INITIATIVE FOR LEGAL AID

(ILA)

INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) POLICY

Version: 1.0

Effective Date: _____

Approved by: Board of Directors

Policy Owner: Executive Director

Responsible Department: Administration and ICT

Review Date: Every two (2) years or as required.

TABLE OF CONTENTS

CHAPTER TEN: BUSINESS CONTINUITY AND DISASTER RECOVERY
10.1 Business Continuity
10.2 Backup Policy
10.3 Recovery Objectives
10.4 Disaster Recovery Procedures
10.5 Recovery Testing
10.6 Emergency Communications

CHAPTER ELEVEN: SOFTWARE MANAGEMENT
11.1 Software Procurement
11.2 Licensing
11.3 Installation
11.4 Updates
11.5 Unauthorized Software
11.6 Open-Source Software

CHAPTER TWELVE: MOBILE DEVICES AND REMOTE WORKING
12.1 Mobile Devices
12.2 Bring Your Own Device (BYOD)
12.3 Remote Working
12.4 Virtual Private Networks (VPNs)
12.5 Device Security

CHAPTER THIRTEEN: WEBSITE, EMAIL AND DIGITAL COMMUNICATIONS
13.1 Website Management
13.2 Official Email
13.3 Domain Management
13.4 Digital Branding
13.5 Electronic Records
13.6 Online Meetings

CHAPTER FOURTEEN: ICT PROCUREMENT AND VENDOR MANAGEMENT
14.1 ICT Procurement Principles
14.2 Vendor Selection
14.3 Service Agreements
14.4 Maintenance Contracts
14.5 Warranty Management

CHAPTER FIFTEEN: ICT INCIDENT MANAGEMENT
15.1 Incident Reporting
15.2 Investigation
15.3 Incident Classification
15.4 Corrective Actions
15.5 Lessons Learned

CHAPTER SIXTEEN: MONITORING, COMPLIANCE AND AUDIT

16.1 Compliance Monitoring
16.2 ICT Audits
16.3 Policy Violations
16.4 Corrective Measures
16.5 Continuous Improvement

CHAPTER SEVENTEEN: POLICY IMPLEMENTATION

17.1 Responsibilities
17.2 Training
17.3 Awareness
17.4 Exceptions
17.5 Review
17.6 Approval
17.7 Effective Date

ANNEXES

- Annex I: ICT Asset Register
- Annex II: ICT Asset Handover Form
- Annex III: ICT Asset Return Form
- Annex IV: ICT User Access Request Form
- Annex V: ICT User Account Closure Checklist
- Annex VI: Password Standards
- Annex VII: Information Classification Matrix
- Annex VIII: ICT Incident Report Form
- Annex IX: ICT Maintenance Log
- Annex X: Backup Register
- Annex XI: ICT Asset Disposal Form
- Annex XII: ICT Acceptable Use Agreement
- Annex XIII: ICT Risk Assessment Template
- Annex XIV: Cybersecurity Incident Response Flowchart
- Annex XV: ICT Equipment Inspection Checklist

CHAPTER ONE

INTRODUCTION

1.1 Background

The Initiative for Legal Aid (ILA) recognizes Information and Communication Technology (ICT) as a strategic enabler for the effective delivery of legal aid services, institutional governance, programme implementation, knowledge management, communication, and organizational accountability. ICT systems support virtually every aspect of the organization's operations, including legal case management, programme administration, financial management, human resource management, monitoring, evaluation, accountability and learning (MEAL), procurement, safeguarding, advocacy, research, and stakeholder engagement.

As a non-profit organization operating in a dynamic legal, humanitarian, and development environment, ILA increasingly relies on digital technologies to enhance efficiency, improve service delivery, protect confidential information, facilitate collaboration, and ensure compliance with legal and donor obligations. The organization also recognizes that the increased use of technology exposes it to various risks, including cyberattacks, unauthorized access, data breaches, malware infections, identity theft, loss of information, system failures, and misuse of ICT resources.

This Information and Communication Technology (ICT) Policy establishes the governance framework for the acquisition, management, security, acceptable use, maintenance, and disposal of ICT resources throughout the organization. It provides clear standards, responsibilities, and procedures for safeguarding the confidentiality, integrity, and availability of organizational information while promoting responsible and ethical use of ICT assets.

The Policy forms an integral part of ILA's overall governance framework and complements other organizational policies, including the Human Resource and Administration Policy, Finance and Accounting Policy, Procurement and Asset Management Policy, Monitoring, Evaluation, Accountability and Learning (MEAL) Policy, Risk Management Policy, Safeguarding and PSEAH Policy, Code of Conduct and Ethics Policy, Data Protection procedures, and other internal regulations.

1.2 Purpose

The purpose of this Policy is to establish a comprehensive framework for the effective governance, management, security, and responsible use of ICT resources within the Initiative for Legal Aid.

Specifically, the Policy seeks to:

- Establish clear ICT governance structures and accountability mechanisms.

- Promote the secure, efficient, reliable, and cost-effective use of ICT resources.
- Protect organizational information against unauthorized access, disclosure, alteration, destruction, or loss.
- Ensure the confidentiality, integrity, availability, and resilience of information systems.
- Minimize operational, financial, legal, reputational, and cybersecurity risks.
- Provide standards for ICT procurement, maintenance, and lifecycle management.
- Promote compliance with applicable laws, donor requirements, contractual obligations, and international good practices.
- Support digital transformation and innovation within the organization.
- Promote business continuity and disaster recovery preparedness.
- Foster a culture of cybersecurity awareness and responsible digital behaviour among all users.

1.3 Objectives

The objectives of this Policy are to:

1. Establish an effective ICT governance system that supports the strategic objectives of ILA.
2. Ensure all ICT assets are acquired, managed, utilized, maintained, and disposed of in a controlled and accountable manner.
3. Protect confidential organizational, employee, beneficiary, partner, and donor information from unauthorized access or misuse.
4. Promote responsible, ethical, and lawful use of ICT resources by all users.
5. Strengthen cybersecurity resilience against internal and external threats.
6. Establish effective user access management and authentication controls.
7. Ensure the availability and reliability of ICT services through appropriate maintenance, backups, and disaster recovery measures.
8. Promote compliance with contractual obligations, donor standards, and applicable legal requirements.
9. Support digital record management and institutional knowledge preservation.
10. Facilitate efficient communication and collaboration through secure digital platforms.
11. Improve operational efficiency through standardized ICT practices.
12. Promote continuous improvement in ICT governance through monitoring, evaluation, audits, and periodic policy reviews.

1.4 Scope

This Policy applies to all ICT resources owned, leased, managed, or used by the Initiative for Legal Aid.

The Policy applies to:

- Members of the Board of Directors.
- Management.
- Employees.

- Volunteers.
- Interns.
- Consultants.
- Temporary staff.
- Individual contractors.
- Partner organizations where applicable.
- Service providers with access to ILA information systems.
- Any other person authorized to use ILA ICT resources.

The Policy covers all organizational ICT assets, including but not limited to:

- Desktop computers.
- Laptop computers.
- Servers.
- Mobile phones.
- Tablets.
- Printers.
- Photocopiers.
- Network equipment.
- Internet services.
- Email systems.
- Websites.
- Cloud services.
- Software applications.
- Databases.
- Storage devices.
- Audio-visual equipment.
- Digital communication platforms.
- Backup systems.
- Information stored in physical or electronic formats.

The Policy applies regardless of whether ICT resources are accessed from ILA offices, field locations, home offices, remote work environments, or any other authorized location.

1.5 Policy Statement

The Initiative for Legal Aid is committed to ensuring that ICT resources are managed securely, responsibly, efficiently, transparently, and in a manner that supports the achievement of its mission and strategic objectives.

ILA shall maintain appropriate administrative, technical, and physical safeguards to protect information assets against accidental or deliberate loss, damage, theft, misuse, unauthorized access, cyber threats, and operational disruption.

Every user of organizational ICT resources has a duty to protect those resources and to use them solely for legitimate organizational purposes in accordance with this Policy and other applicable organizational regulations.

Failure to comply with this Policy may result in disciplinary action, contractual remedies, legal proceedings, or other corrective measures as appropriate.

CHAPTER TWO

ICT GOVERNANCE FRAMEWORK

2.1 Introduction

Effective Information and Communication Technology (ICT) governance is essential to ensure that technology investments support the strategic objectives of the Initiative for Legal Aid (ILA), safeguard organizational information, enhance operational efficiency, and promote accountability. ICT governance establishes the structures, processes, policies, and decision-making mechanisms through which ICT resources are directed, managed, monitored, and continuously improved.

ILA recognizes ICT as a strategic organizational resource rather than merely an administrative support function. Accordingly, ICT governance shall be integrated into the organization's overall governance framework and shall be implemented in a manner that supports legal aid service delivery, programme implementation, institutional management, donor compliance, financial accountability, and organizational sustainability.

2.2 ICT Governance Objectives

The ICT governance framework aims to:

a. Align ICT initiatives with ILA's Vision, Mission, Strategic Plan, and organizational priorities.

b. Ensure ICT investments deliver value for money and measurable organizational benefits.

c. Protect organizational information and ICT infrastructure against internal and external threats.

d. Establish clear roles, responsibilities, and accountability for ICT decision-making.

e. Promote compliance with applicable laws, contractual obligations, donor requirements, and organizational policies.

f. Support business continuity through reliable ICT systems and disaster recovery measures.

g. Promote innovation, continuous improvement, and responsible adoption of emerging technologies.

h. Ensure efficient utilization and lifecycle management of ICT resources.

i. Enhance transparency in ICT procurement, budgeting, and resource allocation.

j. Promote ethical, lawful, and responsible use of ICT resources.

2.3 ICT Governance Principles

ILA shall govern ICT resources in accordance with the following principles:

2.3.1 Strategic Alignment

ICT investments shall directly support the strategic goals, operational priorities, and programme objectives of the organization.

2.3.2 Accountability

Responsibilities for ICT governance shall be clearly assigned, documented, and communicated.

2.3.3 Transparency

ICT decisions shall be made through fair, documented, and accountable processes.

2.3.4 Security by Design

Information security shall be integrated into the planning, procurement, implementation, operation, and retirement of all ICT systems.

2.3.5 Risk-Based Management

ICT decisions shall consider operational, financial, legal, cybersecurity, and reputational risks.

2.3.6 Compliance

ICT activities shall comply with applicable laws, donor requirements, contractual obligations, and internal organizational policies.

2.3.7 Value for Money

ICT resources shall be acquired and managed economically, efficiently, effectively, and sustainably.

2.3.8 Continuous Improvement

ICT governance processes shall be reviewed regularly to improve performance, security, resilience, and service quality.

2.4 ICT Governance Structure

The governance of ICT within ILA shall operate through the following structure:

2.4.1 Board of Directors

The Board shall provide overall strategic oversight of ICT governance by:

- Approving the ICT Policy and significant amendments.
- Approving major ICT investments and projects requiring Board authorization.
- Ensuring ICT risks are incorporated into organizational risk management.
- Monitoring ICT-related strategic risks and institutional resilience.
- Ensuring adequate resources are allocated for ICT development and cybersecurity.

2.4.2 Executive Director

The Executive Director shall:

- Provide executive leadership for ICT governance.
- Ensure implementation of this Policy.
- Approve ICT operational procedures and standards.
- Authorize significant ICT procurements within delegated authority.
- Ensure adequate ICT staffing and budgetary support.
- Report significant ICT risks and incidents to the Board.

2.4.3 Administration and ICT Function

The Administration and ICT function (or designated ICT Officer) shall:

- Manage day-to-day ICT operations.
- Maintain ICT infrastructure and equipment.
- Implement cybersecurity controls.
- Manage user accounts and access permissions.
- Monitor ICT assets and software licensing.
- Conduct routine maintenance and updates.
- Coordinate ICT procurement specifications.
- Maintain ICT documentation and records.
- Deliver ICT user support and training.
- Monitor compliance with this Policy.
- Coordinate backup and disaster recovery activities.

Where ILA does not have a dedicated ICT Officer, these responsibilities may be assigned to a qualified staff member or outsourced to a competent ICT service provider under appropriate supervision.

2.4.4 Department Heads

Department Heads shall:

- Ensure staff comply with this Policy.
- Identify departmental ICT requirements.
- Report ICT incidents promptly.
- Approve user access requests for their staff.
- Ensure proper use of ICT resources within their departments.
- Participate in ICT planning and budgeting.

2.4.5 Employees and Authorized Users

Every authorized user shall:

- Protect ICT assets assigned to them.
- Maintain the confidentiality of passwords and access credentials.
- Report ICT incidents, security breaches, or equipment loss immediately.
- Use ICT resources only for authorized purposes.
- Comply with this Policy and related procedures.
- Participate in mandatory ICT security awareness training.

2.5 ICT Planning

ILA shall prepare an annual ICT Operational Plan that supports the organization's Strategic Plan and Annual Work Plan.

The ICT Plan shall include:

- ICT priorities for the year.
- Planned infrastructure improvements.
- Software acquisition and upgrades.
- Hardware replacement schedules.
- Cybersecurity initiatives.
- Staff ICT capacity-building activities.
- Maintenance schedules.
- Business continuity improvements.
- Budget estimates.
- Risk mitigation activities.

ICT planning shall be reviewed annually and updated as organizational needs evolve.

2.6 ICT Budgeting

The organization shall allocate sufficient financial resources to support the effective implementation of this Policy.

The ICT budget may include funding for:

- Computer equipment.
- Networking infrastructure.
- Internet services.
- Licensed software.
- Cloud services.
- Website hosting.
- Email services.
- Cybersecurity tools.
- Antivirus software.
- Data backup systems.
- Maintenance contracts.
- ICT consultancy services.
- User training.
- Equipment replacement.
- Disaster recovery arrangements.

ICT expenditures shall comply with the Procurement and Asset Management Policy, the Finance and Accounting Policy, and approved budgetary procedures.

2.7 ICT Risk Management

ICT risks shall be integrated into the organization's overall Risk Management Framework.

Key ICT risks include:

- Cyberattacks.
- Unauthorized access.
- Malware infections.
- Data breaches.
- Equipment theft.
- Hardware failure.
- Software failure.
- Internet outages.
- Power interruptions.
- Human error.
- Fraud involving ICT systems.
- Loss of confidential information.
- Third-party service failures.
- Cloud service disruptions.

- Natural disasters affecting ICT infrastructure.

ILA shall identify, assess, mitigate, monitor, and periodically review ICT risks. Appropriate preventive, detective, and corrective controls shall be implemented based on the level of risk.

2.8 ICT Decision-Making

Major ICT decisions shall be guided by:

- Organizational priorities.
- Risk assessments.
- Budget availability.
- Security requirements.
- Legal obligations.
- Donor compliance requirements.
- Operational needs.
- Sustainability considerations.
- Total cost of ownership.
- Compatibility with existing systems.

Significant ICT investments shall be supported by documented needs assessments and, where appropriate, technical evaluations.

2.9 ICT Performance Monitoring

The Administration and ICT function shall monitor the performance of ICT services using appropriate indicators, including:

- System availability (uptime).
- Internet reliability.
- Number and resolution time of ICT support requests.
- Cybersecurity incidents.
- Asset utilization.
- Backup success rates.
- Software licensing compliance.
- User satisfaction.
- Staff completion of ICT security training.
- Implementation of annual ICT work plans.

Performance reports shall be submitted periodically to Senior Management to support informed decision-making and continuous improvement.

2.10 Review of ICT Governance

The ICT governance framework shall be reviewed periodically to ensure it remains effective, relevant, and aligned with:

- ILA's Strategic Plan.
- Organizational growth.
- Technological developments.
- Emerging cybersecurity threats.
- Applicable legal and regulatory requirements.
- Donor expectations.
- International good practice.

Recommendations arising from audits, risk assessments, incident investigations, and performance reviews shall be incorporated into improvements of the ICT governance framework.

CHAPTER THREE

ICT ASSET MANAGEMENT

3.1 Introduction

Information and Communication Technology (ICT) assets are valuable organizational resources that enable the Initiative for Legal Aid (ILA) to deliver legal aid services, manage programmes, communicate with stakeholders, safeguard organizational information, and achieve its strategic objectives. Effective management of ICT assets throughout their lifecycle is essential to ensure operational efficiency, accountability, information security, and value for money.

ILA is committed to acquiring, managing, maintaining, securing, and disposing of ICT assets in a transparent, accountable, and cost-effective manner. All ICT assets shall remain the property of the organization unless otherwise provided by law or contractual agreement.

3.2 Objectives

The objectives of ICT asset management are to:

a. Ensure ICT assets are acquired based on organizational needs and approved plans.

b. Maintain accurate records of all ICT assets.

c. Safeguard ICT assets against theft, loss, misuse, and damage.

d. Promote efficient utilization of ICT resources.

e. Extend the useful life of ICT equipment through preventive maintenance.

f. Ensure accountability for all assigned ICT assets.

g. Facilitate timely replacement of obsolete or defective equipment.

h. Ensure environmentally responsible and secure disposal of ICT assets.

3.3 Scope

This Chapter applies to all ICT assets owned, leased, donated, or otherwise entrusted to ILA, including but not limited to:

- Desktop computers.
- Laptop computers.
- Servers.
- Mobile phones.
- Tablets.
- Printers.
- Scanners.
- Photocopiers.
- Projectors.
- Cameras.
- Video conferencing equipment.
- Routers.
- Switches.
- Firewalls.
- Wi-Fi access points.
- External storage devices.
- Backup devices.
- Software licences.
- Cloud subscriptions.
- Email systems.
- Websites and domains.
- Databases.
- ICT accessories and peripherals.

3.4 ICT Asset Lifecycle Management

All ICT assets shall be managed throughout the following lifecycle stages:

- Needs identification.
- Budgeting.
- Procurement.
- Receipt and inspection.
- Registration.
- Configuration.
- Allocation.
- Use.
- Maintenance.
- Inventory verification.
- Upgrade.
- Transfer.
- Retirement.

- Disposal.

Each stage shall be documented to ensure accountability and traceability.

3.5 ICT Asset Acquisition

3.5.1 General Principles

ICT assets shall only be acquired where there is:

- An approved operational need.
- Budgetary provision.
- Compliance with the Procurement and Asset Management Policy.
- Technical compatibility with existing ICT infrastructure.
- Consideration of lifecycle costs.
- Compliance with security requirements.

3.5.2 Procurement Standards

Before procurement, the responsible department shall ensure:

- Technical specifications are clearly defined.
- Standardization is maintained where practical.
- Equipment is sourced from reputable suppliers.
- Warranty provisions are adequate.
- Maintenance support is available.
- Software licences are genuine and legally obtained.
- Equipment is energy efficient where feasible.

3.5.3 Donations

ICT equipment received through donations shall:

- Meet organizational technical standards.
- Be inspected before acceptance.
- Be registered in the ICT Asset Register.
- Be assigned an asset identification number.
- Become the property of ILA unless otherwise agreed in writing.

