Insurance Regulatory Commission of Sri Lanka

Cybersecurity and Technology Risk Management Guideline

Contents

Document Control

1	**Document Title**	Cybersecurity & Technology Risk Management Guideline
2	**Date of Release**	This Guideline is effective from 1st August 2026 to all insurance companies.
3	**Documents superseded**	N/A
4	**Version No.**	V 1.0
5	**Document Owner/ Author(s)**	Insurance Regulatory Commission of Sri Lanka

Document Approvers

S. No.	Approver	Approved by	Approved date
1	Commission, IRCSL	Members of the Commission at its 275th Commission meeting (No. 275/21/25.06.2026)	25th June 2026

Document Change

Page No.	Description of Amendment	Reason for Amendment	New Version No. & Effective Date	Amendment done by	Approved by

Document Classification: Non - Confidential

1. Introduction

1.1. Objective

This initiative intends to establish a baseline cybersecurity framework for insurance companies in Sri Lanka to manage cybersecurity risks and ensure the confidentiality, integrity, availability, and resilience of insurance information systems, with due regard to the sensitivity of data, criticality of systems, and the underlying technology infrastructure.

2. Applicability

2.1. Scope

The requirements set out in this guideline shall apply to the entire operations of all licensed insurers, including but not limited to services and infrastructure provided by third-party information technology service providers. This Guideline covers all information systems, applications, data centers, disaster recovery environments, cloud environments, and any other supporting systems or technologies used in connection with the insurer's operations and information security. All licensed insurers shall fully comply with the requirements specified in this guideline.

2.2. Data Coverage

This Guideline shall apply to all forms of data, digitally and paper-based, processed, stored, or transmitted by insurers, with particular focus on the protection of policyholder information, financial data, operational data, and other sensitive or critical business data.

3. Definitions

3.1. Data Classification

1. Public Data

The data that is publicly available to everyone to use and republish without any restriction.

2. Customer Data

Any non-public data relating to a past, existing, or potential customer.

3. Confidential Non-customer Data

Any non-public data that do not fall within the definition of customer data and can cause significant financial or reputational loss if used maliciously or leaked, including the licensed insurance financial transactions, submissions to the Board of Directors and management, sensitive employee data, and any other data as determined by the licensed insurance company.

3.2. Critical Information System

Any information system essential to the functioning and continuous operation of the insurance institution or to the stability of the insurance sector, as determined and approved by the Board of Directors, including core insurance systems and relevant systems operated by intermediaries, agents, or third-party service providers.

3.3. Third-party Service Providers

Any external entity with whom a licensed insurance institution has entered into an outsourcing, service, or contractual arrangement for the provision of services, functions, or information technology resources that support or form part of the institution's operations, including arrangements involving the processing, storage, transmission, or management of data or information systems.

Such third-party service providers shall be subject to a formal vendor risk classification framework based on criticality and data sensitivity (e.g., Critical, High, Medium, and Low). The institution shall define and enforce minimum cybersecurity requirements, due diligence procedures, and monitoring frequency commensurate with each risk category. Continuous monitoring and periodic reassessment shall be mandate for vendors classified as critical and high risk.

4. Governance and Oversight

4.1. Responsibilities of the Board of Directors

The Board of Directors of a licensed insurer shall be ultimately responsible for cybersecurity and technology risk management. The Board shall:

1. Approve a cybersecurity and information security governance framework
2. Define the technology and cyber risk appetite of the licensed insurer
3. Ensure allocation of adequate financial, human, and technical resources
4. Oversee management's implementation of cybersecurity controls
5. Receive periodic reports on the cybersecurity risk profile and material cyber incidents.
6. Establish an Information Security Committee (ISC).

4.2. Governance Framework - Information Security Committee (ISC)

1. The ISC is responsible for oversight of cybersecurity and technology risk management of the insurer. The Committee shall be responsible for both strategic and operational aspects of information security and technology risk management.
2. The Principal Officer (PO), Specified Officer (SO), Chief Information Security Officer (CISO), Chief Information Officer (CIO)/Head of IT, and any other key operational heads as decided by the Board of the insurer (including compliance, internal audit, and risk management) shall constitute the ISC, subject to Board approval. The Board of Directors of the insurer may decide

the number of members constituting the ISC, provided that the aforesaid PO, SO, CISO, CIO/Head of IT are included in the Board-approved ISC.

3. Other department heads shall attend as co-opted members when matters relating to their areas are discussed.
4. ISC shall be chaired by the PO and shall report to the Board of Directors through Risk management /Audit committee. ISC shall apprise the Risk management / Audit committee of its proceedings at least on a quarterly basis for such proceedings quarterly.
5. ISC shall meet at least once every quarter and shall have a quorum and terms of reference approved by the Board of Directors.
6. ISC shall promptly report any cybersecurity incidents to relevant authorities depending on the severity of the incident and take appropriate actions in remedying the impact at its earliest.

4.3. Chief Information Security Officer– Appointment & Duties

The insurer shall employ in its senior management at least one individual who has appropriate qualifications and experience to handle information and cybersecurity issues of the company on a full-time basis.

1. The said person shall report to the PO and be responsible for ensuring confidentiality, integrity, and availability of digital information and cybersecurity with respect to the company.
2. The said person shall be responsible for establishing cybersecurity policies, monitoring compliance, managing incidents, and coordinating reporting to the IRCSL through the PO.
3. The insurer shall maintain a register recording all the information systems used, including relevant information systems with third-party service providers and agents, clearly identifying whether the information system is a critical information system or non-critical information system.

5. Identification of Critical Information Systems

5.1. Review of Critical Information Systems

The ISC shall identify and annually review information systems classified as critical information systems and inform the Board of Directors annually.

5.2. Scope of Critical Information Systems

Critical information systems shall include systems that process data that are mentioned in the section 2.2 but not be limited to policy administration systems, claims processing systems, accounting and financial reporting systems, customer portals, digital distribution platforms, and systems supporting regulatory reporting.

5.3. Information Systems Inventory

Insurance companies shall maintain an inventory of information systems, clearly identifying critical systems and the categories of data processed.

6. Technology Risk Management

6.1. Cybersecurity Risk Assessment

Insurers shall assess technology and cybersecurity risks as part of their enterprise risk management framework. Technology Risk Assessments shall be conducted:

1. At least annually
2. Prior to onboarding new system, technology or digital products
3. Prior to outsourcing or material changes to existing systems.
4. Following significant system change

Residual risks shall be formally reviewed and approved by senior management or the Board of Directors, in alignment with the organization's approved risk appetite and governance framework.

7. Information Security Controls and Monitoring

Insurance companies shall establish and implement Board approved policies and procedures on cybersecurity and information security. Such policies and procedures shall, at a minimum, address the following areas:

1. Data classification and handling
2. Data deployment and operation of the platform (Cloud, Hybrid, On premises), and disposal
3. Password Management
4. Access control and identity management
5. Antimalware Management
6. Change management
7. Network Security
8. Logging, monitoring, and vulnerability management
9. Protection of customer data and confidential non-customer data
10. Backup and disaster recovery
11. Incident management reporting, actions and forensic readiness
12. Physical & Environmental Security

8. Data Governance

8.1. Data Classification and Handling Requirements

Insurance companies shall classify data in a manner compatible with the data classification frameworks approved by the Board, including but not limited to categories such as public data, confidential external, confidential internal, restricted, highly restricted confidential, non-customer data, and customer data.

Confidential internal, restricted, and highly restricted customer data and confidential non-customer data shall be subject to enhanced protection controls, including encryption, strict access controls, and continuous monitoring. In particular, the personal data shall be treated at the minimum with the requirements of the Personal Data Protection Act, No. 09 of 2022, as amended.

8.2. Data Localization and Cross-Border Data Transfer

Where customer data or critical systems are hosted outside Sri Lanka, insurance companies shall:

a) Obtain prior approvals required by applicable laws for the state-owned companies
b) Ensure that the insurance companies have unrestricted supervisory access to such data and systems.
c) Maintain access to data required for regulatory, supervisory, and audit purposes.
d) Comply with the Personal Data Protection Act, No. 09 of 2022, regarding personal data.

8.3. Data Retention and Disposal

Insurance companies shall establish documented data retention periods in compliance with applicable legal and regulatory requirements, including the Personal Data Protection Act No. 09 of 2022 (as amended) and other relevant laws of Sri Lanka. Secure destruction (eg; physical destruction (shredding/crushing, magnetic erasure) and cryptographic or software-based wiping) methods shall be implemented upon expiry of retention periods, and all disposal activities shall be properly authorized, recorded, and auditable.

9. Access Control and Identity Management

9.1. Access Control Principles

Access to critical information systems and sensitive data shall be provided strictly on a need-to-know-basis, consistent with the principle of least privilege.

Strong authentication mechanisms, including multi-factor authentication, shall be implemented for access to critical systems, remote access, and privileged accounts.

Insurers shall review user access rights at least quarterly and immediately revoke access upon termination or change of role.

1. Privileged access management
2. Periodic access reviews
3. Remote access controls

10. Log Management and Monitoring

Insurers shall maintain and regularly review system, security, and user activity logs, retain them in accordance with a defined retention policy, and ensure that such logs support forensic investigations and monitoring of security events. Access to critical systems and sensitive data shall be protected through enforced multi-factor authentication (MFA), while user credential management shall follow strong password controls, including a minimum password length, enabled complexity requirements, password expiry days, prohibition of reuse of the last passwords, mandatory password change at first login, and account lockout invalid login attempts.

Insurers shall ensure that the above controls form part of the overall security governance framework and are consistently implemented across all systems and users. The Board of Directors shall approve the log management and authentication policy and ensure that compliance is periodically reviewed as part of the organization's cybersecurity oversight responsibilities.

11. IT Infrastructure and Security

The insurer shall implement appropriate network, infrastructure and endpoint security controls, including

1. Network segmentation including secure configuration
2. Firewalls and intrusion detection/prevention
3. Endpoint protection
4. Secure remote access controls
5. Patch management
6. Secure configuration standards
7. Data loss prevention

12. Email and Communications Security

1. Licensed insurance companies shall ensure that all official electronic communications are conducted exclusively using organization-owned and managed corporate email domains that are formally registered to the institution.
2. The use of public or free email services (including but not limited to gmail.com, yahoo.com, outlook.com) for official business communications is strictly prohibited.

3. Insurance companies shall implement appropriate technical, administrative, and monitoring controls to enforce this requirement and shall periodically review compliance as part of their information security governance and risk management processes.
4. Monitor all emails and enable consistent blocking and detection for sensitive information in outbound email.
5. Data loss prevention controls shall be implemented.

13. Cybersecurity Incident Management

13.1. Supervise and Monitor Incident Response

1. Insurance companies shall establish and maintain a documented cyber incident framework that clearly defines procedures for incident detection, timely escalation, response, recovery, and post-incident review. The framework shall ensure prompt containment of incidents, restoration of affected systems, regulatory reporting where required, and implementation of corrective measures to prevent recurrence.
2. In case of a cyber incident, inform the cyber incident classification and severity levels by the insurance company/ISC to the relevant authorities, with the incident timelines. In the event such a cyber incident involves a personal data breach, the insurance company/ISC shall act in accordance with the Personal Data Protection Act, No. 09 of 2022, as amended, in reporting such a data breach to the Data Protection Authority of Sri Lanka.
3. Cyber incidents with high severity (hacking, data loss, malware, ransomware, malicious activities, viruses, phishing, DoS attacks, unauthorized access, insider threats, and online or digital scams) shall be reported to the IRCSL without undue delay.
4. Insurance companies shall implement an incident reporting mechanism in line with the ISO 27001 standards.

13.2. Incident Response Framework

Insurers shall establish documented procedures for;

1. Detection
2. Classification
3. Escalation
4. Containment
5. Recovery
6. Post-incident review

No	Type of the Report	Timeline for Reporting
1	Immediate reporting	Immediate: Within 2 hours of detection of the incident
2	Preliminary incident report	Within 24 hours
3	Detailed report (root cause, impact)	Within 48–72 hours
4	Final report	Post-incident Within 14 days of detection of the incident

Reporting to the IRCSL —the insurer shall require reporting the above incident to the Director General of the IRCSL in the Cybersecurity Incident Reporting Format of Annexure 1.

14. Business Continuity and Disaster Recovery

1. Insurance companies shall establish and maintain Business Continuity and Disaster Recovery arrangements for critical information systems.
2. Business continuity plans shall be based on Business Impact Analysis and shall be tested at least annually.
3. Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for critical systems should be maintained.
4. Backup for critical systems shall be tested for regular backup verification and restoring on a regular basis, with audit records on the same.

15. Third-party and Outsourcing Risk Management

15.1. Third-party Management

Insurance companies shall ensure that third-party service providers implement cybersecurity controls commensurate with the risk posed. Outsourcing and cloud arrangements shall include provisions on data protection, audit rights, incident reporting, and exit strategies.

15.2. Regular Third-party Audits

Insurance companies shall require third-party service providers, particularly those supporting critical information systems or processing customer data, to undergo regular independent security audits. The Board of Directors through the ISC to assess the adequacy of the service provider's cybersecurity controls shall review such reports periodically. Where gaps identified, insurers shall ensure timely remediation and maintain documented evidence of follow-up actions.

15.3. Exit and Data Return Strategies

Insurance companies shall ensure that outsourcing agreements include clearly defined exit and transition arrangements to safeguard business continuity and data security. Agreements shall require third-party service providers to securely return or irreversibly destroy all customer data and confidential information upon termination or expiry of the agreement. Insurers shall also ensure that data returned

in a usable format, access credentials are revoked, residual data securely deleted, and transition support provided to prevent operational disruption.

The third-party outsourcing risk management of the insurance company shall at the minimum comply with the provisions of the Personal Data Protections Act, No. 09 of 2022 as amended.

16. Mobile Application/ Web Application Security Controls

Insurance companies that develop, operate, or provide mobile applications for policyholders shall implement appropriate cybersecurity controls to ensure the confidentiality, integrity, and availability of customer information (particularly personal data) and services accessed through such applications.

1. Mobile applications shall be developed using secure coding practices and subjected to security testing, including vulnerability assessments and penetration testing, prior to deployment and significant updates.
2. Sensitive customer and financial data transmitted through mobile applications shall be encrypted using secure communication protocols.
3. Mobile applications shall enforce secure session management controls, including automatic session timeout and logout functionality.
4. Mobile applications shall be regularly updated to address security vulnerabilities, software defects, and emerging cyber threats.
5. Customer personal and financial information collected through mobile applications shall be processed and retained in compliance with applicable legal and regulatory requirements, including the Personal Data Protections Act, No. 09 of 2022 as amended.
6. Third-party service providers, software development vendors, and external APIs integrated with the mobile application shall be subject to appropriate security assessments and contractual security requirements.
7. Mobile applications shall be distributed only through trusted and authorized application distribution platforms.
8. Customers shall be provided with guidance on the secure use of the mobile application, including password protection, phishing awareness, and safe device practices within the mobile app.

17. Training and Awareness

17.1. Training and Awareness to Board of Directors

1. A licensed insurance institute shall implement a comprehensive annual training and awareness program on cybersecurity, information security, and technology risk management for the Board of Directors.

2. The objective of such a program shall be to enable the Board of Directors to have effective oversight on the adequacy and effectiveness of cybersecurity, information security, and technology risk management policies and procedures of the licensed insurance institute.
3. Responsibilities of the Board of Directors and Board committees in terms of requirements in this regulatory framework guideline and other applicable Laws and Regulations relating to cybersecurity, information security, and technology risk management shall also be covered through such awareness.
4. Such training shall consist of at least one annual structured training program and one or more awareness sessions by cybersecurity, information security, and technology risk management experts every year.
5. The Board Secretary of the licensed insurance institute shall ensure compliance with the above requirements on training and awareness to the Board of Directors.

17.2. Staff Training

1. All relevant employees shall undergo cybersecurity awareness training on an annual basis.
2. The insurance company shall ensure that the staff of the insurance company and agents exposed to or potentially exposed to critical information systems, customer data, or confidential non-customer data are trained and certified on information security in accordance with the following requirements:

(i) Required persons shall complete a cybersecurity awareness training program based on the cybersecurity policies and procedures of the licensed insurance institute;

(ii) Required persons shall complete an internal certification test, based on cybersecurity awareness training, at least annually.

18. Data Insurance Coverage Requirement

18.1. Mandatory Insurance Coverage

All insurance companies shall obtain and maintain adequate external insurance coverage to protect against risks associated with loss, breach, corruption, or unavailability of company data. This requirement shall, at a minimum, apply to all confidential and sensitive data assets, including customer, financial, and regulatory information.

Self-insurance arrangements **shall not be considered** sufficient to meet this requirement. The insurance policy must be obtained from a licensed third-party insurer and shall provide appropriate coverage for data-related risks, including but not limited to cyber incidents, data breaches, system failures, and claims arising from the same..

Organizations shall ensure that the scope, value, and terms of coverage are proportionate to the nature, volume, and criticality of the data held. Evidence of valid insurance coverage shall be maintained and made available for regulatory review upon request.

19. Audit and Compliance

1. Insurance companies shall ensure compliance with the requirements in this regulatory framework and other IRCSL subordinate legislation relating to cybersecurity, information security, and technology risk management, subject to an external audit at least annually.
2. Audit findings shall be reported to the Board of Directors, and rectifications shall be tracked to completion.
3. The PO and the Information Security Officer shall submit an annual compliance certification to the IRCSL confirming adherence to this guideline and disclosing any material non-compliance, together with remediation plans. The Compliance Certificate shall be in the format of Annexure 2.

