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: