

WAICA Re Information Security, Cybersecurity and ICT Governance Policy Statement

WAICA Re Group Information Security, Cybersecurity and ICT Governance Policy Statement

Public Policy Synopsis

WAICA Re recognises information, technology systems and digital assets as strategic business resources that support underwriting, risk management, customer service, operational resilience and long-term value creation. The Group is committed to maintaining the confidentiality, integrity and availability of information entrusted to it by customers, employees, regulators, business partners, shareholders and other stakeholders. This commitment is supported through Board-approved Information Security, Cybersecurity and Information Communication Technology (ICT) Policies applicable across the Group's operations.

Governance and Oversight

Information security and cybersecurity governance are embedded within WAICA Re's enterprise governance framework. The Board has approved Group-wide Information Security and ICT Policies and assigned responsibilities for implementation, oversight and accountability across management, business units, information asset owners and technology teams. Information security responsibilities are shared across the organisation, reflecting the principle that protecting information assets is the responsibility of all employees, contractors and authorised third parties.

Information security is managed through a risk-based framework aligned to recognised international standards and good practice, including ISO 27001 principles. Governance arrangements incorporate policy oversight, risk assessment, control monitoring, incident management, business continuity planning and periodic reviews of information security controls.

Information Security and Cybersecurity Framework

WAICA Re applies a structured approach to protecting information assets throughout their lifecycle. Information assets are classified according to their confidentiality, integrity and availability requirements, and corresponding protection measures are applied based on risk and business criticality. Information is categorised and managed according to defined classifications, including Restricted, Confidential, Internal and Public information. Sensitive customer, employee and business information receives heightened protection and access controls.

The Group's information security framework covers:

- Information asset identification, ownership and accountability.
- Data classification and handling requirements.
- Information lifecycle management from creation to disposal.
- Secure storage, retrieval and transmission of information.
- Data leakage prevention and protection against unauthorised disclosure.
- Encryption for sensitive information in storage and transmission.
- Protection of confidential customer, employee and business information.
- Secure destruction and disposal of information and technology assets.

Cybersecurity and Technology Protection

WAICA Re maintains cybersecurity controls designed to safeguard critical systems, networks, applications and digital infrastructure from cyber threats and unauthorised access. Cybersecurity measures include secure network design, perimeter protection, network segmentation, malware protection, security monitoring, vulnerability management and access management controls.

The Group's cybersecurity programme includes:

- Protection against malware, ransomware and malicious code.
- Continuous monitoring of network and system activities.
- Security patch and update management.
- Multi-layered network security controls.
- Secure remote access arrangements.
- Device security controls for laptops, mobile devices and portable equipment.
- Secure software acquisition, deployment and maintenance processes.
- Secure systems development and change management practices.
- Logging, audit trails and monitoring of security events.
- Incident reporting and escalation procedures.

Access Control and User Security

WAICA Re operates on a "need-to-know", "least privilege" and segregation-of-duties basis. Access to information systems and information assets is granted only where required for legitimate business purposes and is subject to approval, monitoring and periodic review.

The Group maintains controls relating to:

- User authentication and authorisation.
- Logical access management.
- Password management standards.
- User accountability and traceability.
- Periodic access reviews.
- Privileged account controls.
- User session management and inactivity timeouts.
- Secure management of administrator and service accounts.
- Removal or suspension of access following changes in employment status or responsibilities.

Third-Party and Supplier Security

WAICA Re recognises that information security risks may arise through interactions with third parties, vendors, consultants and service providers. Accordingly, the Group requires appropriate controls, oversight and contractual safeguards when information is shared externally.

The Group's approach includes:

- Third-party risk assessment and management.
- Non-disclosure and confidentiality obligations.
- Appropriate contractual protections for information sharing.
- Vendor oversight and monitoring.
- Secure information exchange requirements.

- Requirements for service providers to comply with information security standards and controls

Data Protection and Confidentiality

WAICA Re is committed to protecting customer, employee and corporate information and ensuring that access is restricted to authorised individuals. The Group applies information handling standards, confidentiality requirements and secure communication practices designed to protect sensitive information against unauthorised disclosure, misuse, alteration or loss.

The Group promotes:

- Protection of personal and sensitive information.
- Secure handling of confidential information.
- Classification-based protection requirements.
- Secure information sharing practices.
- Protection of intellectual property and proprietary information.
- Controlled disclosure of information to external parties.

Technology Asset Management

WAICA Re maintains governance and control processes for the acquisition, use, maintenance and disposal of ICT assets. The Group maintains asset inventories, ownership records and lifecycle management processes for technology resources across its operations.

Technology asset governance includes:

- Asset registration and inventory management.
- Configuration and standards management.
- Hardware and software acquisition controls.
- Management of licensed software.
- Security requirements for corporate devices.
- Secure disposal and sanitisation of technology assets.
- Ongoing maintenance and monitoring of ICT infrastructure

Business Continuity and Disaster Recovery

WAICA Re maintains business continuity and disaster recovery capabilities designed to support operational resilience and continuity of critical business services. Backup, restoration, contingency planning and disaster recovery arrangements are established to minimise disruption and support the timely recovery of critical systems and information resources.

The framework includes:

- Data backup and recovery processes.
- Disaster recovery planning.
- Business continuity planning.
- Recovery testing and validation.
- Critical systems protection.
- Continuity arrangements for essential business activities.
- Incident response and escalation procedures.

Training, Awareness and Culture

WAICA Re recognises that cybersecurity and information security depend on people as well as technology. The Group promotes a culture of awareness, accountability and responsible behaviour through periodic communication, training, education and awareness programmes. Employees are expected to understand and comply with information security requirements relevant to their roles and responsibilities.

Monitoring, Compliance and Continuous Improvement

Compliance with information security and ICT policies is monitored through governance oversight, management reviews, risk assessments, audit processes, incident reporting, access reviews and control monitoring activities. The Group continuously reviews and enhances its cybersecurity, information security and ICT capabilities to address emerging risks, regulatory developments, changing business requirements and evolving technology threats

Responsible and Secure Use of Artificial Intelligence

WAICA Re recognises the opportunities presented by emerging digital technologies, including artificial intelligence (AI), machine learning, automation and advanced

analytics. The Group is committed to ensuring that any deployment or use of AI-related technologies is consistent with applicable legal, regulatory, ethical, information security and data protection requirements.

The Group's approach to AI governance is guided by its existing Information Security, Cybersecurity, Data Classification, ICT Governance, Risk Management and Information Asset Management frameworks. These frameworks establish clear accountability for information assets, access controls, cybersecurity protection, business oversight and risk management activities that also apply to AI-enabled systems and data processing activities.

WAICA Re seeks to ensure that:

- Personal, customer and business information used in digital systems is protected through established confidentiality, access control and information classification requirements.
- Information processed through technology platforms is subject to governance, monitoring, cybersecurity and risk management controls.
- Access to sensitive information, systems and data is restricted according to business need, least-privilege principles and approved authorisations.
- Technology solutions are implemented subject to risk assessment, governance review, change management and approval processes.
- Information systems are protected from unauthorised access, cyber threats, malicious code and data compromise.
- Users remain accountable for activities undertaken within information systems and digital platforms through audit trails, monitoring and security logging arrangements
- Employees receive ongoing awareness and education relating to information security, cybersecurity and responsible technology use

WAICA Re further recognises the importance of human oversight in business decision-making and maintains governance structures that provide accountability, review, approval and oversight over technology-enabled business processes and critical information systems. Significant technology changes are subject to structured governance, impact assessment, testing, approval and monitoring processes. [\[GRP-](#)

The Group continues to monitor developments in artificial intelligence, cybersecurity, data governance, emerging technologies and applicable regulations as part of its broader commitment to responsible innovation, enterprise risk management and operational resilience.

Commitment

WAICA Re remains committed to safeguarding information assets, strengthening cyber resilience, supporting operational continuity and maintaining the trust and confidence of its stakeholders through effective governance, responsible technology management and continuous improvement in information security and cybersecurity practices.