3.6 Receipt and Inspection

Upon delivery of ICT assets:

- Quantities shall be verified.
- Technical specifications shall be confirmed.
- Equipment shall be inspected for defects.

- Warranty documentation shall be collected.
- User manuals shall be retained where applicable.
- Any discrepancies shall be reported immediately.

No ICT asset shall be issued before successful inspection and acceptance.

3.7 ICT Asset Registration

Every ICT asset shall be recorded in the official ICT Asset Register immediately after receipt.

The register shall include, at a minimum:

- Asset identification number.
- Description of the asset.
- Manufacturer.
- Model.
- Serial number.
- Purchase order reference.
- Supplier.
- Date of acquisition.
- Purchase cost.
- Funding source or donor (where applicable).
- Warranty period.
- Assigned location.
- Assigned user.
- Asset condition.
- Maintenance history.
- Disposal details (where applicable).

The ICT Asset Register shall be maintained electronically with appropriate backup measures.

3.8 Asset Identification and Labelling

Every ICT asset shall receive a unique asset identification number.

Where practical, assets shall be labelled using durable asset tags indicating:

- ILA ownership.
- Asset number.
- Department or location.
- Barcode or QR code (where implemented).

Asset labels shall not be removed, altered, or obscured without authorization.

3.9 Allocation of ICT Assets

ICT assets shall only be assigned based on official organizational duties.

Before receiving equipment, users shall:

- Sign an ICT Asset Handover Form.
- Accept responsibility for the assigned equipment.
- Agree to comply with this Policy.
- Return the equipment upon request or separation from the organization.

The ICT function shall maintain records of all asset assignments.

3.10 Responsibilities of Asset Users

Every user assigned an ICT asset shall:

- Exercise reasonable care.
- Protect equipment from theft and damage.
- Keep equipment clean and secure.
- Prevent unauthorized access.
- Use equipment only for authorized organizational purposes.
- Report faults immediately.
- Report loss or theft without delay.
- Return equipment upon request.
- Avoid unauthorized modification of equipment.

Users shall be personally accountable for negligent loss or damage, subject to applicable laws, employment contracts, and disciplinary procedures.

3.11 Movement and Transfer of ICT Assets

ICT assets shall not be moved permanently between offices or departments without authorization.

Transfers shall:

- Be documented.
- Update the ICT Asset Register.
- Include verification of the asset condition.
- Record the receiving officer.
- Be approved by the responsible authority.

Temporary movement of ICT equipment outside organizational premises shall require prior approval unless authorized under approved field operations or remote working arrangements.

3.12 ICT Asset Inventory

ILA shall conduct regular physical verification of ICT assets.

Inventory verification shall be conducted:

- At least annually.
- Before external audits where necessary.
- Upon change of custody.
- Following theft, fire, or disaster.
- Whenever management considers it necessary.

Inventory verification shall confirm:

- Physical existence.
- Asset condition.
- Assigned user.
- Asset location.
- Operational status.
- Accuracy of records.

Discrepancies shall be investigated promptly.

3.13 Maintenance of ICT Assets

ILA shall implement preventive and corrective maintenance programmes to maximize the useful life of ICT assets.

Maintenance activities may include:

- Cleaning equipment.
- Hardware servicing.
- Operating system updates.
- Software updates.
- Security patches.
- Antivirus updates.
- Battery replacement.
- Hardware repairs.
- Network maintenance.
- Performance optimization.

Maintenance shall only be performed by authorized personnel or approved service providers.

3.14 Repairs

Where ICT equipment becomes defective:

- Users shall report faults immediately.
- Unauthorized repairs are prohibited.
- Repairs shall be documented.
- Replacement parts shall meet approved standards.
- Equipment under warranty shall be serviced by authorized providers where applicable.

If repair costs exceed the economic value of the asset, replacement may be recommended.

3.15 Loss, Theft and Damage

Any loss, theft, or damage involving ICT assets shall be reported immediately to:

- The immediate supervisor.
- The Administration and ICT function.
- The Executive Director (for significant incidents).

Where appropriate:

- A written incident report shall be prepared.
- Police reports shall be obtained.
- Insurance claims shall be initiated where applicable.
- Internal investigations shall be conducted.

Failure to report incidents promptly may constitute misconduct.

3.16 Obsolete ICT Equipment

ICT assets shall be assessed periodically to determine whether they have become:

- Technologically obsolete.
- Economically inefficient.
- Beyond repair.
- Incompatible with organizational systems.
- Unsafe for continued use.

Obsolete assets shall be processed in accordance with approved disposal procedures.

3.17 Disposal of ICT Assets

Disposal shall comply with the Procurement and Asset Management Policy and applicable laws.

Approved disposal methods may include:

- Public auction.
- Competitive sale.
- Donation.
- Trade-in.
- Recycling.
- Certified destruction.
- Environmentally responsible disposal.

Prior to disposal:

- Organizational data shall be permanently erased using approved data sanitization methods.
- Storage devices shall be securely wiped or physically destroyed where necessary.
- Software licences shall be deactivated or transferred in accordance with licence terms.
- Disposal shall be authorized by the appropriate approval authority.
- The ICT Asset Register shall be updated.

3.18 Insurance of ICT Assets

Where appropriate and financially feasible, ILA may insure high-value ICT assets against risks such as:

- Theft.
- Fire.
- Flood.
- Accidental damage.
- Electrical damage.
- Natural disasters.

Insurance arrangements shall be reviewed periodically to ensure adequate coverage.

3.19 Asset Management Monitoring

The Administration and ICT function shall periodically monitor compliance with this Chapter by reviewing:

- Asset utilization.
- Inventory accuracy.
- Maintenance records.
- Asset losses.
- Disposal records.
- Warranty management.
- Compliance with handover procedures.

Findings shall be reported to Senior Management, and corrective actions shall be implemented where necessary.

3.20 Non-Compliance

Failure to comply with ICT asset management requirements may result in:

- Recovery of organizational losses where legally permissible.
- Withdrawal of ICT privileges.
- Disciplinary action under the Human Resource and Administration Policy.
- Termination of contracts where applicable.
- Civil or criminal proceedings where warranted by law.

CHAPTER FOUR

ACCEPTABLE USE OF ICT RESOURCES

4.1 Introduction

The Initiative for Legal Aid (ILA) provides Information and Communication Technology (ICT) resources to enable staff, consultants, interns, volunteers, and authorized users to perform their official duties effectively, efficiently, and securely. These resources are organizational assets and shall be used responsibly, ethically, lawfully, and in a manner that protects the confidentiality, integrity, and availability of the organization's information and systems.

This Chapter establishes the standards governing the acceptable use of ICT resources and seeks to minimize legal, operational, cybersecurity, and reputational risks arising from improper use.

4.2 Objectives

The objectives of this Chapter are to:

a. Promote responsible and professional use of ICT resources.

b. Protect ICT systems and organizational information from misuse and abuse.

c. Ensure compliance with applicable laws, organizational policies, and contractual obligations.

d. Reduce cybersecurity risks arising from user behaviour.

e. Promote efficient use of ICT resources in support of ILA's mandate.

4.3 Scope

This Chapter applies to all persons authorized to access or use ILA ICT resources, including:

- Members of the Board of Directors.
- Employees.

- Consultants.
- Volunteers.
- Interns.
- Temporary staff.
- Contractors.
- Service providers.
- Any other authorized user.

It applies whether ICT resources are accessed from:

- ILA offices.
- Field offices.
- Home offices.
- Remote work locations.
- Partner premises.
- Any other approved location.

4.4 ICT Resources Covered

This Chapter applies to, but is not limited to:

- Desktop computers.
- Laptop computers.
- Servers.
- Mobile phones.
- Tablets.
- Email systems.
- Internet services.
- Wi-Fi networks.
- Cloud services.
- Collaboration platforms.
- File storage systems.
- Databases.
- Printers.
- Photocopiers.
- Scanners.
- Audio-visual equipment.
- Official websites.
- Social media accounts.
- Messaging applications.
- USB storage devices.
- External hard drives.
- Software applications.
- Digital records.

4.5 General Principles of Acceptable Use

Users shall:

a. Use ICT resources primarily for official organizational purposes.

b. Exercise professionalism, integrity, and accountability at all times.

c. Protect organizational information from unauthorized disclosure.

d. Comply with this Policy and all related procedures.

e. Respect intellectual property rights.

f. Protect ICT equipment from damage, theft, misuse, and unauthorized access.

g. Report ICT incidents promptly.

4.6 Permitted Use

Authorized users may use ICT resources for:

- Programme implementation.
- Legal aid service delivery.
- Legal research.
- Case management.
- Communication with beneficiaries.
- Donor reporting.
- Financial management.
- Human resource administration.
- Procurement.
- Monitoring, evaluation, accountability and learning (MEAL).
- Training and capacity building.
- Official meetings.
- Advocacy activities.
- Institutional management.
- Approved remote working.
- Other authorized organizational functions.

Reasonable and limited personal use may be permitted provided that such use:

- Does not interfere with official duties.
- Does not incur significant additional costs.
- Does not violate this Policy.
- Does not compromise information security.
- Does not affect network performance.

- Does not damage the reputation of ILA.

Personal use remains a privilege and may be restricted or withdrawn where necessary.

4.7 Prohibited Use

Users shall not use ICT resources to:

a. Conduct illegal activities.

b. Access, create, possess, transmit, or distribute unlawful, offensive, discriminatory, defamatory, obscene, or abusive material.

c. Engage in harassment, bullying, intimidation, or hate speech.

d. Commit fraud or facilitate corruption.

e. Circumvent ICT security controls.

f. Install unauthorized software or applications.

g. Access another user's account without authorization.

h. Share passwords or authentication credentials.

i. Download pirated software or copyrighted material unlawfully.

j. Operate unauthorized servers or network services.

k. Conduct personal commercial activities using ILA ICT resources unless expressly authorized.

l. Mine cryptocurrency or engage in other resource-intensive personal computing activities.

m. Introduce malicious software into organizational systems.

n. Deliberately disrupt ICT services.

o. Remove organizational data without authorization.

p. Connect unauthorized devices to organizational networks.

q. Use organizational ICT resources for political campaigning, partisan political activities, or personal fundraising without authorization.

4.8 Computer and Workstation Use

Users shall:

- Lock their computers whenever leaving their workstations unattended.
- Log out at the end of each working day.
- Keep operating systems updated.
- Store official files only in approved locations.
- Avoid saving confidential information on unsecured local devices where approved shared or cloud storage exists.
- Ensure antivirus protection remains enabled.
- Prevent unauthorized persons from using assigned equipment.
- Shut down or securely lock equipment after working hours unless operational requirements dictate otherwise.

Users shall not disable security settings without authorization.

4.9 Internet Usage

ILA provides internet access to support official organizational activities.

Users shall use the internet responsibly and shall not:

- Visit malicious or unsafe websites.
- Download unauthorized software.
- Access illegal content.
- Engage in excessive personal browsing during working hours.
- Consume excessive bandwidth through non-work-related streaming or downloads.
- Bypass internet security controls.
- Use anonymizing tools or virtual private networks (VPNs) without authorization.

The organization reserves the right to monitor internet usage to protect its systems, ensure compliance with this Policy, and investigate suspected misuse, in accordance with applicable laws and respect for individual privacy.

4.10 Email Usage

Official email accounts are organizational communication tools.

Users shall:

- Use official email addresses for official correspondence.
- Exercise professionalism in all communications.
- Verify recipient addresses before sending confidential information.
- Exercise caution when opening attachments or clicking links.
- Report suspected phishing emails immediately.

- Use appropriate email signatures approved by the organization.
- Retain official correspondence in accordance with records management requirements.

Users shall not:

- Use organizational email for unlawful or fraudulent purposes.
- Forward confidential information without authorization.
- Send spam, chain letters, or unsolicited mass communications.
- Misrepresent themselves using another person's identity.
- Send offensive, discriminatory, or inappropriate messages.

Official email accounts remain the property of ILA.

4.11 Use of Messaging Applications

Messaging platforms such as WhatsApp, Microsoft Teams, Signal, Zoom, Google Meet, and similar services may be used for official purposes where approved.

Users shall:

- Protect confidential information.
- Verify recipients before sharing sensitive information.
- Use official groups responsibly.
- Maintain professional conduct.
- Avoid sharing confidential documents through unapproved platforms.

Where available, organizational accounts should be used in preference to personal accounts for official communication.

4.12 Social Media Use

Employees shall conduct themselves professionally on social media where their activities may reasonably be associated with ILA.

Unless authorized:

- Users shall not speak on behalf of ILA.
- Users shall not disclose confidential organizational information.
- Users shall not publish donor-confidential information.
- Users shall not publish beneficiary information without appropriate authorization and consent.
- Users shall not damage the organization's reputation through inappropriate online conduct.

Official social media accounts shall only be managed by authorized personnel.

4.13 Use of Removable Storage Devices

The use of USB drives, external hard drives, memory cards, and other removable media presents information security risks.

Accordingly:

- Only authorized removable storage devices may be used.
- Devices shall be scanned for malware before use.
- Confidential information stored on removable media shall be encrypted where feasible.
- Lost removable media containing organizational information shall be reported immediately.

4.14 Printing and Document Handling

Users shall:

- Print only where necessary.
- Collect printed documents promptly.
- Secure confidential printouts.
- Dispose of confidential documents using approved destruction methods.
- Avoid unnecessary printing to promote environmental sustainability.

4.15 Software Installation

Only authorized ICT personnel may install, remove, or modify software on organizational ICT equipment.

Users shall not:

- Install unlicensed software.
- Install software downloaded from untrusted sources.
- Disable security applications.
- Modify system configurations without authorization.

4.16 Monitoring of ICT Resources

To protect organizational assets and ensure compliance, ILA may monitor, log, and audit the use of its ICT resources, including:

- Network activity.
- Internet usage.
- Email systems.
- File storage.
- System access logs.
- Security alerts.

- Software installations.
- Device compliance.

Monitoring shall be conducted for legitimate organizational purposes, including cybersecurity, system maintenance, investigations, legal compliance, and protection of organizational assets. Information obtained through monitoring shall be handled confidentially and accessed only by authorized personnel.

4.17 User Responsibilities

Every user shall:

- Read and comply with this Policy.
- Complete required ICT security awareness training.
- Protect passwords and authentication credentials.
- Report ICT incidents immediately.
- Safeguard assigned ICT equipment.
- Use ICT resources responsibly.
- Cooperate during ICT investigations and audits.

Ignorance of this Policy shall not excuse non-compliance.

4.18 Violations of Acceptable Use

Violations of this Chapter may result in one or more of the following actions:

- Verbal or written warning.
- Mandatory retraining.
- Temporary suspension of ICT access.
- Permanent withdrawal of ICT privileges.
- Recovery of losses where legally permissible.
- Disciplinary action under the Human Resource and Administration Policy.
- Termination of employment or contract, where warranted.
- Referral to law enforcement authorities where criminal conduct is suspected.

The severity of the response shall be proportionate to the nature, impact, and recurrence of the violation.

4.19 Exceptions

Any exception to this Chapter shall:

- Be justified by operational necessity.
- Be documented in writing.
- Be approved by the Executive Director or a delegated authority.
- Include appropriate compensating controls to manage any resulting risks.

CHAPTER FIVE

USER ACCESS MANAGEMENT

5.1 Introduction

User Access Management is a fundamental component of information security. Appropriate access controls help ensure that only authorized individuals can access ILA's information systems, applications, networks, databases, and digital resources. Effective user access management protects confidential information, reduces cybersecurity risks, strengthens accountability, and supports compliance with legal, contractual, and donor obligations.

The Initiative for Legal Aid (ILA) shall implement a robust user access management framework based on the principles of least privilege, need-to-know, segregation of duties, and accountability. Access rights shall be granted only to the extent necessary for users to perform their official responsibilities and shall be reviewed regularly throughout the user lifecycle.

5.2 Objectives

The objectives of this Chapter are to:

a. Ensure only authorized individuals have access to ICT resources.

b. Protect organizational information from unauthorized access, disclosure, modification, or destruction.

c. Establish standardized procedures for creating, modifying, reviewing, suspending, and terminating user accounts.

d. Promote accountability through unique user identification and authentication.

e. Reduce cybersecurity risks associated with excessive or inappropriate access privileges.

f. Ensure access rights are promptly updated to reflect changes in employment status, job responsibilities, or contractual arrangements.

5.3 Scope

This Chapter applies to all access to ILA ICT resources, including:

- Network accounts.
- Email accounts.
- Cloud services.
- Case management systems.
- Financial management systems.

- Human resource systems.
- Document management systems.
- Website administration.
- Databases.
- Remote access services.
- Mobile applications.
- Collaboration platforms.
- Shared drives.
- Administrative systems.

It applies to:

- Board Members where access is provided.
- Employees.
- Interns.
- Volunteers.
- Consultants.
- Temporary staff.
- Contractors.
- Third-party service providers.
- Any other authorized users.

5.4 Access Control Principles

ILA shall implement the following access control principles:

5.4.1 Least Privilege

Users shall be granted only the minimum level of access required to perform their assigned duties.

5.4.2 Need-to-Know

Access to confidential or restricted information shall only be provided where there is a legitimate business need.

5.4.3 Segregation of Duties

Critical business processes shall, where practicable, be designed so that no single individual has incompatible responsibilities that could enable fraud, unauthorized transactions, or abuse.

5.4.4 Individual Accountability

Every user shall have a unique user account. Shared accounts shall be avoided except where technically necessary and specifically authorized.

5.4.5 Access by Authorization

No user shall be granted system access without documented approval from the appropriate authority.

5.5 User Account Lifecycle Management

ILA shall manage user accounts throughout the following lifecycle:

- Access request.
- Approval.
- Account creation.
- Access assignment.
- Account maintenance.
- Periodic review.
- Modification.
- Suspension.
- Termination.
- Archiving (where applicable).

Each stage shall be documented.

5.6 User Registration

Before creating any user account:

- The user shall have an approved role within the organization.
- A completed User Access Request Form shall be submitted.
- The relevant Department Head shall approve the requested access.
- The ICT function shall verify the request.
- The appropriate authorization shall be obtained before account activation.

No account shall be created based solely on verbal instructions except in documented emergencies.

5.7 User Identification

Every authorized user shall receive:

- A unique username.
- A unique email address where applicable.
- Individual authentication credentials.
- Appropriate system permissions.

Usernames shall not be reused in a manner that could create confusion or compromise audit trails.

5.8 Access Levels

Access permissions shall be assigned according to official responsibilities.

Typical access levels include:

a. General User

Access limited to ordinary operational functions necessary for assigned duties.

b. Departmental User

Additional access to departmental files, systems, and resources.

c. Supervisor or Manager

Expanded access necessary for supervisory responsibilities, including approval workflows where applicable.

d. System Administrator

Privileged access required for ICT administration, maintenance, monitoring, and technical support.

e. Executive Access

Access necessary for executive decision-making and organizational oversight.

Each access level shall be documented and periodically reviewed.

5.9 Password Management

Passwords are the first line of defense against unauthorized access. All users shall protect their passwords and comply with organizational password requirements.

Passwords shall:

- Be known only to the authorized user.
- Never be shared.
- Never be written in unsecured locations.
- Never be transmitted through unsecured channels.
- Be changed immediately if compromise is suspected.

Where technically feasible, passwords should:

- Meet minimum complexity requirements.

- Avoid dictionary words, personal information, or predictable patterns.
- Be unique for organizational accounts.
- Be supported by password managers approved by ILA where appropriate.

Detailed password standards are provided in **Annex VI: Password Standards**.

5.10 Multi-Factor Authentication (MFA)

Where technically available, ILA shall implement Multi-Factor Authentication (MFA) for:

- Email accounts.
- Cloud services.
- Financial systems.
- Remote access.
- Administrative accounts.
- Website administration.
- Other high-risk systems.

MFA shall combine at least two independent authentication factors, such as:

- Password.
- Authentication application.
- Hardware token.
- Biometric verification.

Users shall not attempt to bypass MFA controls.

5.11 Privileged Accounts

Privileged accounts include:

- System administrators.
- Database administrators.
- Network administrators.
- Domain administrators.
- Cloud administrators.
- Website administrators.
- Security administrators.

These accounts shall:

- Be limited to authorized personnel.
- Be used only for administrative duties.
- Not be used for routine day-to-day activities where standard accounts are sufficient.
- Be subject to enhanced monitoring and logging.

- Be reviewed regularly.

5.12 Shared Accounts

Shared accounts are discouraged because they reduce accountability.

Where operationally unavoidable:

- Written approval shall be obtained.
- Individual accountability mechanisms shall be implemented where possible.
- Passwords shall be changed whenever authorized users change.
- Usage shall be logged and monitored.

5.13 Remote Access

Remote access shall only be permitted where:

- It supports legitimate organizational activities.
- Appropriate security controls are implemented.
- Users comply with remote working requirements.
- Devices meet organizational security standards.

Remote access sessions may be monitored for security purposes.

5.14 Temporary Access

Temporary access may be granted to:

- Consultants.
- Auditors.
- Service providers.
- Trainers.
- Short-term contractors.
- Temporary staff.

Temporary accounts shall:

- Have defined expiration dates.
- Be limited to the minimum necessary access.
- Be automatically disabled or manually removed upon completion of the assignment.

5.15 Access Modification

Access rights shall be reviewed and modified whenever:

- An employee changes position.

- Duties change.
- A contract is renewed.
- New systems are introduced.
- Organizational restructuring occurs.
- Security risks require access adjustments.

Department Heads shall promptly notify the ICT function of any required changes.

5.16 Periodic Access Reviews

The ICT function shall conduct periodic reviews of user access rights to ensure that:

- Access remains appropriate.
- Dormant accounts are identified.
- Excessive privileges are removed.
- Departed users no longer retain access.
- Administrative accounts remain justified.

Access reviews shall be conducted:

- At least every six (6) months.
- Following significant organizational changes.
- Following major security incidents.
- Prior to external ICT audits where appropriate.

5.17 Dormant Accounts

Accounts that remain inactive for an extended period shall be:

- Identified.
- Investigated.
- Temporarily suspended where appropriate.
- Permanently removed where no longer required.

Dormant accounts represent significant cybersecurity risks and shall not remain active unnecessarily.

5.18 Suspension of Access

User access may be suspended where:

- Security breaches are suspected.
- Misuse of ICT resources is alleged.
- Employment is suspended.
- Contracts are temporarily paused.
- Investigations are ongoing.

- Organizational security requires immediate action.

Suspension shall be documented and communicated to the relevant parties, unless restricted by law or the needs of an investigation.

5.19 Termination of Access

Upon resignation, retirement, dismissal, expiry of contract, or other separation from the organization:

The ICT function shall, without undue delay:

- Disable all user accounts.
- Remove network access.
- Disable email accounts.
- Revoke cloud service access.
- Remove remote access privileges.
- Recover ICT equipment.
- Secure organizational data.
- Update access records.
- Archive official emails and files where required by records management procedures.

Department Heads and Human Resources shall notify the ICT function promptly of all staff departures to ensure timely deactivation.

5.20 Third-Party Access

Third-party access shall be strictly controlled.

Before granting access:

- A legitimate business need shall be established.
- Confidentiality obligations shall be documented where appropriate.
- Access shall be approved by management.
- Access duration shall be defined.
- Security requirements shall be communicated.
- Activities may be monitored.

Third-party access shall be revoked immediately upon completion of the authorized work.

5.21 Monitoring and Audit

The ICT function shall maintain logs of:

- User account creation.
- Access approvals.

- Login attempts.
- Failed authentication attempts.
- Password resets.
- Privileged account activities.
- Access modifications.
- Account suspensions.
- Account terminations.

Access logs shall be protected from unauthorized alteration and retained in accordance with the organization's records management requirements.

5.22 User Responsibilities

Every authorized user shall:

- Keep authentication credentials confidential.
- Use only assigned accounts.
- Report suspected unauthorized access immediately.
- Log out after completing work.
- Lock devices when unattended.
- Notify the ICT function if access is no longer required or appears inappropriate.
- Cooperate with access reviews and security investigations.

5.23 Non-Compliance

Failure to comply with this Chapter may result in:

- Immediate suspension of system access.
- Mandatory retraining.
- Disciplinary action under the Human Resource and Administration Policy.
- Recovery of losses where legally permissible.
- Termination of employment or contract where warranted.
- Referral to law enforcement where criminal activity is suspected.

5.24 Exceptions

Any exception to the access management requirements shall:

- Be supported by a documented operational justification.
- Be approved by the Executive Director or delegated authority.
- Be time-bound where appropriate.
- Include compensating security controls.
- Be recorded and subject to periodic review.

CHAPTER SIX

INFORMATION SECURITY

6.1 Introduction

Information is one of the Initiative for Legal Aid's (ILA) most valuable assets. The organization routinely creates, receives, processes, stores, and shares information relating to legal aid clients, beneficiaries, employees, volunteers, partners, donors, suppliers, financial transactions, governance, and programme implementation. The confidentiality, integrity, and availability of this information are essential to maintaining public trust, protecting the rights of beneficiaries, complying with legal and donor obligations, and ensuring organizational continuity.

ILA is committed to implementing appropriate administrative, technical, and physical safeguards to protect information against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, unauthorized access, theft, misuse, and other security threats.

This Chapter establishes the principles, responsibilities, and controls for managing and protecting information throughout its lifecycle.

6.2 Objectives

The objectives of this Chapter are to:

a. Protect the confidentiality, integrity, and availability of organizational information.

b. Establish a standardized information classification system.

c. Promote secure handling, storage, transmission, and disposal of information.

d. Prevent unauthorized access, disclosure, alteration, or destruction of information.

e. Ensure compliance with applicable legal, contractual, and donor requirements relating to information security.

f. Promote a culture of information security awareness and accountability throughout the organization.

6.3 Scope

This Chapter applies to all information owned, processed, received, stored, or managed by ILA, regardless of its format or location, including:

- Electronic records.
- Paper records.
- Emails.

- Databases.
- Audio recordings.
- Video recordings.
- Photographs.
- Case files.
- Contracts.
- Financial records.
- Human resource records.
- Donor reports.
- Research materials.
- Cloud-based information.
- Backup media.
- Portable storage devices.

It applies to all persons who have access to ILA information resources.

6.4 Information Security Principles

ILA shall implement information security based on the following principles:

6.4.1 Confidentiality

Information shall be accessible only to authorized persons with a legitimate business need.

6.4.2 Integrity

Information shall remain accurate, complete, authentic, and protected against unauthorized alteration or destruction.

6.4.3 Availability

Information and information systems shall remain accessible to authorized users whenever required for legitimate organizational purposes.

6.4.4 Accountability

Every user is personally responsible for protecting information entrusted to them and shall be accountable for their actions relating to information security.

6.4.5 Least Privilege

Access to information shall be limited to the minimum necessary to perform assigned duties.

6.4.6 Need-to-Know

Sensitive information shall only be disclosed to persons who require it for authorized organizational purposes.

6.5 Information Classification

ILA shall classify information according to its sensitivity and the potential impact of unauthorized disclosure, alteration, or loss.

Information shall be classified into the following categories:

6.5.1 Public Information

Information approved for public dissemination.

Examples include:

- Published reports.
- Public awareness materials.
- Approved press releases.
- Published legal education materials.
- Public website content.
- Vacancies.
- Public policy statements.

Public information may be freely shared after appropriate approval.

6.5.2 Internal Information

Information intended for internal organizational use but not considered highly sensitive.

Examples include:

- Internal procedures.
- Meeting agendas.
- Routine operational documents.
- Internal communications.
- Training materials.

Internal information shall not be disclosed externally without authorization.

6.5.3 Confidential Information

Information requiring restricted access because unauthorized disclosure could adversely affect the organization or individuals.

Examples include:

- Personnel records.
- Procurement evaluations.
- Financial information.
- Donor agreements.
- Legal advice.
- Investigation reports.
- Internal audit reports.
- Performance appraisals.
- Vendor quotations.

Confidential information shall only be accessed by authorized personnel.

6.5.4 Highly Confidential / Restricted Information

Information requiring the highest level of protection because unauthorized disclosure could result in serious harm to beneficiaries, staff, partners, or the organization.

Examples include:

- Legal case files.
- Beneficiary personal information.
- Child protection records.
- Safeguarding and PSEAH reports.
- Witness information.
- Passwords and encryption keys.
- Bank account credentials.
- Investigation evidence.
- Board confidential deliberations.
- Litigation strategy documents.

Highly Confidential information shall receive enhanced security protections.

6.6 Information Ownership

Every significant information asset shall have a designated Information Owner.

Information Owners shall:

- Determine classification levels.
- Approve access requests.
- Ensure information accuracy.
- Monitor appropriate use.
- Approve information sharing.
- Ensure appropriate retention and disposal.

6.7 Handling of Information

Information shall be handled according to its classification.

Users shall:

- Verify recipients before sharing information.
- Minimize unnecessary copying.
- Store information securely.
- Protect information from unauthorized viewing.
- Avoid discussing confidential matters in public places.
- Use secure communication channels for sensitive information.

Sensitive documents shall not be left unattended in meeting rooms, printers, vehicles, or public areas.

6.8 Storage of Information

Electronic information shall be stored in approved organizational systems, including secure servers and authorized cloud services.

Where appropriate:

- Access permissions shall be applied.
- Storage locations shall be backed up.
- Encryption shall be used for sensitive information.
- Audit logs shall be maintained for critical systems.

Paper records shall be stored in secure cabinets or rooms with access restricted to authorized personnel.

6.9 Transmission of Information

Information shall be transmitted using secure methods appropriate to its classification.

Users shall:

- Use organizational email accounts for official communications.
- Encrypt highly confidential information where technically feasible.
- Verify recipient identities before sending sensitive information.
- Avoid transmitting confidential information through unapproved channels.
- Protect attachments containing sensitive data with appropriate security measures.

Where physical media are used, they shall be packaged and transported securely.

6.10 Encryption

ILA shall implement encryption as an important safeguard for protecting sensitive information.

Encryption should be used for:

- Portable devices containing confidential information.
- Backup media.
- Sensitive electronic files.
- Remote communications where appropriate.
- Cloud storage where supported.
- Portable storage devices used for confidential data.

Encryption keys shall be securely managed and accessible only to authorized personnel.

6.11 Physical Information Security

Physical measures shall be implemented to protect information assets.

These measures include:

- Controlled office access.
- Lockable filing cabinets.
- Visitor management procedures.
- Restricted server rooms.
- CCTV where appropriate.
- Fire protection measures.
- Environmental controls for ICT equipment.
- Secure storage for backup media.

Only authorized personnel shall have access to areas containing critical ICT infrastructure or highly sensitive information.

6.12 Clean Desk and Clear Screen Policy

To reduce the risk of unauthorized access:

Users shall:

- Lock their computers when unattended.
- Remove confidential papers from desks after use.
- Secure files before leaving the office.
- Store portable devices securely.
- Clear whiteboards containing sensitive information after meetings.
- Collect printouts immediately from shared printers.

No confidential documents shall be left visible outside working hours unless secured.

6.13 Information Sharing

Information shall only be shared where:

- There is a legitimate organizational purpose.
- Appropriate authorization has been obtained.
- The recipient has a lawful or contractual basis to receive the information.
- Confidentiality requirements are maintained.
- Data protection obligations are respected.

Information sharing agreements may be required for external parties where appropriate.

6.14 Third-Party Information Security

Third parties with access to organizational information shall:

- Comply with this Policy.
- Maintain appropriate security controls.
- Protect confidential information.
- Report security incidents promptly.
- Return or securely destroy organizational information upon completion of services, where required.

ILA may require confidentiality agreements, non-disclosure agreements (NDAs), or contractual information security clauses before granting access.

6.15 Information Retention

Information shall be retained only for as long as necessary to:

- Fulfil operational needs.
- Meet legal obligations.
- Comply with donor requirements.
- Support audit requirements.
- Protect organizational interests.

Retention periods shall be guided by the organization's Records Management Policy and applicable legal or contractual obligations.

6.16 Secure Disposal of Information

When information is no longer required, it shall be disposed of securely.

Examples include:

Electronic Information

- Secure deletion.
- Cryptographic erasure where appropriate.
- Physical destruction of storage media when necessary.

Paper Information

- Cross-cut shredding.
- Secure destruction by authorized service providers.
- Incineration where appropriate and environmentally acceptable.

Users shall not dispose of confidential documents in ordinary waste bins.

6.17 Information Security Incident Reporting

Every user shall immediately report suspected or actual information security incidents, including:

- Unauthorized disclosure.
- Lost documents.
- Stolen devices.
- Misdirected emails.
- Unauthorized system access.
- Data breaches.
- Missing files.
- Suspected cyberattacks.
- Accidental disclosure of confidential information.

Reports shall be made to the ICT function and the immediate supervisor without delay. Significant incidents shall be escalated to the Executive Director and managed in accordance with Chapter Fifteen (ICT Incident Management).

6.18 Information Security Awareness

ILA shall promote a culture of information security through:

- Staff induction.
- Periodic refresher training.
- Cybersecurity awareness campaigns.
- Phishing awareness exercises where feasible.
- Policy dissemination.
- Security alerts and guidance.
- Lessons learned from security incidents.

All personnel shall participate in mandatory information security awareness activities as directed by the organization.

6.19 Monitoring and Compliance

The Administration and ICT function shall monitor compliance with this Chapter through:

- Security audits.
- Access reviews.
- System monitoring.
- Incident analysis.
- Compliance assessments.
- Spot checks where appropriate.

Non-compliance shall be addressed promptly through corrective actions, training, or disciplinary measures.

6.20 Non-Compliance

Failure to comply with this Chapter may result in:

- Mandatory corrective training.
- Restriction or suspension of access to ICT resources.
- Disciplinary action under the Human Resource and Administration Policy.
- Recovery of losses where legally permissible.
- Termination of employment or contract, where warranted.
- Civil or criminal proceedings where required by applicable law.

6.21 Exceptions

Any exception to this Chapter shall:

- Be documented.
- Be supported by a legitimate operational justification.
- Be approved by the Executive Director or delegated authority.
- Include appropriate compensating security controls.

CHAPTER SEVEN

CYBERSECURITY

7.1 Introduction

The Initiative for Legal Aid (ILA) recognizes that cybersecurity is fundamental to protecting the organization's people, information, operations, and reputation. As ILA increasingly relies on digital technologies to deliver legal aid services, manage programmes, communicate with stakeholders, and safeguard sensitive information, it also faces growing cybersecurity risks, including cyberattacks, ransomware, phishing, malware, data breaches, unauthorized access, insider threats, and disruption of critical ICT services.

ILA is committed to establishing and maintaining a proactive cybersecurity programme that prevents, detects, responds to, and recovers from cyber threats while ensuring the confidentiality, integrity, availability, and resilience of its information systems.

This Chapter establishes the cybersecurity framework applicable to all ICT resources owned, managed, or used by ILA.

7.2 Objectives

The objectives of this Chapter are to:

a. Protect ICT systems against cyber threats and attacks.

b. Reduce the likelihood and impact of cybersecurity incidents.

c. Strengthen the resilience of ICT infrastructure.

d. Ensure timely detection and response to cyber incidents.

e. Promote secure use of ICT resources.

f. Protect organizational information from unauthorized access, disclosure, alteration, or destruction.

g. Foster a culture of cybersecurity awareness among all users.

7.3 Scope

This Chapter applies to:

- Computer systems.
- Servers.
- Mobile devices.

- Networks.
- Cloud platforms.
- Websites.
- Email systems.
- Databases.
- Software applications.
- Collaboration platforms.
- Backup systems.
- Internet connectivity.
- Remote access systems.
- Third-party ICT services.

It applies to all personnel, contractors, consultants, volunteers, interns, service providers, and other authorized users.

7.4 Cybersecurity Principles

ILA shall implement cybersecurity based on the following principles:

7.4.1 Defense in Depth

Multiple layers of administrative, technical, and physical security controls shall be implemented to reduce the likelihood of successful cyberattacks.

7.4.2 Zero Trust Approach

No user, device, or network connection shall automatically be trusted. Access shall be continuously verified based on identity, authorization, and risk.

7.4.3 Risk-Based Security

Cybersecurity controls shall be proportionate to the level of risk presented by systems, information, and operations.

7.4.4 Continuous Improvement

Cybersecurity controls shall be reviewed and improved regularly in response to emerging threats, technological developments, and lessons learned from incidents.

7.4.5 Shared Responsibility

Cybersecurity is the responsibility of every user, not solely the ICT function.

7.5 Cybersecurity Governance

The Administration and ICT function shall coordinate the implementation of cybersecurity measures, including:

- Cybersecurity planning.
- Security monitoring.
- Risk assessments.
- Security awareness programmes.
- Vulnerability management.
- Incident coordination.
- Compliance monitoring.
- Cybersecurity reporting.

Management shall provide adequate financial, technical, and human resources to support cybersecurity.

7.6 Endpoint Security

All organizational devices shall be protected against unauthorized access and cyber threats.

Minimum endpoint security controls include:

- Password-protected user accounts.
- Automatic screen locking.
- Full-disk encryption where feasible, especially for laptops and mobile devices.
- Approved anti-malware software.
- Operating system updates.
- Automatic security patching.
- Device firewalls.
- Secure configuration standards.
- Restricted administrative privileges.
- Secure boot features where supported.

Users shall not disable endpoint security controls without written authorization.

7.7 Malware Protection

ILA shall implement measures to protect ICT systems against malicious software, including:

- Viruses.
- Worms.
- Trojans.
- Spyware.
- Adware.
- Ransomware.
- Rootkits.
- Keyloggers.

- Cryptojacking malware.

Protective measures shall include:

- Centrally managed anti-malware software.
- Automatic malware definition updates.
- Real-time protection.
- Scheduled system scans.
- Email attachment scanning.
- Web content filtering where feasible.
- Restriction of unauthorized software installations.

Any suspected malware infection shall be reported immediately, and the affected device shall be disconnected from the network until assessed by the ICT function.

7.8 Network Security

ILA shall implement appropriate safeguards to protect its networks from unauthorized access and malicious activity.

Network security controls shall include:

- Firewalls.
- Secure router configurations.
- Strong Wi-Fi encryption.
- Segregation of guest and internal networks.
- Network access controls.
- Intrusion detection or prevention solutions where feasible.
- Secure remote access.
- Regular review of network configurations.
- Logging and monitoring of critical network activities.

Wireless networks shall not operate using default passwords or insecure encryption protocols.

7.9 Vulnerability Management

The ICT function shall establish a vulnerability management programme to identify and remediate weaknesses in ICT systems.

Activities shall include:

- Periodic vulnerability assessments.
- Review of vendor security advisories.
- Timely remediation of identified vulnerabilities.
- Prioritization based on risk.
- Verification that corrective actions have been implemented.

Where practical, external vulnerability assessments or penetration testing may be conducted for internet-facing systems.

7.10 Patch Management

Operating systems, applications, firmware, and network devices shall be kept up to date.

Patch management shall include:

- Monitoring vendor updates.
- Evaluating the impact of updates.
- Testing critical updates where feasible.
- Prompt installation of security patches.
- Documentation of update activities.
- Verification of successful implementation.

Critical security patches shall be applied as soon as reasonably practicable after release, taking into account operational needs.

7.11 Email Security

Because email remains a common attack vector, ILA shall implement measures to reduce email-based threats.

Security measures shall include:

- Spam filtering.
- Phishing detection.
- Malware scanning of attachments.
- Blocking of high-risk file types where appropriate.
- Multi-factor authentication for email accounts where supported.
- Secure email configurations.
- User awareness training.

Users shall:

- Verify unexpected requests.
- Avoid opening suspicious attachments or links.
- Report suspected phishing attempts immediately.
- Confirm payment or banking instructions through an independent communication channel before acting.

7.12 Website Security

ILA's website and web applications shall be protected through appropriate security measures, including:

- Secure hosting services.
- HTTPS encryption using valid TLS certificates.
- Timely updates of content management systems, plugins, and themes.
- Strong administrator authentication.
- Regular backups.
- Restriction of administrator access.
- Monitoring for unauthorized changes.
- Removal of unused components.

Website administration shall be limited to authorized personnel.

7.13 Cloud Security

Where cloud services are used, ILA shall ensure:

- Providers meet appropriate security standards.
- Access is controlled through authorized accounts.
- Multi-factor authentication is enabled where available.
- Sensitive information is protected through encryption where feasible.
- Access rights are reviewed periodically.
- Backup and recovery arrangements are understood and tested.

Cloud services shall be approved before use for official organizational information.

7.14 Cybersecurity Monitoring

The ICT function shall monitor organizational ICT systems for indications of cybersecurity threats.

Monitoring activities may include:

- Security event logging.
- Login monitoring.
- Failed authentication monitoring.
- Malware alerts.
- Firewall logs.
- Network traffic monitoring.
- Website monitoring.
- Endpoint security alerts.
- Cloud security notifications.

Monitoring shall be conducted in a manner that respects applicable laws and legitimate privacy expectations while protecting organizational assets.

7.15 Cyber Threat Intelligence

Where appropriate, ILA shall monitor reliable sources of cybersecurity information to remain informed about emerging threats affecting its operations.

Relevant information may include:

- Vendor security bulletins.
- National cybersecurity advisories.
- Software vulnerability notifications.
- Donor security alerts.
- Trusted industry sources.

The ICT function shall assess the relevance of such information and recommend appropriate actions.

7.16 Cybersecurity Incident Response

Any suspected cybersecurity incident shall be reported immediately to the ICT function.

Examples include:

- Phishing attacks.
- Malware infections.
- Ransomware attacks.
- Unauthorized system access.
- Website defacement.
- Denial-of-service attacks.
- Password compromise.
- Data breaches.
- Loss of devices containing organizational information.

Cybersecurity incidents shall be managed in accordance with Chapter Fifteen (ICT Incident Management), including:

- Identification.
- Containment.
- Investigation.
- Eradication.
- Recovery.
- Documentation.
- Lessons learned.

7.17 Digital Forensics

Where significant cybersecurity incidents occur, ILA may undertake or commission digital forensic investigations to:

- Determine the cause of the incident.
- Preserve electronic evidence.
- Support disciplinary or legal proceedings.
- Improve cybersecurity controls.

Electronic evidence shall be collected, preserved, and handled in a manner that maintains its integrity and admissibility.

7.18 User Responsibilities

Every user shall:

- Follow organizational cybersecurity requirements.
- Protect authentication credentials.
- Install only authorized software.
- Report suspicious activities immediately.
- Lock devices when unattended.
- Avoid using unsecured public Wi-Fi for sensitive organizational activities unless protected by approved security measures.
- Complete mandatory cybersecurity awareness training.
- Cooperate with cybersecurity investigations.

7.19 Cybersecurity Awareness and Training

ILA shall conduct regular cybersecurity awareness programmes covering topics such as:

- Password security.
- Phishing and social engineering.
- Safe internet use.
- Secure handling of confidential information.
- Remote working security.
- Mobile device security.
- Incident reporting procedures.
- Emerging cyber threats.

Training shall be provided during staff induction and refreshed periodically.

7.20 Cybersecurity Audits

Periodic cybersecurity assessments shall be conducted to evaluate:

- Compliance with this Policy.
- Security configuration.
- Vulnerability management.
- Patch management.
- User awareness.
- Incident response capability.
- Network security.
- Endpoint security.
- Cloud security.
- Third-party security.

Recommendations from audits shall be documented, prioritized, and implemented within reasonable timeframes.

7.21 Non-Compliance

Failure to comply with cybersecurity requirements may result in:

- Immediate restriction of ICT access.
- Mandatory corrective training.
- Disciplinary action under the Human Resource and Administration Policy.
- Recovery of organizational losses where legally permissible.
- Termination of employment or contract where warranted.
- Referral to law enforcement where criminal conduct is suspected.

7.22 Exceptions

Any exception to this Chapter shall:

- Be documented.
- Be supported by a legitimate operational justification.
- Be approved by the Executive Director or delegated authority.
- Include compensating cybersecurity controls.
- Be reviewed periodically.

- Be reviewed periodically to determine whether the exception remains necessary.

CHAPTER EIGHT

DATA PROTECTION AND PRIVACY

8.1 Introduction

The Initiative for Legal Aid (ILA) is committed to respecting and protecting the privacy, dignity, and rights of all individuals whose personal data it collects, processes, stores, shares, or otherwise handles in the course of its operations. As a legal aid and human rights organization, ILA routinely processes sensitive information relating to beneficiaries, clients, employees, volunteers, consultants, donors, partners, witnesses, children, survivors of violence, and other vulnerable individuals. The improper handling of such information may expose individuals to harm and expose the organization to legal, financial, operational, and reputational risks.

ILA shall process personal data lawfully, fairly, transparently, securely, and only for legitimate organizational purposes. Appropriate technical and organizational measures shall be implemented to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, unauthorized access, or misuse.

This Chapter establishes the principles, responsibilities, and procedures governing the protection and privacy of personal data processed by ILA.

8.2 Objectives

The objectives of this Chapter are to:

a. Protect the privacy and personal data of beneficiaries, clients, employees, donors, partners, and other stakeholders.

b. Establish clear standards for the collection, processing, storage, sharing, retention, and disposal of personal data.

c. Promote lawful, fair, and transparent processing of personal data.

d. Minimize risks associated with unauthorized access, disclosure, alteration, or loss of personal data.

e. Strengthen organizational accountability for data protection and privacy.

f. Ensure compliance with applicable laws, contractual obligations, donor requirements, and recognized international good practices.

8.3 Scope

This Chapter applies to all personal data processed by ILA, whether in electronic, paper, audio, video, photographic, or any other format.

It applies to:

- Board Members.
- Employees.
- Volunteers.
- Interns.
- Consultants.
- Contractors.
- Service providers.
- Partner organizations processing data on behalf of ILA.
- Any person authorized to access personal data held by ILA.

8.4 Definitions

For the purposes of this Policy:

Personal Data means any information relating to an identified or identifiable natural person.

Examples include:

- Name.
- Nationality.
- Date of birth.
- Gender.
- Address.
- Telephone number.
- Email address.
- Identification number.
- Passport details.
- Employment information.
- Financial information.
- Photographs.
- Biometric information where collected.
- Location data.
- Online identifiers.

Sensitive Personal Data means personal information requiring enhanced protection due to the higher risk associated with its disclosure or misuse.

Examples include:

- Legal case information.
- Criminal records.
- Child protection information.
- Safeguarding and PSEAH reports.
- Medical information.

- Disability information.
- Bank account details.
- National identity documents.
- Witness identities.
- Information relating to survivors of violence.

8.5 Data Protection Principles

ILA shall process personal data in accordance with the following principles:

8.5.1 Lawfulness

Personal data shall only be processed where there is a lawful, legitimate, contractual, statutory, or organizational basis for doing so.

8.5.2 Fairness

Individuals shall be treated fairly, and personal data shall not be processed in a manner that is misleading, discriminatory, or abusive.

8.5.3 Transparency

Individuals shall, where appropriate, be informed about:

- What information is collected.
- Why it is collected.
- How it will be used.
- Who may receive it.
- How long it will be retained.
- Their rights concerning the information.

8.5.4 Purpose Limitation

Personal data shall only be collected for specified, explicit, and legitimate organizational purposes and shall not be processed for incompatible purposes without proper authorization or another lawful basis.

8.5.5 Data Minimization

ILA shall collect only the personal data that is necessary, relevant, and proportionate for the intended purpose.

Excessive or unnecessary collection of personal information is prohibited.

8.5.6 Accuracy

Reasonable steps shall be taken to ensure that personal data remains accurate, complete, and up to date.

Incorrect information shall be corrected promptly upon discovery.

8.5.7 Storage Limitation

Personal data shall not be retained longer than necessary for operational, legal, contractual, donor, or archival purposes.

8.5.8 Integrity and Confidentiality

Personal data shall be protected through appropriate administrative, technical, and physical safeguards against unauthorized access, disclosure, alteration, destruction, or loss.

8.5.9 Accountability

ILA shall be accountable for compliance with this Policy and shall maintain appropriate documentation demonstrating responsible data management practices.

8.6 Collection of Personal Data

Personal data shall only be collected where necessary for legitimate organizational purposes, including:

- Legal aid service delivery.
- Case management.
- Programme implementation.
- Human resource administration.
- Volunteer management.
- Financial management.
- Procurement.
- Donor reporting.
- Monitoring, Evaluation, Accountability and Learning (MEAL).
- Safeguarding.
- Security management.
- Legal compliance.

Where feasible, data shall be collected directly from the individual concerned or from an authorized representative.

8.7 Consent

Where consent is the appropriate basis for processing, it shall be:

- Freely given.

- Specific.
- Informed.
- Unambiguous.
- Documented where appropriate.

Individuals may withdraw consent at any time, subject to any legal, contractual, or operational basis that permits continued processing.

Where services are provided to children or other persons lacking legal capacity, consent shall be obtained from a parent, guardian, or other legally authorized representative where required.

8.8 Processing of Sensitive Personal Data

Sensitive personal data shall receive enhanced protection.

Processing shall be limited to authorized personnel who require access to perform official duties.

Additional safeguards may include:

- Encryption.
- Restricted access.
- Confidentiality agreements.
- Secure storage.
- Enhanced monitoring.
- Secure transmission methods.

Sensitive information shall never be disclosed without lawful authority or proper authorization.

8.9 Access to Personal Data

Access to personal data shall be granted only to authorized individuals on a need-to-know basis.

Access permissions shall:

- Reflect job responsibilities.
- Be approved by the appropriate authority.
- Be reviewed periodically.
- Be revoked promptly when no longer required.

Unauthorized access to personal data is strictly prohibited.

8.10 Sharing of Personal Data

Personal data shall only be shared where:

- There is a lawful or legitimate organizational purpose.

- Appropriate authorization has been obtained.
- The recipient has a legitimate need to receive the information.
- Confidentiality obligations are maintained.
- Adequate security measures are in place.

Data sharing with donors, government authorities, partner organizations, consultants, or service providers shall be limited to the minimum information necessary for the intended purpose.

Where appropriate, data-sharing agreements or confidentiality agreements shall be executed before sharing personal data.

8.11 Cross-Border Data Transfers

Where personal data is transferred outside South Sudan, ILA shall take reasonable steps to ensure that:

- The transfer is necessary for legitimate organizational purposes.
- Appropriate contractual or technical safeguards are implemented.
- The recipient maintains adequate security measures.
- Confidentiality obligations continue to apply.

Cloud-based services hosting data outside South Sudan shall only be used where they provide appropriate security protections.

8.12 Security of Personal Data

ILA shall implement appropriate safeguards, including:

Administrative Measures

- Policies and procedures.
- Staff training.
- Confidentiality undertakings.
- Access control procedures.
- Regular audits.

Technical Measures

- Password protection.
- Multi-factor authentication.
- Encryption.
- Firewalls.
- Anti-malware software.
- Secure backups.
- Security monitoring.
- Access logging.

Physical Measures

- Locked offices.
- Secure filing cabinets.
- Controlled server rooms.
- Visitor controls.
- Secure disposal facilities.

8.13 Data Subject Rights

Subject to applicable law and operational considerations, individuals may request to:

- Be informed about the processing of their personal data.
- Access their personal data.
- Request correction of inaccurate information.
- Request deletion where appropriate.
- Request restriction of processing where justified.
- Object to certain forms of processing where applicable.
- Withdraw consent where processing is based on consent.

ILA shall consider such requests promptly and respond in accordance with applicable legal, contractual, and operational requirements.

8.14 Personal Data Breaches

A personal data breach includes any unauthorized or accidental:

- Access.
- Disclosure.
- Alteration.
- Destruction.
- Loss.
- Theft.
- Misdirection.
- Unavailability.

Examples include:

- Sending confidential information to the wrong recipient.
- Loss of a laptop containing personal data.
- Unauthorized disclosure of beneficiary information.
- Hacking of organizational systems.
- Theft of paper files.
- Malware compromising personal information.

All suspected or confirmed breaches shall be reported immediately to the ICT function and the relevant supervisor.

8.15 Data Breach Response

Upon discovery of a data breach, ILA shall:

1. Contain the breach.
2. Assess the scope and impact.
3. Preserve relevant evidence.
4. Investigate the cause.
5. Mitigate potential harm.
6. Restore affected systems where necessary.
7. Implement corrective actions.
8. Document the incident.
9. Review lessons learned to prevent recurrence.

Where required by law, contract, or donor obligations, affected parties and relevant authorities shall be notified within the applicable timelines.

8.16 Data Retention

Personal data shall be retained only for as long as necessary to:

- Deliver services.
- Meet legal obligations.
- Fulfil contractual commitments.
- Satisfy donor requirements.
- Support audits.
- Resolve disputes.
- Protect organizational interests.

Retention periods shall be guided by ILA's Records Management Policy and any applicable legal or contractual requirements.

8.17 Secure Disposal of Personal Data

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

Approved methods include:

Electronic Data

- Secure deletion.
- Cryptographic erasure where appropriate.
- Physical destruction of storage media where necessary.

Paper Records

- Cross-cut shredding.
- Secure destruction by authorized providers.
- Incineration where appropriate and environmentally responsible.

No personal data shall be discarded through ordinary waste disposal methods.

8.18 Confidentiality Obligations

Every person handling personal data shall:

- Maintain strict confidentiality.
- Use personal data only for authorized purposes.
- Avoid discussing confidential information in public places.
- Report suspected privacy breaches immediately.
- Continue to respect confidentiality obligations even after leaving the organization.

8.19 Training and Awareness

ILA shall provide periodic training on:

- Data protection principles.
- Privacy obligations.
- Secure handling of personal data.
- Confidentiality requirements.
- Data breach reporting procedures.
- Safe use of digital technologies.
- Emerging privacy risks.

Training shall be mandatory during induction and refreshed periodically.

8.20 Monitoring and Compliance

Compliance with this Chapter shall be monitored through:

- Internal audits.
- ICT security reviews.
- Access reviews.
- Incident investigations.
- Records inspections.
- Staff awareness assessments.
- Periodic compliance monitoring.

Corrective actions shall be implemented where deficiencies are identified.

8.21 Non-Compliance

Failure to comply with this Chapter may result in:

- Mandatory retraining.
- Suspension of access to ICT systems.
- Disciplinary action under the Human Resource and Administration Policy.
- Termination of employment or contract where warranted.
- Recovery of organizational losses where legally permissible.
- Civil or criminal proceedings where required by applicable law.

8.22 Exceptions

Exceptions to this Chapter shall:

- Be documented.
- Be supported by a legitimate operational justification.
- Be approved by the Executive Director or delegated authority.
- Include appropriate safeguards to minimize privacy and security risks.
- Be reviewed periodically.

CHAPTER NINE

CLOUD COMPUTING AND DIGITAL SERVICES

9.1 Introduction

The Initiative for Legal Aid (ILA) recognizes that cloud computing and digital services enhance organizational efficiency, collaboration, mobility, scalability, and business continuity. Cloud-based technologies enable staff to securely access information, collaborate across offices and field locations, communicate effectively, and support programme implementation while reducing dependence on on-premises infrastructure.

While cloud computing offers significant operational benefits, it also introduces legal, security, privacy, contractual, and operational risks that require appropriate governance. This Chapter establishes the standards governing the acquisition, use, management, security, and monitoring of cloud services and digital platforms used by ILA.

9.2 Objectives

The objectives of this Chapter are to:

a. Promote secure and effective use of cloud computing and digital services.

b. Protect organizational information stored or processed in cloud environments.

c. Ensure cloud services comply with organizational security requirements.

d. Reduce cybersecurity, operational, and legal risks associated with cloud technologies.

e. Establish accountability for selecting, managing, and monitoring cloud service providers.

f. Support secure digital collaboration and remote working.

9.3 Scope

This Chapter applies to all cloud-based and internet-based services used by ILA, including but not limited to:

- Cloud storage services.
- Email hosting services.
- Document collaboration platforms.
- Online productivity suites.
- Case management systems.
- Financial management systems.
- Human Resource Information Systems (HRIS).
- Monitoring, Evaluation, Accountability and Learning (MEAL) platforms.
- Project management applications.
- Customer and stakeholder relationship management systems.
- Website hosting services.
- Domain name services.
- Video conferencing platforms.
- Messaging and collaboration platforms.
- Artificial Intelligence (AI) tools.
- Digital signature platforms.
- Online survey platforms.
- Any Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), or Infrastructure-as-a-Service (IaaS) solutions approved for organizational use.

9.4 Cloud Governance Principles

ILA shall manage cloud computing services in accordance with the following principles:

9.4.1 Security by Design

Security requirements shall be considered before acquiring or implementing any cloud service.

9.4.2 Risk-Based Decision Making

Cloud services shall be selected based on an assessment of operational, legal, financial, privacy, and cybersecurity risks.

9.4.3 Data Protection

Cloud providers shall maintain appropriate safeguards to protect organizational information.

9.4.4 Business Continuity

Cloud services shall support continuity of operations through appropriate backup, redundancy, and recovery capabilities.

9.4.5 Accountability

Departments using cloud services remain responsible for the information they process, regardless of where that information is hosted.

9.5 Approval of Cloud Services

No cloud service shall be used for official organizational purposes unless it has been approved by the Administration and ICT function or other designated authority.

Before approval, the following shall be considered:

- Organizational need.
- Security features.
- Privacy protections.
- Compliance with organizational policies.
- Cost effectiveness.
- Reliability.
- Vendor reputation.
- Availability of technical support.
- Backup and recovery capabilities.
- Integration with existing systems.
- Data ownership and portability.

Employees shall not independently subscribe to or use cloud services for official work without authorization.

9.6 Selection of Cloud Service Providers

When selecting cloud service providers, ILA shall evaluate factors including:

- Information security standards.
- Data encryption capabilities.
- Access control features.
- Multi-factor authentication support.

- Service availability and reliability.
- Disaster recovery capabilities.
- Data backup arrangements.
- Vendor experience and reputation.
- Technical support availability.
- Service Level Agreements (SLAs).
- Compliance with applicable legal and contractual requirements.
- Exit and data migration options.

Preference shall be given to providers with demonstrated commitment to internationally recognized information security practices.

9.7 Cloud Data Management

Organizational information stored in cloud environments shall:

- Be classified according to the Information Security Policy.
- Be accessible only to authorized users.
- Be protected against unauthorized disclosure.
- Be backed up where appropriate.
- Be recoverable in the event of service disruption.
- Be retained and disposed of in accordance with organizational records management requirements.

Users shall avoid storing organizational information in personal cloud accounts.

9.8 User Access to Cloud Services

Access to cloud services shall be managed in accordance with Chapter Five (User Access Management).

The ICT function shall ensure:

- User accounts are approved before activation.
- Access is based on job responsibilities.
- Multi-factor authentication is enabled where available.
- Dormant accounts are disabled.
- Access rights are reviewed periodically.
- Accounts are promptly deactivated upon staff separation.

Sharing login credentials is strictly prohibited.

9.9 Collaboration Platforms

Approved collaboration platforms may be used for:

- Internal communication.
- Document sharing.
- Team collaboration.
- Programme coordination.
- Virtual meetings.
- Task management.
- Knowledge sharing.

Users shall:

- Maintain professional conduct.
- Protect confidential information.
- Verify participant identities before sharing sensitive information.
- Avoid uploading confidential information to unapproved platforms.

9.10 Video Conferencing

Video conferencing platforms shall be used responsibly.

Meeting organizers shall:

- Use organizational accounts where available.
- Restrict meeting access to invited participants.
- Protect meetings using passwords or waiting rooms where appropriate.
- Control screen sharing permissions.
- Record meetings only where necessary and authorized.
- Inform participants when meetings are being recorded.

Confidential discussions shall not be conducted over insecure or unauthorized platforms.

9.11 Artificial Intelligence (AI) Tools

ILA recognizes the potential benefits of Artificial Intelligence (AI) tools in improving efficiency, legal research, document drafting, translation, data analysis, and administrative support. However, AI tools also present risks relating to confidentiality, privacy, accuracy, intellectual property, and bias.

Accordingly:

a. AI tools may only be used for legitimate organizational purposes.

b. Users shall not input confidential, privileged, or highly sensitive organizational information into publicly accessible AI platforms unless the platform has been approved for such use and appropriate safeguards are in place.

c. AI-generated outputs shall be reviewed by a competent human before being relied upon for legal advice, policy decisions, financial reporting, programme implementation, or external communications.

d. AI shall not replace professional judgment, legal analysis, or management decision-making.

e. AI-generated content must be verified for factual accuracy, legal compliance, and consistency with organizational standards.

f. The use of AI must comply with applicable laws, donor requirements, confidentiality obligations, and this Policy.

9.12 Digital Signatures and Electronic Documents

Electronic signatures may be used where:

- Permitted by applicable law.
- Accepted by contractual parties.
- Approved by management.
- Appropriate identity verification measures are in place.

Digital documents shall be protected against unauthorized alteration and stored securely.

9.13 Third-Party Applications

Before integrating third-party applications with organizational systems:

- Security risks shall be assessed.
- Necessary approvals shall be obtained.
- Access permissions shall be limited.
- Data-sharing implications shall be evaluated.
- Contracts shall include appropriate confidentiality and security provisions where applicable.

Unused integrations shall be removed promptly.

9.14 Cloud Security Controls

ILA shall implement appropriate security controls for cloud services, including:

- Strong authentication.
- Multi-factor authentication.
- Encryption of data in transit and, where supported, at rest.
- Access logging.
- Role-based access controls.

- Security monitoring.
- Backup verification.
- Secure configuration.
- Periodic access reviews.
- Prompt application of security updates where applicable.

9.15 Backup and Recovery

Critical cloud-based information shall be backed up in accordance with the organization's Backup and Disaster Recovery procedures.

Where feasible:

- Recovery procedures shall be tested periodically.
- Backup integrity shall be verified.
- Recovery time objectives shall be defined for critical systems.
- Data restoration processes shall be documented.

9.16 Vendor Management

The Administration and ICT function shall maintain oversight of cloud service providers by monitoring:

- Service performance.
- Security incidents.
- Service availability.
- Contract compliance.
- Licence renewals.
- Subscription costs.
- Vendor support responsiveness.
- Compliance with agreed service levels.

Significant vendor risks shall be reported to Senior Management.

9.17 Termination of Cloud Services

When discontinuing a cloud service, ILA shall ensure that:

- Organizational data is securely retrieved or migrated.
- User accounts are deactivated.
- Access permissions are revoked.
- Confidential information is securely deleted from the provider's environment where contractually and technically feasible.
- Subscriptions and licences are cancelled.
- Service termination is documented.

9.18 User Responsibilities

Users of cloud services shall:

- Use only approved cloud platforms.
- Protect login credentials.
- Enable multi-factor authentication where available.
- Avoid storing organizational information in personal cloud accounts.
- Verify recipients before sharing cloud-based documents.
- Report suspected cloud security incidents immediately.
- Comply with organizational information security requirements.

9.19 Monitoring and Compliance

The Administration and ICT function shall periodically monitor:

- Cloud service usage.
- User access.
- Security alerts.
- Subscription management.
- Licence compliance.
- Storage utilization.
- Unauthorized cloud applications ("shadow IT").
- Compliance with this Policy.

Corrective actions shall be implemented where necessary.

9.20 Non-Compliance

Failure to comply with this Chapter may result in:

- Suspension of access to cloud services.
- Removal of unauthorized applications.
- Mandatory retraining.
- Disciplinary action under the Human Resource and Administration Policy.
- Recovery of organizational losses where legally permissible.
- Termination of employment or contract where warranted.
- Legal action where appropriate.

9.21 Exceptions

Any exception to this Chapter shall:

- Be documented in writing.
- Be justified by a legitimate operational need.
- Be approved by the Executive Director or delegated authority.

- Include compensating security controls.
- Be reviewed periodically to ensure continued necessity.

CHAPTER TEN

BUSINESS CONTINUITY AND DISASTER RECOVERY

10.1 Introduction

The Initiative for Legal Aid (ILA) recognizes that interruptions to Information and Communication Technology (ICT) services may significantly affect legal aid service delivery, programme implementation, financial management, human resource administration, communications, donor reporting, and organizational governance. Such interruptions may result from cyberattacks, power failures, hardware or software failures, telecommunications outages, natural disasters, fire, theft, vandalism, civil unrest, human error, or other unforeseen events.

ILA is committed to maintaining the resilience of its ICT environment by implementing effective Business Continuity Management (BCM) and Disaster Recovery (DR) measures. The organization shall establish procedures to ensure that critical ICT services can continue during disruptions and that systems and data can be restored within acceptable timeframes following an incident.

This Chapter establishes the framework for preventing, preparing for, responding to, and recovering from ICT-related disruptions.

10.2 Objectives

The objectives of this Chapter are to:

a. Ensure continuity of critical ICT services during disruptions.

b. Minimize operational downtime and data loss.

c. Protect critical organizational information and ICT infrastructure.

d. Establish clear procedures for disaster response and system recovery.

e. Define responsibilities for business continuity and disaster recovery activities.

f. Promote organizational resilience against operational, technological, environmental, and cybersecurity threats.

g. Ensure periodic testing and continuous improvement of continuity and recovery arrangements.

10.3 Scope

This Chapter applies to all ICT systems, facilities, information assets, personnel, and service providers supporting ILA's operations, including:

- Computer systems.
- Servers.
- Networks.
- Internet services.
- Email systems.
- Cloud platforms.
- Data storage systems.
- Backup infrastructure.
- Power supply systems.
- Communication systems.
- Digital records.
- Websites.
- Mobile technologies.
- Third-party hosted services.

10.4 Business Continuity Principles

ILA shall implement Business Continuity Management based on the following principles:

10.4.1 Preparedness

The organization shall proactively identify risks and prepare for potential disruptions before they occur.

10.4.2 Resilience

Critical services shall be designed and managed to continue operating despite disruptions wherever reasonably practicable.

10.4.3 Rapid Recovery

ICT systems shall be restored as quickly as possible following an incident to minimize operational impacts.

10.4.4 Continuous Improvement

Business continuity and disaster recovery arrangements shall be reviewed and improved regularly based on experience, testing, audits, and changing risks.

10.4.5 Shared Responsibility

Business continuity is the responsibility of management, the ICT function, all employees, and relevant service providers.

10.5 Business Impact Analysis (BIA)

ILA shall periodically conduct a Business Impact Analysis to identify:

- Critical organizational functions.
- Essential ICT systems.
- Critical business processes.
- Key information assets.
- Maximum acceptable downtime.
- Dependencies between systems and services.
- Recovery priorities.
- Potential operational, legal, financial, and reputational impacts of disruptions.

The results of the Business Impact Analysis shall guide continuity planning and resource allocation.

10.6 Risk Assessment

The ICT function shall periodically assess risks that may affect the availability of ICT services, including:

- Cyberattacks.
- Ransomware.
- Malware.
- Hardware failures.
- Software failures.
- Internet service interruptions.
- Electrical power failures.
- Fire.
- Flooding.
- Theft.
- Civil unrest.
- Human error.
- Third-party service failures.
- Supply chain disruptions.
- Environmental hazards.

Appropriate preventive and mitigating measures shall be implemented based on the assessed level of risk.

10.7 Business Continuity Plan

ILA shall maintain a documented Business Continuity Plan (BCP) that includes:

- Continuity objectives.
- Roles and responsibilities.
- Incident response procedures.
- Emergency communication arrangements.
- Critical business processes.
- Alternative working arrangements.
- Contact lists.
- Resource requirements.
- Recovery priorities.
- Escalation procedures.
- Coordination with service providers.
- Plan review procedures.

The Business Continuity Plan shall be reviewed at least annually and after any significant incident.

10.8 Disaster Recovery Plan

ILA shall maintain a Disaster Recovery Plan (DRP) for ICT systems.

The Disaster Recovery Plan shall include:

- Recovery procedures for critical systems.
- Backup restoration procedures.
- System recovery priorities.
- Recovery responsibilities.
- Recovery checklists.
- Alternative operating arrangements.
- Technical recovery procedures.
- Communication protocols.
- Vendor contact information.
- Recovery testing schedules.

The Disaster Recovery Plan shall be maintained securely and be accessible to authorized personnel during emergencies.

10.9 Backup Management

Regular backups are essential for protecting organizational information against accidental loss, system failures, cyber incidents, and disasters.

ILA shall ensure that:

- Critical organizational data is backed up regularly.
- Backup schedules are documented.
- Backup processes are automated where feasible.
- Backup integrity is periodically verified.
- Multiple backup generations are maintained where appropriate.
- Backup failures are investigated promptly.

Backups shall include, as appropriate:

- Databases.
- Financial records.
- Human resource records.
- Legal case files.
- Programme documentation.
- Email systems.
- Website data.
- Cloud-based information.
- Configuration files.
- Shared network drives.

10.10 Backup Storage

Backups shall be protected against unauthorized access, loss, theft, fire, and other hazards.

Where practicable:

- At least one backup copy shall be maintained separately from the primary systems.
- Backup media shall be encrypted where appropriate.
- Access to backups shall be restricted to authorized personnel.
- Cloud backups shall utilize approved providers.
- Physical backup media shall be stored in secure environments.

10.11 Recovery Objectives

Recovery priorities shall be established based on operational needs.

The ICT function shall define:

Recovery Time Objective (RTO)

The maximum acceptable period within which a system or service should be restored after disruption.

Recovery Point Objective (RPO)

The maximum acceptable amount of data loss measured by the time between the last successful backup and the disruption.

Recovery objectives shall be reviewed periodically and aligned with organizational priorities.

10.12 Emergency Communications

During significant ICT disruptions, ILA shall establish effective communication with:

- Employees.
- Management.
- Board of Directors where appropriate.
- Beneficiaries where necessary.
- Donors where required.
- Service providers.
- Regulatory authorities where applicable.
- Law enforcement where appropriate.

Emergency communications shall be accurate, timely, coordinated, and approved by the appropriate authority.

10.13 Alternative Working Arrangements

Where ICT services become unavailable, ILA may implement alternative arrangements including:

- Remote working.
- Temporary relocation.
- Manual business processes.
- Use of backup equipment.
- Alternative communication channels.
- Temporary service providers.
- Alternative internet connections.

Alternative arrangements shall maintain appropriate information security controls.

10.14 Power Continuity

Where feasible, critical ICT infrastructure shall be supported by appropriate power continuity measures, including:

- Uninterruptible Power Supply (UPS) units.
- Surge protection.
- Backup generators.

- Battery backup systems.
- Voltage regulation equipment.

Critical equipment shall be prioritized during power interruptions.

10.15 Recovery of ICT Infrastructure

Following a disaster or major incident, recovery activities may include:

- Restoration of electrical power.
- Network restoration.
- Server recovery.
- Workstation restoration.
- Database restoration.
- Email service recovery.
- Website restoration.
- Cloud service verification.
- Security validation.
- User access restoration.
- System functionality testing.

Recovery activities shall be documented.

10.16 Testing of Business Continuity and Disaster Recovery Plans

Business continuity and disaster recovery arrangements shall be tested periodically.

Testing may include:

- Tabletop exercises.
- Simulation exercises.
- Backup restoration testing.
- Disaster recovery drills.
- Cyber incident simulations.
- Emergency communication exercises.
- System failover testing where applicable.

Lessons learned shall be documented and incorporated into future improvements.

10.17 Roles and Responsibilities

Board of Directors

The Board shall:

- Provide oversight of organizational resilience.
- Ensure appropriate resources are allocated for business continuity.

Executive Director

The Executive Director shall:

- Approve continuity and disaster recovery plans.
- Coordinate organizational response to major disruptions.
- Ensure continuity arrangements are implemented.

Administration and ICT Function

The ICT function shall:

- Develop and maintain continuity and recovery plans.
- Perform backups.
- Test recovery procedures.
- Restore ICT systems.
- Maintain recovery documentation.
- Coordinate technical recovery activities.

Department Heads

Department Heads shall:

- Identify critical business functions.
- Support continuity planning.
- Ensure staff understand continuity procedures.

Employees

Employees shall:

- Follow continuity procedures.
- Protect organizational information during disruptions.
- Participate in continuity training and exercises.
- Report incidents promptly.

10.18 Documentation

The following documentation shall be maintained:

- Business Continuity Plan.
- Disaster Recovery Plan.
- ICT Asset Register.
- Backup Register.
- Emergency Contact List.
- Vendor Contact List.
- Recovery Checklists.
- Recovery Test Reports.
- Incident Reports.
- Lessons Learned Register.

Documentation shall be reviewed and updated regularly.

10.19 Monitoring and Review

The Administration and ICT function shall periodically review:

- Backup success rates.
- Recovery testing results.
- Incident trends.
- Continuity risks.
- Recovery performance.
- Vendor readiness.
- Infrastructure resilience.

Recommendations shall be implemented to strengthen organizational preparedness.

10.20 Non-Compliance

Failure to comply with this Chapter may result in:

- Corrective action.
- Mandatory retraining.
- Restriction of ICT privileges where appropriate.
- Disciplinary action under the Human Resource and Administration Policy.
- Recovery of losses where legally permissible.
- Contract termination where applicable.

10.21 Exceptions

Any exception to this Chapter shall:

- Be documented in writing.
- Be supported by a legitimate operational need.
- Be approved by the Executive Director or delegated authority.
- Include appropriate risk mitigation measures.
- Be reviewed periodically.

CHAPTER ELEVEN

SOFTWARE MANAGEMENT

11.1 Introduction

Software is a critical organizational asset that enables the Initiative for Legal Aid (ILA) to deliver legal aid services, manage programmes, administer finances, support human resources, communicate with stakeholders, and maintain organizational records. Improper acquisition, installation, licensing, configuration, or use of software can expose the organization to cybersecurity threats, legal liability, operational disruption, financial losses, and reputational damage.

ILA is committed to ensuring that all software used within the organization is properly authorized, legally licensed, securely configured, maintained, and monitored throughout its lifecycle.

This Chapter establishes the framework governing the procurement, installation, use, maintenance, licensing, monitoring, and disposal of software used by ILA.

11.2 Objectives

The objectives of this Chapter are to:

a. Ensure all software used by ILA is authorized and legally licensed.

b. Protect ICT systems from vulnerabilities associated with unauthorized or insecure software.

c. Establish standardized procedures for software acquisition, deployment, maintenance, and retirement.

d. Promote compliance with intellectual property and licensing obligations.

e. Reduce cybersecurity and operational risks associated with software management.

f. Ensure software supports organizational efficiency, security, and sustainability.

11.3 Scope

This Chapter applies to all software used by ILA, including:

- Operating systems.
- Office productivity software.
- Financial management systems.
- Human Resource Information Systems (HRIS).
- Legal case management systems.
- Monitoring, Evaluation, Accountability and Learning (MEAL) systems.
- Procurement systems.
- Database applications.
- Antivirus software.
- Website management software.
- Mobile applications.
- Cloud-based software (SaaS).
- Open-source software.
- Utility software.
- Collaboration platforms.
- Artificial Intelligence (AI) applications.
- Software installed on desktops, laptops, servers, tablets, and mobile devices.

11.4 Software Management Principles

ILA shall manage software in accordance with the following principles:

11.4.1 Authorization

Only approved software shall be installed or used for official organizational purposes.

11.4.2 Legal Compliance

Software shall be acquired and used in compliance with applicable licensing agreements and intellectual property laws.

11.4.3 Security

Software shall be evaluated for security risks before implementation and maintained through timely updates and patches.

11.4.4 Standardization

Where practicable, ILA shall standardize software platforms to improve compatibility, security, user support, and cost efficiency.

11.4.5 Lifecycle Management

Software shall be managed throughout its lifecycle from acquisition to secure retirement.

11.5 Software Acquisition

Software may only be acquired through approved procurement procedures.

Before acquiring software, the Administration and ICT function shall consider:

- Organizational requirements.
- Security features.
- Licensing terms.
- Compatibility with existing systems.
- Vendor reputation.
- Technical support availability.
- Cost-effectiveness.
- Scalability.
- Maintenance requirements.
- Data protection implications.
- Business continuity considerations.

Departments shall not independently purchase or subscribe to software without prior approval.

11.6 Software Approval

Before installation, software shall be reviewed and approved by the Administration and ICT function.

Approval shall consider:

- Business need.
- Security risks.
- Legal licensing requirements.
- Compatibility.
- Resource requirements.
- Privacy implications.
- Integration with existing ICT infrastructure.

Software that has not been approved shall not be installed on organizational devices.

11.7 Software Installation

Only authorized ICT personnel or designated administrators may install, configure, modify, or uninstall software on organizational ICT equipment.

Users shall not:

- Install software independently.
- Disable security controls during installation.
- Install software from untrusted websites.
- Install cracked, pirated, or illegally modified software.
- Circumvent software licensing restrictions.

Installation activities shall be documented where appropriate.

11.8 Software Licensing

ILA shall maintain valid licences for all commercial software used within the organization.

The Administration and ICT function shall maintain a Software Licence Register containing, where applicable:

- Software name.
- Version.
- Vendor.
- Licence type.
- Licence key or subscription details.
- Number of authorized users or devices.
- Purchase date.
- Renewal date.
- Responsible department.

Software shall not be used beyond the scope permitted by its licence.

11.9 Open-Source Software

ILA may use open-source software where appropriate.

Before adoption, open-source software shall be evaluated for:

- Security.
- Stability.
- Community support.
- Compatibility.
- Maintenance requirements.
- Licensing obligations.
- Long-term sustainability.

Open-source software shall not be adopted without approval from the Administration and ICT function.

11.10 Software Updates and Patch Management

Software shall be kept current to reduce security vulnerabilities and improve functionality.

The Administration and ICT function shall:

- Monitor software updates.
- Apply security patches promptly.
- Test significant updates where feasible.
- Document major upgrades.
- Remove unsupported software from production environments.

Users shall not disable automatic updates without authorization.

11.11 Unsupported and End-of-Life Software

Software that is no longer supported by its vendor presents significant security risks.

Accordingly:

- End-of-life software shall be identified.
- Risk assessments shall be conducted.
- Replacement or upgrade plans shall be developed.
- Unsupported software shall be removed or isolated where continued use is temporarily unavoidable.

Temporary continued use shall require documented approval and compensating security controls.

11.12 Mobile Applications

Only approved mobile applications may be used to process, access, or store official organizational information.

Applications shall:

- Be downloaded from trusted sources.
- Receive regular updates.
- Comply with organizational security requirements.
- Protect confidential information.

Applications requiring excessive permissions or posing security risks shall not be used.

11.13 Artificial Intelligence (AI) Applications

The use of AI applications shall comply with Chapter Nine (Cloud Computing and Digital Services).

In addition:

- AI-generated outputs shall be reviewed by qualified personnel before official use.
- AI shall not be used to generate legal opinions, financial decisions, or policy positions without human review and approval.
- Confidential or privileged information shall not be entered into unapproved AI platforms.
- AI-assisted work shall meet the same standards of accuracy, ethics, confidentiality, and professionalism as work produced without AI.

11.14 Software Asset Management

ILA shall maintain an accurate inventory of software assets.

The Software Asset Register shall include:

- Installed software.
- Licence information.
- Assigned users.
- Assigned devices.
- Version numbers.
- Installation dates.
- Renewal schedules.
- Support status.
- Responsible departments.

Periodic software audits shall be conducted to verify compliance.

11.15 Software Security

Appropriate safeguards shall be implemented to protect software from unauthorized access or modification.

These safeguards include:

- Access controls.
- Role-based permissions.
- Multi-factor authentication where available.
- Secure configuration.
- Audit logging.
- Anti-malware protection.
- Encryption where appropriate.
- Regular vulnerability assessments.

Critical software systems shall be monitored for security incidents.

11.16 Software Testing

Before introducing new software into production, appropriate testing shall be conducted to verify:

- Functionality.
- Security.
- Compatibility.
- Performance.
- Reliability.
- Data integrity.
- User acceptance where appropriate.

Testing shall be proportionate to the complexity and criticality of the software.

11.17 Software Retirement

When software is no longer required:

- User access shall be removed.
- Data shall be securely migrated where necessary.
- Licences shall be cancelled or reassigned where permitted.
- Software shall be uninstalled.
- Related accounts shall be deactivated.
- Residual organizational data shall be securely deleted in accordance with the Records Management and Information Security Policies.

Retirement activities shall be documented.

11.18 Vendor Management

Software vendors shall be monitored to ensure:

- Continued service availability.
- Security updates.
- Technical support.
- Licence compliance.
- Contract performance.
- Renewal management.

Vendor risks shall be periodically reviewed.

11.19 User Responsibilities

Every user shall:

- Use only approved software.
- Report software malfunctions promptly.
- Avoid installing unauthorized applications.
- Protect software licences and activation credentials.
- Comply with licensing conditions.
- Report suspected software vulnerabilities or security issues immediately.

11.20 Monitoring and Compliance

The Administration and ICT function shall monitor compliance through:

- Software inventories.
- Licence audits.
- Security assessments.
- Patch management reviews.
- Configuration reviews.
- Device inspections.
- Internal ICT audits.

Corrective actions shall be implemented where non-compliance is identified.

11.21 Non-Compliance

Failure to comply with this Chapter may result in:

- Removal of unauthorized software.
- Suspension of ICT access.
- Mandatory retraining.
- Disciplinary action under the Human Resource and Administration Policy.
- Recovery of financial losses where legally permissible.
- Termination of employment or contract where warranted.
- Civil or criminal proceedings where applicable.

11.22 Exceptions

Exceptions to this Chapter shall:

- Be documented.
- Be supported by a legitimate operational need.
- Be approved by the Executive Director or delegated authority.
- Include appropriate risk mitigation measures.
- Be subject to periodic review.

CHAPTER TWELVE

ICT ASSET MANAGEMENT

12.1 Introduction

Information and Communication Technology (ICT) assets are essential resources that enable the Initiative for Legal Aid (ILA) to deliver legal aid services, implement programmes, manage operations, safeguard information, and support organizational governance. ICT assets represent a significant organizational investment and require effective management throughout their lifecycle to maximize value, maintain operational efficiency, protect information security, and ensure accountability.

ILA shall establish and maintain a comprehensive ICT Asset Management framework covering the planning, acquisition, registration, deployment, maintenance, transfer, inventory, disposal, and audit of all ICT assets. This Chapter complements the Procurement and Asset Management Policy by providing ICT-specific requirements and controls.

12.2 Objectives

The objectives of this Chapter are to:

a. Ensure ICT assets are acquired, used, maintained, and disposed of efficiently and responsibly.

b. Protect ICT assets against loss, theft, damage, misuse, and unauthorized use.

c. Establish accountability for ICT assets assigned to employees and other authorized users.

d. Maintain accurate records of ICT assets throughout their lifecycle.

e. Support effective budgeting, maintenance planning, and asset replacement.

f. Promote compliance with procurement, financial management, and information security requirements.

12.3 Scope

This Chapter applies to all ICT assets owned, leased, donated, or otherwise managed by ILA, including:

- Desktop computers.
- Laptop computers.
- Servers.
- Tablets.

- Mobile phones.
- Printers.
- Scanners.
- Photocopiers.
- Projectors.
- Network equipment.
- Routers.
- Switches.
- Firewalls.
- Wireless access points.
- External storage devices.
- Backup devices.
- CCTV equipment.
- Video conferencing equipment.
- Software licences.
- Cloud service subscriptions.
- Peripherals.
- Accessories.
- Any other ICT-related equipment or digital asset.

12.4 ICT Asset Management Principles

ILA shall manage ICT assets in accordance with the following principles:

12.4.1 Accountability

Every ICT asset shall have a designated custodian responsible for its proper use and care.

12.4.2 Lifecycle Management

ICT assets shall be managed from planning and acquisition through deployment, maintenance, transfer, replacement, and disposal.

12.4.3 Value for Money

ICT assets shall be acquired and managed in a cost-effective manner that supports organizational objectives.

12.4.4 Security

ICT assets shall be protected against unauthorized access, theft, misuse, and damage.

12.4.5 Accuracy

Complete and accurate records of ICT assets shall be maintained at all times.

12.5 ICT Asset Planning

The Administration and ICT function shall identify ICT asset requirements based on:

- Strategic objectives.
- Programme needs.
- Staffing requirements.
- Operational priorities.
- Budget availability.
- Technology lifecycle considerations.
- Business continuity requirements.
- Security requirements.

Annual ICT asset plans shall inform procurement and budgeting processes.

12.6 Acquisition of ICT Assets

ICT assets shall be acquired through the procedures established in the Procurement and Asset Management Policy.

Before acquisition, consideration shall be given to:

- Organizational needs.
- Technical specifications.
- Compatibility.
- Security features.
- Warranty coverage.
- Vendor support.
- Energy efficiency.
- Total cost of ownership.
- Scalability.
- Expected useful life.

Only authorized procurement processes shall be used.

12.7 ICT Asset Registration

Every ICT asset shall be recorded in the ICT Asset Register immediately upon acquisition.

The ICT Asset Register shall include, where applicable:

- Asset identification number.
- Asset description.
- Asset category.
- Manufacturer.
- Model.

- Serial number.
- Purchase date.
- Purchase cost.
- Supplier.
- Warranty details.
- Location.
- Assigned custodian.
- Department.
- Asset condition.
- Expected useful life.
- Maintenance history.
- Disposal status.

Asset records shall be maintained accurately and updated promptly.

12.8 Asset Identification and Labelling

Each ICT asset shall be assigned a unique asset identification number.

Where practical, assets shall bear durable labels indicating:

- Asset number.
- Organizational ownership.
- Inventory reference.

Labels shall not be removed or altered without authorization.

12.9 Assignment of ICT Assets

ICT assets shall be assigned only to authorized users for official organizational purposes.

Before receiving an ICT asset, the recipient shall:

- Sign an ICT Asset Handover Form.
- Acknowledge responsibility for the asset.
- Comply with applicable ICT policies.
- Report any defects immediately.

Assignment records shall be maintained by the Administration and ICT function.

12.10 Responsibilities of Asset Custodians

Users assigned ICT assets shall:

- Exercise reasonable care.
- Protect assets from theft and damage.

- Use assets only for authorized purposes.
- Prevent unauthorized use.
- Keep devices physically secure.
- Report faults promptly.
- Report loss or theft immediately.
- Return assets upon request or separation from the organization.
- Comply with all ICT security requirements.

Users shall not lend assigned ICT assets to unauthorized persons without approval.

12.11 ICT Asset Maintenance

ICT assets shall receive appropriate preventive and corrective maintenance to maximize their useful life.

Maintenance activities may include:

- Software updates.
- Security patching.
- Hardware inspections.
- Cleaning.
- Battery replacement.
- Antivirus updates.
- Hardware repairs.
- Performance optimization.
- Warranty servicing.

Maintenance records shall be documented.

12.12 Repairs

Where ICT equipment becomes defective:

- Users shall report faults immediately.
- Unauthorized repairs shall not be undertaken.
- Repairs shall be performed only by authorized personnel or approved service providers.
- Warranty conditions shall be observed.
- Repairs shall be recorded in the maintenance history.

Where equipment cannot be economically repaired, replacement or disposal procedures shall be initiated.

12.13 ICT Asset Transfers

Transfers of ICT assets between users, departments, or locations shall:

- Be authorized.
- Be documented using an ICT Asset Transfer Form.
- Update the ICT Asset Register.
- Include verification of asset condition.

The receiving custodian shall assume responsibility upon completion of the transfer.

12.14 Temporary Loans

Temporary allocation of ICT assets may be approved for:

- Official travel.
- Field activities.
- Training.
- Conferences.
- Remote working.
- Emergency operational requirements.

Temporary loans shall:

- Be documented.
- Specify the loan period.
- Identify the responsible custodian.
- Require return upon completion of the authorized activity.

12.15 ICT Asset Inventory

The Administration and ICT function shall conduct periodic physical verification of ICT assets.

Inventory verification shall include:

- Confirmation of asset location.
- Verification of assigned custodian.
- Assessment of asset condition.
- Verification of asset labels.
- Identification of missing assets.
- Identification of obsolete assets.
- Reconciliation with the ICT Asset Register.

A comprehensive inventory shall be conducted at least annually.

12.16 Loss, Theft, or Damage

Any loss, theft, or significant damage to an ICT asset shall be reported immediately to:

- The immediate supervisor.
- The Administration and ICT function.
- Security personnel where applicable.

The organization may conduct investigations to determine the circumstances of the incident and identify appropriate corrective actions.

Where negligence or misconduct is established, disciplinary or recovery measures may be taken in accordance with applicable policies and laws.

12.17 Return of ICT Assets

ICT assets shall be returned:

- Upon resignation.
- Upon retirement.
- Upon termination of employment.
- Upon expiry of a consultancy or contract.
- Upon transfer where reassignment is required.
- Upon replacement of equipment.
- Whenever requested by management.

Returned assets shall be inspected, documented, and recorded using the ICT Asset Return Form.

12.18 Disposal of ICT Assets

ICT assets shall only be disposed of in accordance with the Procurement and Asset Management Policy and applicable legal requirements.

Approved disposal methods may include:

- Transfer to another department.
- Donation, where authorized.
- Trade-in.
- Sale through approved procedures.
- Recycling.
- Environmentally responsible destruction.

Before disposal:

- All organizational data shall be securely erased or destroyed.
- Asset records shall be updated.

- Licences or subscriptions shall be cancelled or transferred where appropriate.

12.19 Environmentally Responsible Disposal

ILA is committed to environmentally responsible management of electronic waste (e-waste).

Where practicable:

- Electronic waste shall be recycled through authorized service providers.
- Hazardous components shall be disposed of safely.
- Reusable components may be recovered where appropriate.
- Applicable environmental laws and regulations shall be observed.

12.20 ICT Asset Audits

Periodic ICT asset audits shall be conducted to:

- Verify inventory accuracy.
- Confirm asset utilization.
- Identify missing assets.
- Detect unauthorized assets.
- Assess maintenance practices.
- Support financial reporting.
- Improve asset management controls.

Audit findings shall be documented and corrective actions implemented.

12.21 Roles and Responsibilities

Board of Directors

The Board shall provide oversight of ICT asset governance through approval of policies and monitoring of significant asset investments.

Executive Director

The Executive Director shall:

- Approve major ICT asset acquisitions.
- Ensure adequate resources for ICT asset management.
- Support implementation of this Chapter.

Administration and ICT Function

The Administration and ICT function shall:

- Maintain the ICT Asset Register.
- Coordinate asset acquisition and deployment.
- Conduct inventories.
- Arrange maintenance and repairs.
- Maintain asset documentation.
- Coordinate asset disposal.
- Monitor compliance with this Chapter.

Department Heads

Department Heads shall:

- Ensure ICT assets are used responsibly within their departments.
- Notify the ICT function of staffing changes affecting asset assignments.
- Support inventory verification.

Asset Custodians

Every asset custodian shall:

- Safeguard assigned assets.
- Report incidents promptly.
- Comply with organizational ICT policies.
- Return assets when required.

12.22 Monitoring and Compliance

Compliance with this Chapter shall be monitored through:

- Asset inventories.
- Internal audits.
- Spot inspections.
- Maintenance reviews.
- Asset reconciliation exercises.
- Financial audits.
- Procurement reviews.

Non-compliance shall be addressed through corrective action, retraining, or disciplinary measures as appropriate.

12.23 Non-Compliance

Failure to comply with this Chapter may result in:

- Withdrawal of ICT equipment.
- Suspension of ICT privileges.
- Mandatory corrective training.
- Disciplinary action under the Human Resource and Administration Policy.
- Recovery of losses where legally permissible.
- Termination of employment or contract where warranted.
- Referral to law enforcement where criminal conduct is suspected.

12.24 Exceptions

Any exception to this Chapter shall:

- Be documented.
- Be supported by a legitimate operational justification.
- Be approved by the Executive Director or delegated authority.
- Include appropriate compensating controls.
- Be reviewed periodically.

CHAPTER THIRTEEN

ICT PROCUREMENT AND VENDOR MANAGEMENT

13.1 Introduction

The Initiative for Legal Aid (ILA) recognizes that the effective procurement of Information and Communication Technology (ICT) goods and services is essential to achieving organizational objectives, maintaining secure and reliable ICT operations, and ensuring value for money. ICT procurement differs from general procurement because it involves specialized technical requirements, cybersecurity considerations, software licensing, interoperability, maintenance, and long-term vendor support.

ILA shall ensure that all ICT procurement is conducted transparently, competitively, ethically, and in accordance with the Procurement and Asset Management Policy, Financial and Accounting Policy, applicable laws, donor requirements, and this ICT Policy.

This Chapter establishes the framework for planning, procuring, managing, monitoring, and evaluating ICT suppliers, contractors, consultants, and service providers.

13.2 Objectives

The objectives of this Chapter are to:

a. Ensure ICT goods and services meet organizational requirements.

b. Promote transparent, competitive, and cost-effective ICT procurement.

c. Minimize legal, operational, financial, and cybersecurity risks associated with ICT vendors.

d. Establish standards for vendor selection, contract management, and performance monitoring.

e. Ensure ICT suppliers comply with ILA's information security, confidentiality, and data protection requirements.

f. Promote long-term sustainability and value throughout the lifecycle of ICT investments.

13.3 Scope

This Chapter applies to the procurement and management of:

- Computer hardware.
- Servers.
- Networking equipment.
- Software.
- Cloud services.
- Internet services.
- Website development and hosting.
- Cybersecurity solutions.
- ICT consultancy services.
- ICT maintenance services.
- Mobile communication services.
- Data recovery services.
- ICT training services.
- Technical support contracts.
- Managed ICT services.
- Software subscriptions.
- Digital platforms.
- Artificial Intelligence (AI) services.
- Any other ICT-related goods or services.

13.4 Guiding Principles

ICT procurement and vendor management shall be guided by the following principles:

13.4.1 Transparency

Procurement decisions shall be documented, objective, and capable of independent review.

13.4.2 Value for Money

ICT investments shall achieve the optimum balance between cost, quality, security, functionality, sustainability, and long-term support.

13.4.3 Fair Competition

Qualified suppliers shall be provided with fair opportunities to compete, consistent with the Procurement and Asset Management Policy.

13.4.4 Security by Design

Security requirements shall be incorporated into procurement specifications and vendor selection processes.

13.4.5 Accountability

Procurement responsibilities shall be clearly assigned and subject to appropriate oversight.

13.5 ICT Procurement Planning

ICT procurement shall be based on approved organizational needs.

Annual ICT procurement planning shall consider:

- Strategic priorities.
- Programme requirements.
- Asset replacement schedules.
- Staffing requirements.
- Business continuity needs.
- Information security requirements.
- Budget availability.
- Technology trends.
- Donor-funded projects.
- Existing ICT infrastructure.

Unplanned procurement shall be minimized and require appropriate justification and approval.

13.6 Technical Specifications

Technical specifications shall be prepared before initiating procurement.

Specifications shall:

- Be clear and objective.
- Avoid unnecessary restrictions on competition.
- Reflect operational needs.
- Include cybersecurity requirements.
- Address compatibility with existing ICT systems.
- Consider scalability and future expansion.
- Include maintenance and warranty requirements where appropriate.

Technical specifications shall not be drafted to unfairly favor a particular supplier unless justified by compatibility or other legitimate operational reasons.

13.7 Vendor Selection

ICT suppliers shall be evaluated using criteria that may include:

- Technical capability.
- Relevant experience.
- Financial stability.
- Security practices.
- Quality of products or services.
- Warranty terms.
- Maintenance and support capacity.
- Delivery timelines.
- References and past performance.
- Compliance with legal requirements.
- Cost and overall value for money.

Vendor evaluations shall be documented.

13.8 Due Diligence

Before awarding significant ICT contracts, ILA shall conduct appropriate due diligence, including verification of:

- Legal registration.
- Business licences where applicable.
- Tax compliance where required.
- Technical competence.
- References from previous clients.
- Financial capacity where relevant.

- Cybersecurity practices.
- Data protection capabilities.
- Insurance coverage where appropriate.
- History of litigation or regulatory sanctions where material to the engagement.

The extent of due diligence shall be proportionate to the value, complexity, and risk of the procurement.

13.9 ICT Contracts

ICT contracts shall clearly define, as appropriate:

- Scope of work.
- Technical specifications.
- Deliverables.
- Implementation timelines.
- Payment terms.
- Service levels.
- Acceptance criteria.
- Warranty obligations.
- Maintenance responsibilities.
- Security requirements.
- Confidentiality obligations.
- Data ownership.
- Intellectual property rights.
- Dispute resolution mechanisms.
- Termination provisions.

Contracts shall be reviewed by the appropriate technical and legal personnel before execution.

13.10 Service Level Agreements (SLAs)

Where ICT services are outsourced, Service Level Agreements shall be established where appropriate.

SLAs may address:

- Service availability.
- Response times.
- Resolution times.
- Preventive maintenance.
- Scheduled maintenance windows.
- Escalation procedures.
- Performance reporting.
- Security obligations.
- Business continuity commitments.

- Penalties or remedies for significant service failures, where appropriate.

Compliance with SLAs shall be monitored throughout the contract period.

13.11 Information Security Requirements

ICT vendors with access to organizational systems or information shall comply with ILA's information security requirements.

Depending on the nature of the engagement, vendors may be required to:

- Sign confidentiality or non-disclosure agreements.
- Implement appropriate cybersecurity controls.
- Protect organizational information against unauthorized access.
- Report security incidents promptly.
- Restrict access to authorized personnel.
- Return or securely destroy organizational information upon completion of services.
- Cooperate with security audits where contractually agreed.

13.12 Data Protection Requirements

Where vendors process personal data on behalf of ILA, they shall:

- Process personal data only for authorized purposes.
- Maintain appropriate administrative, technical, and physical safeguards.
- Prevent unauthorized disclosure.
- Notify ILA promptly of actual or suspected data breaches.
- Support ILA in complying with applicable legal and contractual obligations relating to personal data.

Data processing responsibilities shall be reflected in written agreements where appropriate.

13.13 Software Licensing and Intellectual Property

ICT procurement involving software shall ensure:

- Appropriate software licences are obtained.
- Licence terms are understood and complied with.
- Intellectual property rights are respected.
- Subscription renewals are monitored.
- Licence records are maintained.

ILA shall not knowingly procure or use counterfeit, pirated, or unlicensed software.

13.14 Vendor Access to ICT Systems

Where vendors require access to organizational ICT resources:

- Access shall be approved in advance.
- Access shall be limited to the minimum necessary.
- Access shall be time-bound where practicable.
- Vendor activities may be monitored.
- Access shall be revoked promptly upon completion of the engagement.

Vendors shall comply with ILA's User Access Management and Information Security requirements.

13.15 Performance Monitoring

Vendor performance shall be monitored throughout the contract period.

Performance indicators may include:

- Timeliness of delivery.
- Product quality.
- Service reliability.
- Compliance with contractual obligations.
- Responsiveness to support requests.
- Security performance.
- User satisfaction.
- Compliance with agreed service levels.

Performance issues shall be documented and addressed promptly.

13.16 Contract Changes

Changes to ICT contracts shall:

- Be documented.
- Be justified by operational requirements.
- Be approved in accordance with delegated authority.
- Consider financial, technical, legal, and security implications.

Unauthorized changes to contract scope shall not be permitted.

13.17 Contract Renewal and Termination

Before renewing ICT contracts, ILA shall assess:

- Vendor performance.

- Continuing business need.
- Cost-effectiveness.
- Security performance.
- Availability of alternative suppliers.
- Compliance with contractual obligations.

Upon termination:

- Vendor access shall be revoked.
- Organizational data shall be returned or securely destroyed as agreed.
- Equipment shall be returned where applicable.
- Outstanding obligations shall be resolved.
- Relevant records shall be updated.

13.18 Vendor Risk Management

ILA shall identify and manage risks associated with ICT vendors, including:

- Cybersecurity risks.
- Supply chain disruptions.
- Financial instability.
- Service interruptions.
- Data breaches.
- Regulatory non-compliance.
- Dependence on a single supplier.
- Technology obsolescence.

Appropriate mitigation measures shall be implemented based on the level of risk.

13.19 Records Management

The Administration and ICT function shall maintain records relating to ICT procurement, including:

- Procurement plans.
- Technical specifications.
- Evaluation reports.
- Contracts.
- Service Level Agreements.
- Warranty documentation.
- Licence records.
- Vendor performance reports.
- Maintenance records.
- Contract renewal and termination records.

Records shall be retained in accordance with the Records Management Policy.

13.20 Roles and Responsibilities

Board of Directors

The Board shall provide oversight of major ICT investments and ensure appropriate governance over significant procurement decisions.

Executive Director

The Executive Director shall:

- Approve ICT procurements within delegated authority.
- Ensure adequate resources are available for ICT investments.
- Oversee implementation of this Chapter.

Procurement Committee

The Procurement Committee shall:

- Review ICT procurement processes.
- Evaluate procurement recommendations where required.
- Ensure compliance with procurement policies.

Administration and ICT Function

The Administration and ICT function shall:

- Develop technical specifications.
- Evaluate technical proposals.
- Monitor vendor performance.
- Maintain ICT procurement records.
- Manage ICT contracts from a technical perspective.

Finance Function

The Finance function shall:

- Verify budget availability.
- Process payments in accordance with contractual terms.
- Maintain financial records relating to ICT procurement.

13.21 Monitoring and Compliance

Compliance with this Chapter shall be monitored through:

- Procurement audits.

- Contract reviews.
- Vendor performance evaluations.
- Licence compliance reviews.
- Security assessments.
- Internal audits.
- Financial audits.

Corrective actions shall be implemented where deficiencies are identified.

13.22 Non-Compliance

Failure to comply with this Chapter may result in:

- Cancellation of procurement processes.
- Suspension of vendor access.
- Corrective actions.
- Disciplinary measures under the Human Resource and Administration Policy.
- Recovery of losses where legally permissible.
- Contract termination.
- Referral for investigation where fraud, corruption, or criminal conduct is suspected.

13.23 Exceptions

Exceptions to this Chapter shall:

- Be documented in writing.
- Be supported by a legitimate operational justification.
- Be approved by the Executive Director or delegated authority.
- Include appropriate risk mitigation measures.
- Be reviewed periodically.

CHAPTER FOURTEEN

ICT OPERATIONS, MAINTENANCE, AND TECHNICAL SUPPORT

14.1 Introduction

The Initiative for Legal Aid (ILA) recognizes that effective ICT operations are essential to maintaining reliable, secure, and efficient information systems that support legal aid services, programme implementation, governance, financial management, and organizational administration. The continuous availability and performance of ICT services depend upon structured operational procedures, preventive maintenance, timely technical support, and effective management of changes to ICT infrastructure.

ILA shall establish standardized procedures for the operation, maintenance, monitoring, and support of ICT resources to ensure that systems remain secure, functional, resilient, and responsive to organizational needs.

14.2 Objectives

The objectives of this Chapter are to:

a. Ensure reliable and efficient operation of ICT systems.

b. Minimize system downtime through preventive maintenance.

c. Provide timely and effective technical support to users.

d. Standardize ICT operational procedures.

e. Improve service quality through monitoring and continual improvement.

f. Protect ICT infrastructure from operational failures and security risks.

g. Promote accountability in ICT service delivery.

14.3 Scope

This Chapter applies to all ICT operational activities, including:

- ICT service delivery.
- User support.
- Help desk operations.
- Preventive maintenance.
- Corrective maintenance.
- System monitoring.
- Network operations.
- Server administration.
- Website administration.
- Email administration.
- Configuration management.
- Change management.
- Performance monitoring.
- Technical documentation.
- Capacity management.
- System upgrades.

14.4 ICT Operations Principles

ICT operations shall be guided by the following principles:

14.4.1 Reliability

ICT services shall be operated to maximize availability and minimize disruption.

14.4.2 Standardization

Operational procedures shall be documented and consistently applied.

14.4.3 Preventive Maintenance

Preventive maintenance shall be prioritized over reactive repairs wherever practicable.

14.4.4 Continuous Improvement

ICT services shall be reviewed regularly to improve efficiency, security, and user satisfaction.

14.4.5 Accountability

Roles and responsibilities for ICT operations shall be clearly defined.

14.5 ICT Service Desk

ILA shall establish an ICT Service Desk or designated ICT support function responsible for receiving, recording, tracking, and resolving ICT support requests.

The Service Desk shall:

- Serve as the primary point of contact for ICT support.
- Record all reported incidents and service requests.
- Assign requests for resolution.
- Monitor progress.
- Communicate with users regarding status updates.
- Maintain records of completed requests.
- Escalate unresolved issues where necessary.

14.6 ICT Support Requests

Users requiring ICT assistance shall report issues through approved communication channels, including:

- Official email.
- ICT help desk.
- Telephone.
- Approved ticketing system.
- Other approved reporting mechanisms.

Support requests should include sufficient information to facilitate diagnosis, including:

- User name.
- Location.
- Device identification where applicable.
- Description of the issue.
- Date and time of occurrence.
- Error messages where available.

14.7 Incident Prioritization

ICT incidents shall be prioritized according to their urgency and impact.

Typical priority levels include:

Critical Priority

Incidents causing complete interruption of critical organizational services requiring immediate response.

Examples:

- Server failure.
- Internet outage affecting the organization.
- Ransomware attack.
- Financial system failure.

High Priority

Incidents significantly affecting departmental operations but with temporary workarounds available.

Medium Priority

Incidents affecting individual users without major operational disruption.

Low Priority

Routine requests such as:

- Software installation.
- Password resets.
- Minor configuration changes.
- General user assistance.

Priority classifications shall guide response and resolution efforts.

14.8 Response and Resolution Targets

The Administration and ICT function shall establish internal service targets for acknowledging, responding to, and resolving ICT incidents based on their priority.

Performance targets shall be reviewed periodically to improve service quality.

Actual response times shall be monitored and analyzed to identify opportunities for improvement.

14.9 Preventive Maintenance

Preventive maintenance shall be conducted on ICT assets at scheduled intervals.

Activities may include:

- Hardware inspections.
- Cleaning of equipment.
- Operating system updates.
- Security patch installation.
- Antivirus updates.
- Disk optimization where appropriate.
- Performance checks.
- Battery testing.
- Printer servicing.
- Network equipment inspections.

Preventive maintenance schedules shall be documented and maintained.

14.10 Corrective Maintenance

Corrective maintenance shall be performed whenever ICT equipment develops faults.

Corrective maintenance activities include:

- Fault diagnosis.
- Hardware repair.
- Software troubleshooting.
- Component replacement.
- System restoration.
- Configuration correction.
- Network troubleshooting.

Repairs shall be documented in maintenance records.

14.11 System Monitoring

The Administration and ICT function shall monitor critical ICT systems to identify operational issues before they significantly affect organizational activities.

Monitoring may include:

- Server performance.
- Network availability.
- Storage utilization.
- System errors.
- Website availability.
- Internet connectivity.
- Email services.
- Security alerts.
- Backup status.
- Cloud service availability.

Monitoring results shall be reviewed regularly.

14.12 Configuration Management

Configuration management ensures that ICT systems remain secure, stable, and properly documented.

The Administration and ICT function shall maintain records of significant ICT configurations, including:

- Server configurations.
- Network configurations.
- Firewall rules.
- User access configurations.
- Software versions.
- Operating system versions.
- Device configurations.
- Cloud service configurations.

Unauthorized configuration changes are prohibited.

14.13 Change Management

Changes to ICT infrastructure shall be planned, evaluated, authorized, implemented, and documented.

Changes may include:

- Software upgrades.
- Hardware replacements.
- Network modifications.
- Security configuration changes.
- Cloud service implementation.
- Website updates.
- Infrastructure expansion.

Significant changes shall, where practicable:

- Be risk assessed.
- Be tested before implementation.
- Include rollback procedures.
- Be scheduled to minimize disruption.
- Be communicated to affected users.

Emergency changes may be implemented immediately where necessary to protect organizational operations or security, but shall be documented and reviewed afterwards.

14.14 Capacity Management

ILA shall monitor ICT capacity to ensure that organizational systems continue to meet operational needs.

Capacity planning shall consider:

- Storage utilization.
- Network bandwidth.
- Processing capacity.
- Number of users.
- Cloud subscriptions.
- Future programme growth.
- Technology upgrades.

Recommendations for expansion shall be incorporated into ICT planning and budgeting.

14.15 Performance Management

ICT operational performance shall be monitored using appropriate indicators such as:

- System availability.
- Incident response times.
- Incident resolution times.
- Help desk workload.

- User satisfaction.
- Backup success rates.
- Preventive maintenance completion.
- Website uptime.
- Network reliability.

Performance reports shall be reviewed periodically by management.

14.16 Technical Documentation

The Administration and ICT function shall maintain accurate technical documentation, including:

- Network diagrams.
- System architecture.
- Server inventories.
- ICT asset records.
- Software inventories.
- Configuration records.
- User guides.
- Standard operating procedures.
- Maintenance logs.
- Vendor documentation.
- Disaster recovery procedures.

Documentation shall be updated whenever significant changes occur.

14.17 User Support

The Administration and ICT function shall provide users with reasonable technical assistance relating to:

- Hardware.
- Software.
- Email.
- Network access.
- Printing.
- Mobile devices.
- Collaboration platforms.
- Password management.
- Remote access.
- Cloud services.

Support shall be delivered professionally, respectfully, and in a timely manner.

14.18 Vendor Support

Where specialized expertise is required, authorized ICT vendors or service providers may provide support in accordance with approved contracts.

Vendor support shall be coordinated by the Administration and ICT function.

Vendor activities affecting ICT systems shall be supervised where appropriate.

14.19 Scheduled Maintenance

Scheduled maintenance requiring temporary interruption of ICT services shall:

- Be planned in advance.
- Be approved by the appropriate authority.
- Be communicated to affected users in advance where practicable.
- Minimize operational disruption.
- Be documented.

Emergency maintenance may proceed immediately where necessary to address significant operational or security risks.

14.20 Knowledge Management

The Administration and ICT function shall maintain a knowledge repository containing, where appropriate:

- Frequently Asked Questions (FAQs).
- Troubleshooting guides.
- User manuals.
- Technical procedures.
- Lessons learned.
- Known issue resolutions.
- Standard configurations.

Knowledge sharing shall support efficient and consistent ICT service delivery.

14.21 Roles and Responsibilities

Board of Directors

The Board shall provide oversight of ICT governance and ensure adequate resources are available for ICT operations.

Executive Director

The Executive Director shall:

- Approve major ICT operational initiatives.
- Support implementation of this Chapter.
- Ensure appropriate staffing and budgeting for ICT operations.

Administration and ICT Function

The Administration and ICT function shall:

- Operate ICT infrastructure.
- Provide technical support.
- Perform preventive and corrective maintenance.
- Monitor system performance.
- Maintain technical documentation.
- Coordinate change management.
- Manage ICT service delivery.

Department Heads

Department Heads shall:

- Encourage timely reporting of ICT issues.
- Support planned maintenance activities.
- Coordinate operational requirements with the ICT function.

Users

Users shall:

- Report ICT faults promptly.
- Follow ICT procedures.
- Cooperate during maintenance activities.
- Protect assigned ICT equipment.
- Avoid unauthorized modifications to ICT systems.

14.22 Monitoring and Compliance

Compliance with this Chapter shall be monitored through:

- ICT operational reviews.
- Help desk reports.
- Maintenance records.
- Performance reports.

- Internal audits.
- User feedback.
- System monitoring reports.

Corrective actions shall be implemented where deficiencies are identified.

14.23 Non-Compliance

Failure to comply with this Chapter may result in:

- Restriction of ICT support services.
- Withdrawal of ICT privileges where appropriate.
- Mandatory corrective training.
- Disciplinary action under the Human Resource and Administration Policy.
- Recovery of organizational losses where legally permissible.
- Termination of employment or contract where warranted.

14.24 Exceptions

Exceptions to this Chapter shall:

- Be documented.
- Be supported by a legitimate operational justification.
- Be approved by the Executive Director or delegated authority.
- Include appropriate compensating controls.
- Be reviewed periodically.

CHAPTER FIFTEEN

ICT INCIDENT MANAGEMENT AND DIGITAL INVESTIGATIONS

15.1 Introduction

The Initiative for Legal Aid (ILA) recognizes that ICT incidents, cybersecurity events, and data breaches can disrupt operations, compromise confidential information, damage organizational reputation, and expose the organization to legal, financial, and operational risks. Prompt detection, reporting, investigation, containment, recovery, and post-incident learning are essential to maintaining the confidentiality, integrity, and availability of ILA's information assets.

ILA shall maintain a structured ICT Incident Management framework to ensure that ICT incidents are managed consistently, efficiently, and in a manner that minimizes harm while preserving evidence where required.

This Chapter establishes the procedures for reporting, responding to, investigating, documenting, and learning from ICT-related incidents.

15.2 Objectives

The objectives of this Chapter are to:

a. Establish a structured process for managing ICT incidents.

b. Minimize the operational impact of ICT disruptions.

c. Protect organizational information and ICT assets.

d. Ensure timely reporting and escalation of ICT incidents.

e. Preserve digital evidence for investigations where necessary.

f. Improve organizational resilience through post-incident learning.

g. Ensure compliance with legal, contractual, and donor reporting obligations.

15.3 Scope

This Chapter applies to all ICT incidents affecting ILA, including incidents involving:

- Computer systems.
- Networks.
- Mobile devices.
- Servers.
- Cloud services.
- Websites.
- Email systems.
- Information assets.
- Digital communications.
- Third-party ICT services.
- Remote working environments.

It applies to all employees, Board Members, volunteers, interns, consultants, contractors, service providers, and any other persons authorized to use ILA's ICT resources.

15.4 ICT Incident Management Principles

ICT incident management shall be guided by the following principles:

15.4.1 Timely Reporting

ICT incidents shall be reported immediately upon discovery.

15.4.2 Rapid Response

Appropriate action shall be taken promptly to contain and minimize the impact of incidents.

15.4.3 Evidence Preservation

Where an incident may require investigation or legal action, digital evidence shall be preserved in a manner that maintains its integrity.

15.4.4 Confidentiality

Information relating to ICT incidents shall be shared only with authorized persons.

15.4.5 Continuous Improvement

Lessons learned from ICT incidents shall be used to strengthen organizational security and resilience.

15.5 Definition of an ICT Incident

An ICT incident is any event that adversely affects, or has the potential to adversely affect, the confidentiality, integrity, availability, or proper functioning of ICT systems or organizational information.

Examples include:

- Malware infection.
- Ransomware attack.
- Phishing attack.
- Unauthorized system access.
- Password compromise.
- Data breach.
- Loss or theft of ICT equipment.
- Website defacement.
- Denial-of-service attacks.
- Unauthorized disclosure of confidential information.
- Insider misuse of ICT systems.
- Network intrusion.
- Server failure.
- Major software malfunction.
- Email compromise.
- Internet outage affecting operations.
- Cloud service disruption.

15.6 Incident Reporting

Every user has a responsibility to report suspected or actual ICT incidents immediately.

Reports shall be made to:

- The immediate supervisor.
- The Administration and ICT function.
- The Executive Director where the incident is significant.
- Other designated officers where required.

Reports should include, where available:

- Date and time of the incident.
- Description of the incident.
- Systems affected.
- Persons involved.
- Screenshots or error messages.
- Actions already taken.
- Potential impact.

Failure to report known ICT incidents may constitute misconduct.

15.7 Incident Classification

ICT incidents shall be classified according to their severity.

Level 1 – Low

Minor incidents affecting individual users with limited operational impact.

Examples:

- Forgotten passwords.
- Minor software errors.
- Printer connectivity issues.

Level 2 – Moderate

Incidents affecting departmental operations.

Examples:

- Failure of shared network drives.
- Email service interruptions.
- Localized malware detection.

Level 3 – High

Incidents significantly affecting organizational operations.

Examples:

- Network failure.
- Website compromise.
- Major server malfunction.
- Unauthorized access to organizational systems.

Level 4 – Critical

Incidents posing serious threats to organizational operations, information security, or legal compliance.

Examples:

- Ransomware attacks.
- Large-scale data breaches.
- Complete ICT infrastructure failure.
- Significant cyberattacks affecting multiple systems.

15.8 Incident Response Process

The Administration and ICT function shall follow a structured incident response process consisting of:

Step 1 – Detection

Identify and confirm the incident.

Step 2 – Reporting

Notify appropriate personnel.

Step 3 – Assessment

Determine:

- Nature of the incident.
- Severity.
- Scope.
- Systems affected.
- Potential risks.

Step 4 – Containment

Prevent further damage by:

- Disconnecting affected systems.
- Disabling compromised accounts.
- Blocking malicious traffic.
- Isolating infected devices.

Step 5 – Investigation

Determine:

- Root cause.
- Method of attack.
- Information affected.
- Persons involved.
- Impact.

Step 6 – Recovery

Restore systems using approved recovery procedures.

Step 7 – Closure

Document actions taken and formally close the incident.

Step 8 – Lessons Learned

Review the incident and identify improvements to policies, procedures, technologies, training, or controls.

15.9 Incident Response Team (IRT)

For significant ICT incidents, the Executive Director may establish or activate an Incident Response Team.

Depending on the nature of the incident, the Team may include representatives from:

- Administration and ICT.
- Executive Management.
- Finance.
- Human Resources.
- Programmes.
- Legal.
- Communications.

- Safeguarding (where relevant).
- External ICT specialists.
- Law enforcement agencies, where necessary.

The Incident Response Team shall coordinate response activities, decision-making, communications, and recovery.

15.10 Digital Evidence Preservation

Where an ICT incident may result in disciplinary, civil, criminal, regulatory, or contractual proceedings, digital evidence shall be preserved.

Digital evidence may include:

- System logs.
- Email records.
- Network logs.
- CCTV recordings.
- Hard drives.
- Mobile devices.
- USB storage devices.
- Cloud audit logs.
- Screenshots.
- Backup copies.

Evidence shall be handled in a manner that preserves authenticity, integrity, and chain of custody.

15.11 Digital Investigations

Digital investigations shall be conducted only by authorized personnel or qualified external specialists.

Investigations may include:

- Log analysis.
- Malware analysis.
- Network traffic analysis.
- Device examination.
- Email analysis.
- User activity review.
- Recovery of deleted files where lawful and technically feasible.
- Timeline reconstruction.

Investigations shall respect applicable legal requirements, privacy obligations, and employment policies.

15.12 Chain of Custody

Where digital evidence may be relied upon in legal or disciplinary proceedings, a documented Chain of Custody shall be maintained.

The Chain of Custody shall record:

- Description of the evidence.
- Date and time collected.
- Person collecting the evidence.
- Method of collection.
- Storage location.
- Persons accessing the evidence.
- Transfers of custody.
- Final disposition.

15.13 Communications During Incidents

Information relating to ICT incidents shall be managed carefully.

Only authorized persons may communicate externally regarding ICT incidents.

Where appropriate, communications may be made to:

- Employees.
- Donors.
- Beneficiaries.
- Government authorities.
- Law enforcement.
- Service providers.
- Media, through the Executive Director or an authorized spokesperson.

Communications shall be accurate, timely, and protect confidential information.

15.14 Data Breach Notification

Where an ICT incident involves a personal data breach, ILA shall:

- Assess the nature and severity of the breach.
- Take immediate containment measures.
- Evaluate risks to affected individuals.
- Notify affected persons where required.
- Notify donors, regulators, or other authorities where required by law or contractual obligations.
- Document all actions taken.

15.15 Recovery and Restoration

Following containment and investigation, ICT systems shall be restored in accordance with the Business Continuity and Disaster Recovery Plan.

Restoration activities shall include:

- Verification of system integrity.
- Removal of malicious software.
- Restoration from trusted backups.
- Password resets where appropriate.
- Security patching.
- Validation of normal operations.
- Enhanced monitoring after recovery.

15.16 Post-Incident Review

Following significant ICT incidents, a formal review shall be conducted.

The review shall examine:

- Root causes.
- Response effectiveness.
- Recovery performance.
- Communication effectiveness.
- Policy compliance.
- Technical weaknesses.
- Lessons learned.
- Recommended improvements.

Recommendations shall be tracked until implemented.

15.17 Incident Documentation

The Administration and ICT function shall maintain an ICT Incident Register containing, where applicable:

- Incident reference number.
- Date reported.
- Date resolved.
- Incident category.
- Severity level.
- Systems affected.
- Description.
- Root cause.
- Actions taken.

- Recovery measures.
- Responsible officers.
- Lessons learned.
- Follow-up actions.

Records shall be retained in accordance with the Records Management Policy.

15.18 Training and Awareness

ILA shall provide periodic training covering:

- Identification of cyber threats.
- Incident reporting procedures.
- Phishing awareness.
- Safe handling of digital evidence.
- Data breach response.
- Cybersecurity responsibilities.
- Incident response roles.

Simulation exercises and tabletop drills may be conducted periodically.

15.19 Roles and Responsibilities

Board of Directors

The Board shall:

- Provide oversight of ICT risk management.
- Review reports on major ICT incidents.
- Ensure adequate resources for incident management.

Executive Director

The Executive Director shall:

- Direct the organizational response to major ICT incidents.
- Approve significant external communications.
- Authorize external investigations where necessary.

Administration and ICT Function

The Administration and ICT function shall:

- Receive incident reports.
- Coordinate incident response.
- Conduct technical investigations.

- Preserve digital evidence.
- Maintain the ICT Incident Register.
- Recommend corrective actions.

Department Heads

Department Heads shall:

- Ensure incidents are reported promptly.
- Support investigations.
- Implement corrective actions within their departments.

Users

All users shall:

- Report incidents immediately.
- Cooperate with investigations.
- Preserve evidence where instructed.
- Avoid interfering with affected systems unless necessary to prevent further harm.

15.20 Monitoring and Compliance

Compliance with this Chapter shall be monitored through:

- Incident trend analysis.
- Incident response reviews.
- Internal audits.
- Cybersecurity assessments.
- Lessons learned reviews.
- Management reports.
- Periodic testing of incident response procedures.

Corrective actions shall be implemented where weaknesses are identified.

15.21 Non-Compliance

Failure to comply with this Chapter may result in:

- Mandatory retraining.
- Restriction or suspension of ICT access.
- Disciplinary action under the Human Resource and Administration Policy.
- Recovery of organizational losses where legally permissible.
- Termination of employment or contract where warranted.
- Referral to law enforcement where criminal conduct is suspected.

15.22 Exceptions

Exceptions to this Chapter shall:

- Be documented in writing.
- Be supported by a legitimate operational justification.
- Be approved by the Executive Director or delegated authority.
- Include appropriate compensating controls.
- Be reviewed periodically.

CHAPTER SIXTEEN

ICT COMPLIANCE, MONITORING, AUDIT, AND POLICY REVIEW

16.1 Introduction

The Initiative for Legal Aid (ILA) is committed to maintaining a robust system of ICT governance through continuous monitoring, compliance assessment, internal control, periodic auditing, and regular policy review. Effective oversight ensures that ICT resources are managed responsibly, organizational information is protected, legal and donor obligations are met, and ICT investments continue to support the strategic objectives of the organization.

This Chapter establishes the framework for monitoring compliance with this ICT Policy, evaluating the effectiveness of ICT controls, conducting ICT audits, reporting on ICT performance, managing risks, and reviewing this Policy to ensure its continued relevance and effectiveness.

16.2 Objectives

The objectives of this Chapter are to:

a. Promote compliance with this ICT Policy and related organizational policies.

b. Ensure ICT controls remain effective and responsive to emerging risks.

c. Provide a framework for ICT monitoring and performance evaluation.

d. Facilitate internal and external ICT audits.

e. Promote accountability and continuous improvement in ICT governance.

f. Ensure periodic review and updating of this Policy.

g. Strengthen organizational resilience and information security.

16.3 Scope

This Chapter applies to:

- All ICT systems.
- Information assets.
- ICT infrastructure.
- ICT operations.
- Employees.
- Board Members.
- Volunteers.
- Consultants.
- Contractors.
- Third-party ICT service providers.
- ICT projects.
- ICT procurement.
- Information security controls.
- Digital records.
- Cloud services.
- Mobile technologies.

16.4 ICT Governance Principles

ILA shall manage ICT governance in accordance with the following principles:

16.4.1 Accountability

Every individual shall be accountable for compliance with applicable ICT requirements.

16.4.2 Transparency

ICT governance activities shall be documented and capable of independent review.

16.4.3 Continuous Improvement

ICT controls, procedures, and technologies shall be reviewed and improved regularly.

16.4.4 Risk-Based Management

ICT governance activities shall prioritize areas presenting the greatest operational, legal, financial, and cybersecurity risks.

16.4.5 Compliance

ICT activities shall comply with applicable laws, donor requirements, contractual obligations, and organizational policies.

16.5 ICT Compliance Monitoring

The Administration and ICT function shall monitor compliance with this Policy through:

- Periodic compliance reviews.
- ICT inspections.
- User access reviews.
- Security monitoring.
- Software licence verification.
- Asset inventories.
- Backup verification.
- Configuration reviews.
- Incident trend analysis.
- User awareness assessments.

Monitoring activities shall be documented and reported to Management.

16.6 Internal ICT Audits

ILA shall periodically conduct internal ICT audits to assess:

- Compliance with this Policy.
- Effectiveness of ICT controls.
- Information security practices.
- ICT asset management.
- Software licence compliance.
- User access management.
- Backup and recovery arrangements.
- Vendor management.
- Cybersecurity preparedness.
- Business continuity arrangements.
- Data protection practices.

Audit findings shall be documented and appropriate corrective actions implemented.

16.7 External ICT Audits

Where appropriate, ILA may engage independent auditors or qualified specialists to conduct external ICT assessments.

External reviews may include:

- Information security audits.
- Cybersecurity assessments.
- Vulnerability assessments.
- Penetration testing.

- Software licence audits.
- Cloud security assessments.
- Donor compliance reviews.
- Digital forensic reviews.
- ICT governance assessments.

Management shall consider and implement recommendations arising from external reviews where appropriate.

16.8 ICT Risk Assessments

The Administration and ICT function shall conduct periodic ICT risk assessments.

Risk assessments shall evaluate:

- Cybersecurity threats.
- Operational risks.
- Legal risks.
- Privacy risks.
- Vendor risks.
- Technology risks.
- Business continuity risks.
- Emerging threats.
- Regulatory changes.

Risk assessments shall support organizational planning, budgeting, and control improvements.

16.9 Key Performance Indicators (KPIs)

To measure the effectiveness of ICT operations, the Administration and ICT function shall monitor appropriate Key Performance Indicators, which may include:

- System availability (uptime).
- Average incident response time.
- Average incident resolution time.
- Number of unresolved incidents.
- Backup success rate.
- Successful recovery test rate.
- Software patch compliance rate.
- ICT asset inventory accuracy.
- User satisfaction levels.
- Percentage of staff completing ICT security awareness training.
- Number of cybersecurity incidents.
- Percentage of systems using multi-factor authentication.
- Number of overdue software licences.
- Compliance audit findings resolved within agreed timelines.

KPI results shall be reviewed periodically to identify trends and opportunities for improvement.

16.10 Management Reporting

The Administration and ICT function shall prepare periodic ICT management reports for Senior Management.

Reports may include:

- ICT performance.
- Major incidents.
- Cybersecurity threats.
- Compliance status.
- Asset management.
- ICT expenditure.
- Procurement activities.
- Vendor performance.
- Business continuity readiness.
- Audit findings.
- Risk assessment results.
- Improvement initiatives.

Significant matters shall be escalated to the Executive Director and the Board where appropriate.

16.11 Corrective and Preventive Actions

Where deficiencies are identified through monitoring, audits, incidents, or reviews, corrective and preventive actions shall be implemented.

Actions may include:

- Policy revisions.
- Procedure improvements.
- Technical upgrades.
- Staff training.
- Enhanced monitoring.
- Additional security controls.
- Vendor management improvements.
- Disciplinary action where appropriate.

Action plans shall identify:

- Responsible officers.
- Required activities.
- Target completion dates.
- Monitoring arrangements.

Implementation shall be tracked until completion.

16.12 Staff Awareness and Capacity Building

ILA shall promote continuous ICT awareness through:

- Induction training.
- Refresher training.
- Cybersecurity awareness campaigns.
- Phishing simulation exercises.
- User guidance materials.
- Policy dissemination.
- Lessons learned from ICT incidents.
- Specialized technical training where appropriate.

Training records shall be maintained by the Administration and Human Resources functions.

16.13 Policy Review

This ICT Policy shall be reviewed:

- At least once every three (3) years.
- Following major ICT incidents.
- Following significant organizational restructuring.
- Following major legislative or regulatory changes.
- Following significant technological developments.
- Where audit findings indicate the need for revision.
- Where donor requirements materially change.

Interim amendments may be made where necessary to address urgent operational, legal, or security requirements.

16.14 Policy Amendment Procedure

Amendments to this Policy shall:

1. Be initiated by the Administration and ICT function, Management, or the Board.
2. Be supported by appropriate justification.
3. Be reviewed by relevant departments.
4. Be approved by the Executive Director before submission to the Board where Board approval is required.
5. Be communicated to all affected personnel.
6. Be incorporated into future editions of the Policy.

The current version of the Policy shall always be clearly identified.

16.15 Record Keeping

The Administration and ICT function shall maintain records relating to:

- ICT audits.
- Compliance reviews.
- Risk assessments.
- Training.
- ICT incidents.
- Corrective action plans.
- Policy revisions.
- ICT performance reports.
- Vendor assessments.
- Asset inventories.
- Security assessments.

Records shall be maintained in accordance with the Records Management Policy.

16.16 Roles and Responsibilities

Board of Directors

The Board shall:

- Approve the ICT Policy and major amendments.
- Provide oversight of ICT governance and strategic ICT risks.
- Review significant ICT audit findings and management responses.
- Ensure adequate resources are allocated for ICT governance.

Executive Director

The Executive Director shall:

- Ensure implementation of this Policy.
- Promote a culture of ICT compliance and information security.
- Review major ICT risks and approve corrective action plans.
- Report significant ICT matters to the Board.

Administration and ICT Function

The Administration and ICT function shall:

- Implement and monitor this Policy.
- Conduct ICT compliance reviews.
- Coordinate ICT audits and risk assessments.
- Maintain ICT governance documentation.

- Report on ICT performance.
- Recommend policy improvements.

Department Heads

Department Heads shall:

- Ensure compliance within their departments.
- Support ICT monitoring and audits.
- Ensure staff participate in required ICT training.
- Implement corrective actions assigned to their departments.

Employees, Volunteers, Consultants, and Contractors

All personnel shall:

- Comply with this ICT Policy.
- Participate in mandatory ICT training.
- Cooperate with ICT audits and compliance reviews.
- Report suspected non-compliance or ICT risks.
- Protect organizational ICT assets and information.

16.17 Non-Compliance

Failure to comply with this Policy may result in one or more of the following, depending on the nature and seriousness of the breach:

- Verbal or written warning.
- Mandatory retraining.
- Restriction or suspension of ICT privileges.
- Recovery of organizational losses where legally permissible.
- Disciplinary action under the Human Resource and Administration Policy.
- Termination of employment, consultancy, or contract where warranted.
- Civil proceedings.
- Referral to law enforcement authorities where criminal conduct is suspected.

16.18 Exceptions

Exceptions to this Policy shall:

- Be documented in writing.
- Be based on a legitimate operational requirement.
- Be supported by an appropriate risk assessment.
- Be approved by the Executive Director or delegated authority.
- Include compensating controls to mitigate identified risks.
- Be subject to periodic review and withdrawal where no longer justified.

16.19 Effective Date

This ICT Policy shall become effective on the date of its approval by the Board of Directors of the Initiative for Legal Aid (ILA) and shall remain in force until amended or repealed.

16.20 Approval

This ICT Policy is approved by the Board of Directors of the Initiative for Legal Aid (ILA).

Approved By	**Board of Directors**
Policy Owner	Executive Director
Policy Custodian	Administration and ICT Function
Effective Date	_____
Review Date	_____
Version	1.0