CYBERSECURITY POLICY

Type of policy:	Cybersecurity Policy
Executive summary:	The scope of this policy is applicable to Constantia Risk and Insurance Holdings (Pty) Limited and Constantia Life Limited
Area of governance:	Compliance, Legal and Risk
Approving authority:	The Board of Constantia Risk and Insurance Holdings (Pty) Limited
Group Exco support	Operations Manager
Responsible department:	Operations
Date of approval:	September 2024
Review frequency:	Annually
Date of next review:	September 2025
Version:	V1.0
Draft resolution:	The Constantia Group of insurance companies recognises the value as well as the risks associated with outsourcing any of its activities. Whilst legislative requirements form the foundation of this policy, this statement is more practical in its application and utilizes basic business principles and practices as its overall primary standard. This policy has been approved by the Board of Directors of each of the above listed insurers who have duly authorised the signatories to this document. The Board is required to approve the policy in line with regulations with specific reference to Governance and Operational Standards for Insurers (GOI 3)

SIGNED AT Kyalami ON THE DAY 09 OF October 2024

Themba Baloyi
Themba Baloyi (Oct 9, 2024 21:15 GMT+2)

TP BALOYI
CHAIR OF THE BOARD
INDEPENDENT NON-EXECUTIVE

SIGNED AT Cape Town ON THE DAY 7th OF November 2024

Lusani Mulaudzi (Nov 7, 2024 12:39 GMT+2)

LK MULAUDZI
CHAIR OF THE JOINT RGA COMMITTEE
INDEPENDENT NON-EXECUTIVE

Table of Contents

1. APPLICATION

1.1. This policy applies to all employees, and is deemed to include:

- Non-Executive Directors
- Executive Directors and Senior Management
- Managers and Senior Officials
- Permanent staff
- Temporary staff

2. PURPOSE

2.1. The purpose of the Policy is to provide a clear and comprehensive framework for managing and safeguarding the Company's information systems, data, and assets from various cyber threats and risks.

2.2. The primary objectives of the Policy include:

- Risk management;
- Compliance;
- Protection of assets;
- Operational continuity;
- Customer and stakeholder trust;
- Legal and regulatory obligations;
- Preventing data breaches;
- Promoting a security culture; and
- Incident response.

3. SCOPE

3.1. The scope of this Policy defines the boundaries and areas that the policy covers within the Company. It typically encompasses:

- assets;
- personnel;
- technologies;
- data;
- access control;
- incident management;
- training and awareness;
- physical security;
- third-party relationships;
- compliance and legal obligations;
- monitoring and auditing.

3.2. The Company is committed to cybersecurity as a fundamental pillar of our operations and a cornerstone of our responsibility to our stakeholders.

3.3. The Company recognizes the critical role cybersecurity plays in protecting our assets, data, and the privacy of those we serve.

3.4. The Company has established a Work-from-Home Policy which sets out the working environment of the Group and therefore this Policy has been aligned with the working environment.

4. PURPOSE

4.1. This policy is intended to help employees determine what information can be disclosed to non-employees as well as the relative sensitivity of information that should not be disclosed outside the Company without proper authorisation.

4.2. The content covered in these guidelines includes, but is not limited to, information that is either stored or shared via any means. This includes: electronic information, information on paper and information share orally or visually (such as telephone or video conferencing).

4.3. All employees should familiarise themselves with the information labeling and handling guidelines that follow this introduction. It should be noted that the sensitivity level definitions were created as guidelines and to emphasise common sense steps that you can take to protect the Company's confidential information (e.g. confidential information should not be left unattended in conference rooms).

5. DEFINITIONS

"access control" means the process of limiting access to authorised users or systems and restricting unauthorized access to resources or data.

"cybersecurity incident" means any event that compromises the confidentiality, integrity, or availability of data, systems, or networks.

"data encryption" means the process of converting plain text data into cipher text to protect it from unauthorized access during transmission or storage.

"incident response plan (IRP)" means a predefined set of procedures and actions to be followed in the event of a cybersecurity incident.

"malware" means malicious software designed to disrupt, damage, or gain unauthorized access to computer systems or data.

"patch management" means the process of identifying, applying, and managing software updates (patches) to address security vulnerabilities.

"phishing" means a type of cyber-attack that involves tricking individuals into revealing sensitive information, such as passwords or financial details.

"risk assessment" means the process of evaluating and analysing potential cybersecurity risks to determine their impact and likelihood.

"social engineering" means the tactic of manipulating, influencing, or deceiving a victim in order to gain control over a computer system, or to steal personal and financial information.

"two-factor authentication (2FA)" means a security process that requires users to provide two separate authentication factors, usually something they know (password) and something they have (token or smartphone).

"vulnerability assessment" means the process of identifying and evaluating weaknesses in the Company's systems, applications, or processes that could be exploited by attackers.

6. IMPORTANCE OF CYBERSECURITY

6.1. Protection of Assets

The Company acknowledges that our assets are vital to our ability to deliver value to our customers, partners, and shareholders. Cybersecurity safeguards these assets from unauthorized access, damage, or theft, ensuring our continued success and growth.

6.2. Data Integrity and Confidentiality

We understand the paramount importance of data. Data is the lifeblood of our operations and a trust we hold with our customers. Cybersecurity safeguards the integrity and confidentiality of this data, ensuring that it remains reliable and secure.

6.3. Privacy

We respect the privacy of our customers and stakeholders. Cybersecurity is our commitment to protecting the personal and sensitive information entrusted to us. It ensures that this information is used only for its intended purpose and is kept safe from unauthorized disclosure or misuse.

6.4. Operational Resilience

Cybersecurity strengthens our operational resilience. By safeguarding our systems and networks, we ensure that our services remain available and uninterrupted, even in the face of cyber threats or disruptions.

6.5. Trust and Reputation

We recognize that trust is the foundation of our relationships with customers, partners, and the broader community. Our cybersecurity commitment is a testament to our dedication to maintaining that trust and upholding our reputation for integrity and responsibility.

7. GOVERNANCE AND RESPONSIBILITIES

7.1. Management

Management support and is committed to all cybersecurity efforts and are essential for establishing a strong cybersecurity position within the Company. Their involvement sets the tone for the entire organisation and ensures that cybersecurity is prioritized and integrated into the business strategy. Here's how management will demonstrate support and commitment to cybersecurity:

7.1.1. Establishing a cybersecurity culture

Management should actively promote a cybersecurity culture by emphasizing the importance of security throughout the Company. They should communicate that cybersecurity is not just an IT issue bue a fundamental aspect of business operations.

7.1.2. Resource allocation

Allocate the necessary resources, including budget, personnel and technology, to support robust cybersecurity measures. This includes investments in security technologies, training programs, and engaging with skilled cybersecurity professionals.

7.1.3. Board-level oversight

Ensure that cybersecurity is on the agenda at board meetings and that the board is actively engaged in overseeing cybersecurity initiatives. This demonstrates that cybersecurity is a top-level concern.

7.1.4. Setting clear expectations

Define clear expectations and objectives for cybersecurity initiatives and communicate them to the entire Company. This includes setting specific goals, metrics, and performance indicators for cybersecurity.

7.1.5. Risk assessment and management

Engage in the assessment and management of cybersecurity risks at a strategic level. Management should be involved in identifying, assessing, and prioritizing cybersecurity risks that could impact the Company's strategic goals.

7.1.6. Policy development and enforcement

Participate in the development and enforcement of cybersecurity policies, standards, and procedures. They should ensure that policies align with industry best practices and legal/regulatory requirements.

7.1.7. Establishing a cybersecurity culture

Management should actively promote a cybersecurity culture by emphasizing the importance of security throughout the Company. They should communicate that cybersecurity is not just an IT issue bue a fundamental aspect of business operations.

7.1.8. Incident Response Planning:

Work closely with the cybersecurity team to develop and maintain an effective incident response plan. Management's involvement is crucial for the plan's success, as they play a critical role in decision-making during incidents.

7.1.9. Compliance and Regulation:

Stay informed about relevant cybersecurity laws and regulations. Ensure that the Company complies with these requirements and takes proactive steps to address any regulatory changes.

7.1.10. Employee Training and Awareness:

Support cybersecurity training and awareness programs for all employees. Management can set an example by participating in these programs and emphasizing their importance.

7.1.11. Vendor and Third-Party Relationships:

Oversee the cybersecurity practices of third-party vendors and contractors. Ensure that cybersecurity requirements are included in contracts and agreements with external partners.

7.1.12. Continuous Improvement:

Encourage a culture of continuous improvement in cybersecurity. This includes regularly reviewing and updating cybersecurity measures to adapt to evolving threats and technologies.

7.1.13. Transparency and Communication:

Maintain open lines of communication with all stakeholders regarding cybersecurity. In the event of a significant cybersecurity incident, management should be prepared to communicate effectively with internal and external stakeholders.

7.1.14. Leading by Example:

Lead by example in following cybersecurity best practices. This includes adhering to password policies, using two-factor authentication, and practicing safe online behaviour.

7.1.15. Reporting and Accountability:

Hold all levels of the organization accountable for cybersecurity performance. Encourage reporting of security incidents and near-misses without fear of retaliation.

7.2. Roles and Responsibilities

7.2.1. Security Operations Center (SOC) Team (includes operations, management & third-party service providers)

Responsibilities:

- Develop and implement the organization's cybersecurity strategy, policies and procedures.
- Oversee (lead and manage) all aspects of the cybersecurity program, including risk management, compliance, and incident response.
- Conduct risk assessments and vulnerability assessments.
- Coordinate incident response and recovery efforts.
- Monitor security technologies and systems Provide leadership and guidance to the end-users.
- Ensure alignment of cybersecurity initiatives with business objectives.
- Monitor the threat landscape and adapt security measures accordingly.
- Conduct security assessments and penetration tests.
- Stay informed about emerging threats and vulnerabilities.
- Act as the primary point of contact for cybersecurity matters with the board.

7.2.2. Network Security Team

Responsibilities:

- Implement and maintain network security controls.
- Monitor network traffic for security anomalies.
- Respond to network security incidents.
- Manage firewall rules and configurations.
- Implement network segmentation for enhanced security.
- Ensure secure remote access to the network.

7.2.3. End-user Security Awareness and Training Team

Responsibilities:

- Develop and deliver security awareness and training programs.
- Conduct phishing simulations and user security assessments.
- Provide guidance to employees on secure practices.
- Create and distribute security-related educational materials.
- Monitor and report on employee compliance with security policies.

8. INFORMATION SECURITY FRAMEWORK

8.1. Information Classification

8.1.1. Sensitive Data

Sensitive data is information that, if disclosed, altered, or accessed by unauthorised parties, could result in significant harm to individuals, organisations, or stakeholders. This category often includes data that is subject to strict legal, regulatory, or contractual requirements. Sensitive data may include:

- **Personal Identifiable Information (PII)**: Information that can be used to identify individuals, such as names, addresses, identity numbers, and financial data.
- **Protected Health Information (PHI)**: Medical and health-related information.
- **Financial Data**: Data related to financial transactions, bank account numbers, credit card information, and payment details.
- **Intellectual Property**: Proprietary information, trade secrets, research, and development data.
- **Legal Documents**: Attorney-client privileged information, confidential legal agreements, and court records.

8.1.2. Confidential Data:

Confidential data is information that requires protection to prevent unauthorized access or disclosure but may not have the same strict legal or regulatory requirements as sensitive data. It is still critical to safeguard confidential data to maintain trust and competitive advantage. Examples of confidential data include:

- **Non-Public Business Information:** Financial reports, business strategies, and internal communications.
- **Customer Lists:** Lists of customers, clients, or partners that are not publicly available.
- **Product Designs:** Information related to product designs, blueprints, and manufacturing processes.
- **Employee Records:** Personnel records, salaries, and performance evaluations.
- **Contractual Agreements:** Confidential agreements with suppliers, contractors, or business partners.

8.1.3. Public Data:

Public data is information that is openly available and does not require special protection. It can be freely accessed and shared without compromising security or privacy. Public data may include:

- **Publicly Available Information:** Information that is intentionally made public, such as website content, press releases, and marketing materials.

- **Non-Sensitive News and Publications:** Information that has been publicly disclosed, including news articles, reports, and research papers.
- **General Contact Information:** Contact details for public representatives or publicly available support contacts.