Annexure 1 – Cybersecurity Incident Reporting Format

Section	Required Information
Reporting Organization	Name of the insurance company
Date and Time of Report	Date and time the report is submitted
Report Type	Immediate / Preliminary / Detailed / Final
Incident Reference Number	Unique incident identification number
Date and Time of Incident Detection	Date and time the incident was first identified
Incident Classification	Malware / Ransomware / Phishing / Unauthorized Access / Data Breach / DoS Attack / Insider Threat / System Compromise / Other
Severity Level	Low / Medium / High / Critical
Affected Systems / Services	Systems, applications, servers, databases, or services impacted
Description of the Incident	Summary of the incident and how it was detected
Root Cause (if identified)	Technical or operational cause of the incident
Impact Assessment	Operational, financial, legal, reputational, or data impact
Data Affected	Type of data affected
Actions Taken	Immediate containment and mitigation actions implemented
Current Status	Ongoing / Contained / Recovered / Closed
External Parties Involved	IRCSL, SLCERT, law enforcement, vendors, third parties, etc.
Recovery Measures	Steps taken to restore systems and services
Preventive Actions	Measures implemented to prevent recurrence
Regulatory Notifications	Date and time notified to IRCSL
Report Prepared By	Name, designation, and contact details
Approved By	Name and designation of approving authority

Annexure 2: Annual Compliance Checklist

Company Name:		**Review Period:**	

Complete this checklist annually. For each item, tick the checkbox (☐ → ✓) and record any exceptions or remediation plans in the Remarks column. Non-compliant items must be address.

No.	Section	Compliance Requirement	✓	Remarks
1	**Governance & Oversight**	The board approves the cybersecurity governance framework, defines the cyber risk, ensures adequate resources, and receives periodic reports on the cybersecurity risk profile and incidents.	☐	
2	**Governance & Oversight**	Information Security Committee (ISC) established with required members, meets at least quarterly with Board-approved quorum and terms of reference, and reports to the Risk Management / Audit Committee.	☐	
3	**CISO**	A qualified Chief Information Security Officer (CISO) is appointed full-time in senior management, with clearly defined responsibilities for policy, compliance, incident management, and regulatory reporting.	☐	
4	**Critical Info. Systems**	ISC maintains and annually reviews the register of critical information systems, including third party and agent-operated systems, and reports findings to the Board.	☐	
5	**Technology Risk Mgmt.**	Cybersecurity risk assessments shall be conducted annually and before new system, outsourcing, or material changes, with remaining risks approved by senior management or the Board.	☐	
6	**Policies & Procedures**	Board-approved cybersecurity and information security policies are in place covering data classification, access control, change management, logging, incident management, backup, and disaster recovery.	☐	
7	**Access Control**	Access to critical systems and data granted on a least-privilege basis with MFA enforced. User access rights reviewed quarterly, and access revoked immediately upon termination or role change.	☐	
8	**Log Management**	System, security, and user activity logs maintained, regularly reviewed, retained per Board-approved log management policy, and capable of supporting forensic investigations.	☐	
9	**IT Infrastructure**	Network segmentation, firewalls, intrusion detection/prevention, endpoint protection, patch management, secure remote access controls, DLP, and secure configuration standards are implemented and reviewed.	☐	
10	**Email & Communications**	All official communications use organization-owned corporate email domains. Use of public email services is prohibited and enforced. Data loss prevention (DLP)	☐	

		controls are implemented, and outbound email is monitored.		
11	**Incident Management**	A documented cyber incident management framework is in place. High-severity incidents are reported to IRCSL and SLCERT within 2 hours (initial), 24 hours (preliminary), 48–72 hours (detailed), and 14 days (final post-incident report).	☐	
12	**Business Continuity**	Business Continuity and Disaster Recovery arrangements for critical systems are established based on a Business Impact Analysis, with defined RTO/RPO, and tested at least annually with regular backup verification.	☐	
13	**Training & Awareness**	Annual structured cybersecurity training is conducted for the Board of Directors. All relevant staff and agents undergo cybersecurity awareness training and complete an annual internal certification test.	☐	
14	**Data Insurance**	Adequate external cyber/data insurance coverage is obtained from a licensed third-party insurer, proportionate to the nature and criticality of data held, and evidence of valid coverage is maintained for regulatory review.	☐	
15	**Audit & Compliance**	An external audit of compliance with this guideline and IRCSL cybersecurity regulations is conducted annually. Findings are reported to the Board and tracked to completion.	☐	

Sign-off & Certification

We confirm that this checklist has been completed to the best of our knowledge and that all material non-compliances have been disclosed with remediation plans in place.

PO	CISO
Name:	Name:
Designation: Signature:	Designation: Signature:
Date:	Date: