5
- 5.3 Weekly progress reporting and presentation . . . 5
- 5.4 Removal for consecutive progress-report absence . . . 6
- 5.5 Milestone review . . . 6
- 5.6 Completion and closure . . . 6

6 Meetings, Attendance, and Communication 6
- 6.1 Regular meetings . . . 6

6.2 Notice, quorum, and decisions . . . 6
6.3 Attendance . . . 6
6.4 Minutes and official communication . . . 7

7 Time, Access, and Workspace Management 7
7.1 Opening hours and access . . . 7
7.2 Booking and fair use . . . 7
7.3 Clean-desk and end-of-session rules . . . 7
7.4 Storage and labeling . . . 7

8 Resource, Equipment, and Financial Management 7
8.1 Inventory control . . . 7
8.2 Equipment checkout . . . 8
8.3 Consumables and procurement . . . 8
8.4 Software, cloud services, and accounts . . . 8
8.5 Financial transparency . . . 8
8.6 Monthly membership fee . . . 8
8.7 GPU time application and scheduling . . . 8

9 Safety, Security, and Incident Response 8
9.1 General safety . . . 8
9.2 Emergency action . . . 9
9.3 Incident and near-miss reporting . . . 9
9.4 Stop-work authority . . . 9

10 Responsible Use of Technology 9
10.1 Acceptable use . . . 9
10.2 AI and machine learning . . . 9
10.3 IoT and embedded systems . . . 9
10.4 Web technologies . . . 9
10.5 Cybersecurity research . . . 9

11 Data, Privacy, Records, and Confidentiality 10
11.1 Data governance . . . 10
11.2 Human participants and sensitive data . . . 10
11.3 Access control and credentials . . . 10
11.4 Official records . . . 10
11.5 Confidentiality . . . 10

12 Research Integrity, Authorship, and Intellectual Property 10
12.1 Research integrity . . . 10
12.2 Authorship and acknowledgment . . . 10
12.3 Intellectual property . . . 11
12.4 Open-source and third-party materials . . . 11
12.5 Conflicts of interest . . . 11

13 Conduct, Inclusion, and Professional Standards 11

14 Events, Visitors, Partnerships, and Public Communication 11
14.1 Events and visitors . . . 11
14.2 External partnerships and sponsorship . . . 11
14.3 Media, branding, and public statements . . . 12

15 Performance, Recognition, and Capacity Building **12**

16 Discipline, Complaints, and Appeals **12**
16.1 Principles 12
16.2 Possible measures 12
16.3 Complaints 12
16.4 Appeals 12

17 Continuity, Audit, and Annual Planning **13**

18 Amendment, Review, and Dissolution **13**
18.1 Amendment 13
18.2 Periodic review 13
18.3 Dissolution or suspension 13

19 Adoption and Signatures **13**

A Membership and Project Proposal Application **15**

B Weekly Project Progress Report **16**

C Equipment Checkout and Return Record **17**

D Incident and Near-Miss Report **18**

E Project Closure and Handover Checklist **19**

Article 1 Name, Status, Vision, and Mission

1.1 Name and institutional status

The organization shall be known as the **ICT Innovation Lab**. It shall operate as an innovation facility under Department of Information and Communication Technology and Islamic University, Kushtia-7003, Bangladesh and its designated department or administrative unit. The Lab is non-partisan, non-discriminatory, not-for-profit, and dedicated to education, research, innovation, and responsible technology development.

1.2 Vision

To become a collaborative center of excellence where students, faculty, and partners transform ideas into ethical, useful, and research-driven ICT solutions.

1.3 Mission

The Lab shall:

a) Support high-quality research, experimentation, prototyping, and product development;

b) Develop practical competence through mentoring, peer learning, and interdisciplinary teamwork;

c) Promote responsible innovation, research integrity, privacy, security, accessibility, and social benefit;

d) Connect academic learning with community, industry, and institutional needs; and

e) Preserve shared equipment, data, software, knowledge, and working space for future members.

Article 2 Objectives and Scope

2.1 Core objectives

The objectives of the Lab are to:

1. Incubate approved student and faculty projects and research;
2. Provide a structured environment for experimentation and collaboration;
3. Facilitate publications, competitions, demonstrations, patents, open-source contributions, and responsible technology transfer;
4. Arrange seminars, workshops, training, hackathons, exhibitions, and outreach activities;
5. Create reusable documentation, datasets, code, designs, and prototypes; and
6. Evaluate members through measurable progress, conduct, contribution, and stewardship.

2.2 Technical sections

The initial sections of the Lab shall be:

a) Artificial Intelligence and Machine Learning (AI/ML);

b) Internet of Things (IoT) and Embedded Systems;

c) Web Technologies and Software Engineering; and

d) Cybersecurity and Digital Forensics.

The Coordinator may establish, merge, rename, suspend, or retire sections after consulting the Faculty Advisory Committee and recording the decision. Projects may belong to more than one section, but one section shall be designated as the lead section for reporting and resource allocation.

Article 3 Governance and Chain of Command

3.1 Governance bodies

The governance structure shall consist of:

1. the Institutional Authority;
2. the Faculty Advisory Committee;
3. the Lab Coordinator;
4. the Deputy or Assistant Coordinator, if appointed;
5. Section Mentors or Faculty Advisers;
6. the Student Executive Committee;
7. Section Leads and Project Leads; and
8. general members.

3.2 Order of authority

For operational matters, the chain of command shall ordinarily be:



Members shall first raise routine matters with their Project Lead or Section Lead. Matters involving safety, harassment, research misconduct, security incidents, conflicts of interest, or urgent

institutional risk may be reported directly to the Coordinator or the appropriate institutional office without following intermediate steps.

3.3 Institutional Authority

The Institutional Authority shall approve the Constitution, appoint or confirm the Coordinator as required by institutional rules, provide oversight, and hear appeals or matters beyond the Lab's authority.

3.4 Faculty Advisory Committee

The Faculty Advisory Committee should include the Coordinator and at least two other faculty members where practicable. It shall advise on strategy, ethics, funding, safety, partnerships, high-risk projects, disciplinary appeals, and annual performance. It shall meet at least once per academic term.

3.5 Lab Coordinator

The Coordinator is the chief academic and administrative officer of the Lab and shall:

a) approve, conditionally approve, return for revision, or reject membership and project applications;

b) appoint mentors, student officers, section leads, and project leads, with consultation where appropriate;

c) authorize access levels, budgets, purchases, external collaboration, events, and use of sensitive resources;

d) convene meetings and evaluate project progress;

e) maintain or delegate maintenance of official records, inventories, schedules, and reports;

f) suspend activities presenting safety, legal, ethical, financial, or cybersecurity risks; and

g) submit an annual Lab report to the competent authority.

The Coordinator may delegate duties but retains supervisory responsibility.

3.6 Student Executive Committee

Subject to appointment or confirmation by the Coordinator, the Committee may include a President or Convener, Secretary, Operations and Resource Officer, Finance Officer, Communications and Events Officer, and Section Leads. Its term shall ordinarily be one academic year. It shall implement approved plans, maintain records, coordinate schedules, and support members. It may not approve membership, commit institutional funds, sign external agreements, or overrule the Coordinator.

3.7 Role accountability

Every office-holder shall maintain a handover record. An officer may be removed for inactivity, misconduct, conflict of interest, loss of eligibility, or failure to perform assigned duties, after notice and an opportunity to respond.

Article 4 Membership and Admission

4.1 Membership categories

Membership may include:

a) **Faculty Members and Mentors**, who provide academic and technical supervision;

b) **Student Researchers or Developers**, admitted through an approved proposal;

c) **Associate Members**, admitted for training or limited contribution without independent resource privileges;

d) **Alumni Members**, who may mentor or collaborate with approval; and

e) **External Collaborators**, admitted under a written scope, confidentiality, access, and supervision arrangement.

4.2 Eligibility

An applicant shall demonstrate genuine interest, sufficient time, willingness to follow Lab rules, and the competence or learning plan necessary for the proposed work. Admission shall not be denied on grounds prohibited by applicable law or institutional policy.

4.3 Application through a project or research proposal

Admission shall normally require a written project or research proposal submitted to the Coordinator. The proposal shall contain, at minimum:

a) applicant identity, academic affiliation, contact information, and relevant skills;

b) project title, lead section, team members, and intended mentor;

c) problem statement, motivation, objectives, and expected contribution;

d) brief review of relevant work or comparable solutions;

e) methodology, technical architecture, datasets, tools, and work plan;

f) milestones, expected outputs, timeline, and success criteria;

g) required hardware, software, workspace, budget, and external support;

h) foreseeable safety, ethical, legal, privacy, security, environmental, and intellectual-property issues; and

i) dissemination, documentation, maintenance, and project-closure plans.

4.4 Review and decision

The Coordinator may consult relevant mentors or reviewers. Proposals shall be assessed on feasibility, originality or value, academic merit, ethics, risk, resource availability, applicant capacity, and alignment with Lab objectives. The decision shall be one of: approved, conditionally approved, revision required, deferred, or rejected. Reasons should be recorded. Approval may carry conditions, milestones, probation, access restrictions, or training requirements. Approval of

membership does not automatically approve funding, publication, human-subject research, use of personal data, security testing, or external deployment.

4.5 Induction and activation

Before receiving active access, an accepted applicant shall:

a) sign the membership and rules acknowledgment;

b) complete safety, ethics, information-security, and equipment induction appropriate to the project;

c) receive an assigned section, mentor or supervisor, project identifier, access level, and initial review date; and

d) understand emergency contacts, booking procedures, and incident reporting.

New members may serve a probationary period of four to eight weeks, as specified in the approval decision.

4.6 Continuation, inactivity, and exit

Membership shall be reviewed at least once per academic term. A member who is inactive for four consecutive weeks without approved leave, repeatedly misses required meetings, or shows insufficient proposal progress may be placed on probation or have membership suspended. On exit, every member shall return Lab property, settle records, transfer credentials through approved procedures, archive project materials, remove personal belongings, and complete a handover. Confidentiality, attribution, data protection, and intellectual-property duties survive departure.

Article 5 Project Governance and Progress Review

5.1 Project registration

Each approved project shall have a project code, Project Lead, supervisor or mentor, approved scope, milestone schedule, member list, resource allocation, risk classification, and designated repository or documentation location. Material changes to objectives, data, methods, team, budget, external access, or deployment require prior approval.

5.2 Project Lead duties

The Project Lead shall organize work, assign tasks fairly, maintain the project plan and risk register, protect credentials and data, document decisions, report progress honestly, and ensure that outputs can be reproduced or transferred.

5.3 Weekly progress reporting and presentation

Every active project shall submit a concise weekly progress report and present progress at the scheduled Lab or section meeting unless excused. The report shall state:

a) work planned and work completed;

b) evidence such as commits, experiments, designs, test results, literature notes, or prototypes;

c) obstacles, risks, resource needs, and decisions requested;

d) contributions of each team member; and

e) tasks and measurable targets for the next week.

Reports shall be retained in the approved project record. Fabricated, copied, or misleading progress evidence constitutes misconduct.

5.4 Removal for consecutive progress-report absence

A member who, without approved leave or a reason accepted by the Coordinator, is absent from two consecutive scheduled progress-report sessions shall be subject to removal from the Lab. Before removal, the member shall receive notice of the recorded absences and a reasonable opportunity to provide an explanation. The Coordinator shall record and communicate the final decision.

5.5 Milestone review

At each milestone, the Coordinator or delegate may decide to continue, revise, pause, merge, transfer, or close a project. Projects showing repeated lack of progress may lose priority access to resources. Paused projects shall have a recorded reason, review date, and preservation plan.

5.6 Completion and closure

A project is complete only after submission of agreed outputs, technical and user documentation, source files where applicable, test or evaluation results, inventory reconciliation, data disposition, financial reconciliation, and a final presentation or demonstration. The Coordinator shall record whether the project is completed, archived, transferred, continued, or discontinued.

Article 6 Meetings, Attendance, and Communication

6.1 Regular meetings

The Lab shall hold a general meeting at least once each week during active academic periods. Sections may hold additional technical meetings. The regular meeting should include attendance, notices, safety or resource issues, short project presentations, decisions, action items, responsible persons, and deadlines.

6.2 Notice, quorum, and decisions

Routine meeting notice should be given at least 24 hours in advance. For a formal general meeting, quorum shall be one-half of active voting members, including the Coordinator or an authorized faculty delegate. Decisions should be reached by consensus; where a vote is required, a simple majority of members present and voting shall decide. The chair has a casting vote in a tie. Changes to this Constitution follow Article 18, not this ordinary voting rule.

6.3 Attendance

Members shall attend required meetings punctually. Absence should be reported in advance with a reason. Three unexcused absences in a rolling eight-week period may trigger a membership review. Attendance shall be evaluated with reasonable accommodation for academic, health, religious, family, accessibility, and other legitimate circumstances.

6.4 Minutes and official communication

The Secretary or assigned recorder shall issue minutes within three working days. Minutes shall record decisions and actions, not unnecessary sensitive discussion. Official notices shall be sent through channels approved by the Coordinator. Members are responsible for checking those channels and responding within stated deadlines.

Article 7 Time, Access, and Workspace Management

7.1 Opening hours and access

Lab hours shall be published each term. Access outside normal hours requires written approval and compliance with institutional security rules. Members shall not lend access cards, keys, accounts, or entry credentials. Visitors shall sign in and remain with an authorized host unless other arrangements are approved.

7.2 Booking and fair use

Workstations, benches, rooms, testing environments, and equipment shall be reserved using the approved booking system. Priority shall ordinarily be:

1. Safety-critical or deadline-bound approved research;
2. Scheduled teaching, demonstrations, and approved events;
3. Active projects meeting milestones; and
4. Training and exploratory use.

Unused bookings should be released promptly. Repeated no-shows may lead to temporary booking restrictions.

7.3 Clean-desk and end-of-session rules

At the end of every session, users shall save and back up work appropriately, log out, shut down equipment when required, return tools, label permitted work-in-progress, remove waste, clear common surfaces, arrange chairs, and report faults. Food and drink are prohibited near electronics, tools, chemicals, batteries, or designated clean areas. Personal belongings shall not obstruct walkways or occupy shared storage without permission.

7.4 Storage and labeling

All stored items shall show the project code, owner, contact, date stored, contents or hazard, and review or removal date. Unlabeled, unsafe, abandoned, or expired items may be quarantined and, after reasonable notice, disposed of under institutional procedure.

Article 8 Resource, Equipment, and Financial Management

8.1 Inventory control

All Lab assets shall be recorded with an asset or inventory identifier, description, location, custodian, condition, acquisition source, and loan history where applicable. No member may remove, relocate, alter, disassemble, repair, or dispose of an asset without authorization.

8.2 Equipment checkout

Borrowing requires an approved checkout record. The borrower is responsible for reasonable care, approved use, timely return, and immediate reporting of loss, damage, or malfunction. Equipment shall not be loaned to another person without updating the official record. Liability shall be determined under institutional policy after considering normal wear, training, supervision, and circumstances.

8.3 Consumables and procurement

Consumables shall be issued against an approved project or activity. Purchase requests shall state purpose, specification, quantity, estimated cost, funding source, alternatives considered, and responsible custodian. Only authorized officials may commit funds or place orders. Splitting purchases to avoid approval thresholds is prohibited.

8.4 Software, cloud services, and accounts

Only lawfully licensed or properly authorized software, datasets, platforms, cloud services, APIs, and accounts may be used. Shared administrative credentials shall be avoided; where unavoidable, they shall be stored in an approved secret management system. Personal payment methods and unapproved cloud subscriptions shall not create obligations for the Lab.

8.5 Financial transparency

Income, sponsorship, grants, registration fees, reimbursements, and expenditure shall follow institutional financial rules. The Finance Officer or designated administrator shall maintain supporting records. No Lab officer or member may personally receive funds on behalf of the Lab unless formally authorized.

8.6 Monthly membership fee

Each active member shall pay a monthly membership fee of BDT 100 (one hundred Bangladeshi taka) no later than the seventh day of each month. Payment shall be made through the collection method authorized by the Lab, and the Finance Officer or designated administrator shall maintain an official payment record.

8.7 GPU time application and scheduling

Any member who needs to use a Lab GPU shall first submit a request through the approved application or booking process, stating the project, purpose, required resources, and estimated duration. GPU time shall be assigned according to the approved schedule and resource availability. The applicant shall be notified of the allocated time and may use the GPU only during that designated period, unless a schedule change is approved. Unused time should be released promptly so that it may be reassigned.

Article 9 Safety, Security, and Incident Response

9.1 General safety

Members shall follow posted safety instructions, use required protective equipment, maintain clear exits, and operate tools only after training. Work involving mains electricity, soldering, batteries, heat, moving machinery, radio transmitters, lasers, chemicals, or other hazards requires suitable supervision and risk controls. Working alone on designated high-risk activities is prohibited.

9.2 Emergency action

In an emergency, persons shall prioritize life safety, stop work if safe, warn others, contact institutional emergency services, evacuate or isolate the area as directed, and inform the Coordinator. Members shall not conceal an incident or disturb evidence except to prevent harm.

9.3 Incident and near-miss reporting

Injury, equipment damage, loss, theft, data exposure, cybersecurity incidents, policy breaches, and near misses shall be reported promptly. The Coordinator shall ensure containment, documentation, notification, investigation, corrective action, and lessons learned, while protecting confidentiality and due process. Good-faith reporting shall not result in retaliation.

9.4 Stop-work authority

Any member may stop an activity that reasonably appears to present imminent danger or serious legal, ethical, security, or environmental risk. Work may resume only after review and authorization by the competent person.

Article 10 Responsible Use of Technology

10.1 Acceptable use

Lab resources shall be used only for approved academic, research, training, administrative, or community purposes. Prohibited conduct includes unauthorized commercial use, cryptocurrency mining, harassment, surveillance, bypassing controls, illegal content, academic dishonesty, and activity that threatens the institution or third parties.

10.2 AI and machine learning

AI/ML projects shall document data provenance, consent or lawful basis, preprocessing, limitations, evaluation methods, bias and fairness risks, model versions, and human oversight. High-impact or sensitive applications require enhanced review. Members shall disclose material use of generative AI in work products when required by academic, publication, competition, or institutional rules, and shall verify outputs rather than present them as automatically true.

10.3 IoT and embedded systems

IoT work shall address electrical and physical safety, radio-frequency rules, device identity, secure configuration, firmware update, credential protection, network segmentation, data minimization, and end-of-life disposal. Devices shall not be connected to institutional networks without required approval.

10.4 Web technologies

Web systems shall follow secure development practices, access control, input validation, dependency management, logging, backup, accessibility, privacy, and deployment approval requirements. Public release shall not occur until ownership, security, data, branding, and maintenance responsibilities are resolved.

10.5 Cybersecurity research

Cybersecurity testing shall be performed only on systems, accounts, networks, devices, and data for which explicit written authorization defines scope, time, method, contacts, and reporting.

Unauthorized scanning, exploitation, credential testing, interception, persistence, malware deployment, social engineering, or data access is prohibited. Tools and findings that could enable harm shall be secured and disclosed responsibly through approved channels.

Article 11 Data, Privacy, Records, and Confidentiality

11.1 Data governance

Projects shall collect and retain only data necessary for approved objectives. Before collection or access, the project shall identify ownership, lawful basis or consent, sensitivity, storage location, access list, retention period, sharing conditions, backup, anonymization or pseudonymization, and secure destruction method.

11.2 Human participants and sensitive data

Research involving human participants, personal data, health data, minors, biometrics, confidential institutional information, or other sensitive material shall not begin until all required ethics and administrative approvals are obtained. Lab approval alone is not ethics approval.

11.3 Access control and credentials

Access shall follow least privilege and be reviewed when roles change. Members shall use strong authentication, protect credentials, apply security updates, encrypt sensitive data where appropriate, and never place secrets in public or unapproved repositories. Access shall be revoked promptly when no longer needed.

11.4 Official records

Official records may include applications, approvals, membership registers, minutes, inventories, checkouts, budgets, project reports, risk assessments, incident records, training records, and publication or intellectual-property records. Records shall be accurate, access-controlled, retained, and disposed of according to institutional policy.

11.5 Confidentiality

Members shall not disclose confidential information except for an approved purpose or where disclosure is required by law or institutional policy. Confidentiality shall not be used to suppress good-faith reports of misconduct, safety issues, or legal violations to an authorized body.

Article 12 Research Integrity, Authorship, and Intellectual Property

12.1 Research integrity

Members shall follow honest and reproducible research practices. Fabrication, falsification, plagiarism, deceptive manipulation, undisclosed conflicts, misrepresentation of contribution, and destruction or concealment of required records are prohibited. Errors shall be corrected transparently.

12.2 Authorship and acknowledgment

Authorship shall reflect substantial intellectual contribution and accountability, consistent with applicable disciplinary and publication standards. Routine access, position, funding, or super-

vision alone does not guarantee authorship. Contributors, the Lab, funding sources, datasets, software, and facilities shall be acknowledged as appropriate.

12.3 Intellectual property

Ownership of inventions, software, designs, datasets, documentation, media, and other outputs shall be determined by applicable law, institutional policy, funding terms, and written collaboration agreements. Before external release, commercialization, patent filing, licensing, or competition submission, the Project Lead shall obtain required approvals and document contributor rights.

12.4 Open-source and third-party materials

Members shall comply with software, content, dataset, and hardware licenses. Open-source release requires approval of ownership, confidentiality, security, license compatibility, attribution, and maintenance plans.

12.5 Conflicts of interest

Members shall disclose financial, personal, academic, supervisory, or external interests that could influence a decision. The Coordinator shall record an appropriate mitigation, which may include recusal or independent review.

Article 13 Conduct, Inclusion, and Professional Standards

Every member shall behave respectfully, professionally, and collaboratively. Harassment, discrimination, bullying, hazing, intimidation, retaliation, violence, deliberate exclusion, sabotage, theft, and misuse of authority are prohibited. Members shall respect accessibility needs, cultural and religious diversity, academic commitments, and reasonable differences of opinion.

Technical criticism shall address the work rather than the person. Team members shall receive clear responsibilities, fair access to learning and recognition, and timely feedback. Romantic, financial, or close personal relationships that create supervisory conflicts shall be disclosed and managed according to institutional policy.

Article 14 Events, Visitors, Partnerships, and Public Communication

14.1 Events and visitors

Events require an approved purpose, organizer, schedule, space plan, budget, safety assessment, participant rules, and post-event restoration plan. Visitors shall receive appropriate safety and confidentiality instructions. Minors shall be supervised in accordance with institutional safeguarding rules.

14.2 External partnerships and sponsorship

No member may represent that the Lab or institution has entered a partnership, accepted sponsorship, endorsed a product, or assumed an obligation without written authorization. Agreements shall address scope, funding, deliverables, data, confidentiality, publication, intellectual property, branding, liability, security, and termination.

14.3 Media, branding, and public statements

Use of the institution's or Lab's name, logo, photographs, facilities, or public channels shall follow approval and branding rules. Members shall not disclose confidential work or speak on behalf of the Lab unless authorized. Demonstrations and claims shall accurately describe capabilities, limitations, contributors, and development status.

Article 15 Performance, Recognition, and Capacity Building

Member performance may be assessed using proposal progress, quality of work, meeting participation, documentation, teamwork, responsible resource use, training completed, mentoring, and contribution to Lab activities. Evaluation shall be fair, evidence-based, and appropriate to the member's role and available time.

The Lab may recognize achievement through certificates, recommendations, showcases, leadership opportunities, travel or competition support, and priority for advanced projects, subject to institutional rules and available resources. Recognition shall not override authorship or intellectual-property standards.

Each section should maintain a learning pathway including induction, foundational skills, supervised practice, independent project work, peer mentoring, and advanced responsibility.

Article 16 Discipline, Complaints, and Appeals

16.1 Principles

Disciplinary action shall be proportionate, documented, timely, impartial, and consistent with institutional policy. The person concerned shall be informed of the concern and given a reasonable opportunity to respond, except where immediate temporary action is necessary to protect people, systems, evidence, or property.

16.2 Possible measures

Depending on seriousness and history, measures may include coaching, verbal or written warning, retraining, corrective action, restitution under institutional rules, restriction of access, removal from a project or office, probation, suspension, termination of membership, or referral to the competent authority. Serious matters may bypass progressive measures.

16.3 Complaints

Complaints may be submitted to the Coordinator or the appropriate institutional office. A complaint involving the Coordinator shall be referred directly to the Faculty Advisory Committee or Institutional Authority. Confidentiality shall be maintained to the extent compatible with fair review and safety.

16.4 Appeals

A person affected by a final Lab-level disciplinary or membership decision may submit a written appeal within ten working days, stating the decision challenged, grounds, and supporting information. Appeals shall be handled by an authority not materially involved in the original decision. Institutional appeal rules shall prevail.

Article 17 Continuity, Audit, and Annual Planning

The Lab shall maintain an annual operating plan covering projects, training, events, budget, procurement, maintenance, risk, partnerships, and performance indicators. At least annually, the Coordinator shall arrange a review of:

a) membership and access permissions;

b) inventory, equipment condition, licenses, and account ownership;

c) active, paused, and archived projects;

d) finances, sponsorship, and outstanding commitments;

e) safety, security, privacy, ethics, and incident trends;

f) publications, competitions, prototypes, community impact, and learning outcomes; and

g) constitutional and procedural improvements.

Critical administrative credentials, records, repositories, and inventories shall not depend on a single student or personal account. Outgoing officers shall complete a documented handover before the end of their term.

Article 18 Amendment, Review, and Dissolution

18.1 Amendment

An amendment may be proposed by the Coordinator, the Faculty Advisory Committee, the Student Executive Committee, or at least one-third of active members. The text and rationale shall be circulated at least seven calendar days before consideration. Adoption requires approval by two-thirds of members present and voting at a quorate meeting, endorsement by the Coordinator, and final approval by the competent Institutional Authority. Administrative schedules and forms may be updated by the Coordinator provided they do not contradict this Constitution.

18.2 Periodic review

This Constitution shall be reviewed annually and comprehensively at least once every three years, or earlier when required by legal, institutional, technical, or operational change.

18.3 Dissolution or suspension

The Lab may be dissolved or suspended only by the competent Institutional Authority. On dissolution or extended suspension, assets, records, funds, data, credentials, active obligations, and project materials shall be transferred or disposed of under institutional policy. No member has an individual claim over Lab assets merely by reason of membership or contribution.

Article 19 Adoption and Signatures

This Constitution was adopted on 18 September 2026 and takes effect upon final institutional approval. The signatories confirm that the document has been reviewed and that implementation responsibilities have been assigned.

[Coordinator's Name]
Coordinator, ICT Innovation Lab
Date: _____

[Name of Head / Approving Authority]
[Title]
Date: _____

[Faculty Advisory Representative]
Faculty Advisory Committee
Date: _____

[Student Representative]
Student Executive Committee
Date: _____

Appendix A Membership and Project Proposal Application

Applicant name	
Student / employee ID	
Department and program	
Email and telephone	
Project title and code	
Lead section	☐ AI/ML ☐ IoT ☐ Web ☐ Cybersecurity ☐ Other
Proposed mentor	
Team members	
Requested start and end dates	

Proposal content

Attach a proposal addressing the problem, objectives, relevant work, methodology, tools and data, milestones, deliverables, evaluation, resources, budget, risks, ethics, privacy, security, intellectual property, dissemination, maintenance, and closure plan.

Applicant declaration

I certify that the information is accurate. If admitted, I agree to follow this Constitution, institutional rules, approval conditions, and lawful instructions; to use resources responsibly; and to report incidents and material project changes promptly.

Applicant signature: _____ Date: _____

Review decision

☐ Approved ☐ Conditionally approved ☐ Revision required ☐ Deferred ☐ Rejected

Conditions / reasons:

Access level: _____ First review date: _____

Coordinator signature: _____ Date: _____

Appendix B Weekly Project Progress Report

Project title and code

Week ending

Project Lead

Team members reporting

Overall status ☐ On track ☐ At risk ☐ Delayed ☐ Blocked

Planned work

Completed work and evidence

Experiments / tests / results

Problems and risks

Resources or decisions needed

Individual contributions

Next-week targets

Presenter: _____ Reviewer: _____ Date: _____

Appendix C Equipment Checkout and Return Record

Borrower and ID	
Project title and code	
Asset ID and description	
Accessories / quantity	
Condition at issue	
Purpose and location of use	
Checkout date and time	
Due date and time	
Approved by	

I accept responsibility for reasonable care, approved use, timely return, and prompt reporting of loss, damage, malfunction, or incident.

Borrower signature: _____ Date: _____

Return: Condition and discrepancies:

Returned on: _____ Received by: _____

Appendix D Incident and Near-Miss Report

Reporter and contact	
Date, time, and location	
Incident type	☐ Injury ☐ Equipment ☐ Data / cyber ☐ Loss / theft ☐ Near miss ☐ Other
People / systems affected	
Immediate action taken	

Description of what happened:

Known or suspected causes:

Recommended corrective action:

Escalated to: _____ Date / time: _____

Review outcome and follow-up owner:

Appendix E Project Closure and Handover Checklist

Project title and code	
Project Lead and mentor	
Closure date and status	☐ Completed ☐ Transferred ☐ Archived ☐ Discontinued

	Required item	Verified by / date
☐	Final report, results, and presentation submitted	
☐	Source code, designs, configurations, and build instructions archived	
☐	Data, consent, retention, sharing, and deletion obligations resolved	
☐	Security findings, credentials, keys, and access transferred or revoked	
☐	Hardware, tools, assets, and consumables reconciled	
☐	Financial records, licenses, subscriptions, and commitments reconciled	
☐	Authorship, acknowledgments, intellectual property, and release status recorded	
☐	Maintenance owner, known issues, and next steps documented	
☐	Workspace and storage cleared or relabeled	

Project Lead: _____ Mentor: _____

Coordinator approval: _____ Date: _____