8.2. Risk Management

8.2.1. Identification of cybersecurity risks

- **Asset Inventory:** Creating an inventory of all assets within the Company. This includes hardware, software, data, personnel, and facilities.
- **Threat Identification:** Identify potential cybersecurity threats that could impact the Company. Common threats include malware, phishing, insider threats, and external attacks.
- **Vulnerability Assessment:** Conduct a vulnerability assessment to identify weaknesses in the systems and applications that could be exploited by threats. This involves using tools and techniques to identify known vulnerabilities.
- **Data Classification:** Classify data into categories such as sensitive, confidential, and public to understand which information requires heightened protection.
- **System and Network Mapping:** Create a map of IT systems, networks, and their interconnections. This helps in understanding the attack surface and potential points of vulnerability.
- **Regulatory and Compliance Requirements:** Consider the legal and regulatory requirements that the Company must adhere to, as non-compliance can result in significant cybersecurity risks.

8.2.2. Assessment of Cybersecurity Risks:

- **Risk Quantification:** Evaluate the potential impact and likelihood of each identified risk. Use a risk assessment methodology to assign numerical values to these factors.
- **Risk Prioritization:** Prioritise risks based on their level of criticality. Risks with high potential impact and likelihood should be addressed first.
- **Risk Scenarios:** Create risk scenarios that illustrate how specific threats could exploit vulnerabilities to impact your organization. This helps in understanding the real-world consequences of risks.
- **Residual Risk Assessment:** Assess the remaining risk after existing controls and mitigations are considered. Determine whether the residual risk is within acceptable levels or if additional measures are needed.
- **Third-Party Risk Assessment:** Evaluate the cybersecurity practices and risks associated with third-party vendors and service providers who have access to your data or systems.

8.2.3. Management of Cybersecurity Risks:

- **Risk Mitigation and Controls:** Develop and implement risk mitigation strategies and controls to reduce the impact and likelihood of identified risks. These controls may include firewalls, encryption, access controls, and security policies.

- **Incident Response Planning:** Develop and maintain an incident response plan to manage cybersecurity incidents effectively when they occur. This plan outlines the steps to take in response to different types of incidents.

- **Continuous Monitoring:** Implement continuous monitoring of systems, networks, and data to detect and respond to emerging threats and vulnerabilities in real-time.

- **Security Awareness and Training:** Educate employees and stakeholders about cybersecurity risks and best practices to reduce human-related vulnerabilities.

- **Regular Risk Assessment Updates:** Periodically revisit and update your risk assessment to account for changes in the threat landscape, technology, and your organization's operations.

- **Documentation and Reporting:** Document the results of risk assessments, mitigation efforts, and incident response activities. Regularly report to senior management and the board to keep them informed about cybersecurity risk management efforts.

- **Insurance:** Consider cybersecurity insurance as a risk management tool to mitigate financial losses in case of a significant cyber incident.

- **Board and Senior Management Involvement:** Ensure that senior management and the board are actively engaged in cybersecurity risk management and decision-making.

9. SECURITY AWARENESS AND TRAINING

9.1. Needs Assessment

- **Identify Target Audiences:** Determine which groups within the Company require cybersecurity awareness and training. This may include employees, contractors, vendors, and third-party partners.

- **Assess Current Knowledge:** Conduct baseline assessments to understand the current level of cybersecurity knowledge and awareness among the target audiences. This can help tailor training content appropriately.

9.2. Customised Training Programs

- **Tailor Content:** Develop cybersecurity training materials and content that are specific to the roles and responsibilities of each group. Content should be relevant, engaging, and easy to understand.

- **Delivery Methods:** Offer a variety of training methods, including in-person sessions, online courses, workshops, webinars, and self-paced e-learning modules. Different individuals may learn best through different approaches.

- **Phishing Simulations:** Conduct regular phishing simulations to test employees' ability to recognize and respond to phishing attempts. Use these simulations as educational opportunities to reinforce awareness.

- **Interactive Learning:** Encourage interactive learning through real-world scenarios, case studies, and practical exercises to help participants apply what they've learned.

9.3. Continuous Education

- **Ongoing Training:** Cybersecurity is an evolving field. Provide regular and ongoing training to keep employees, contractors, and third parties updated on the latest threats, vulnerabilities, and best practices.
- **Awareness Campaigns:** Run awareness campaigns to reinforce key cybersecurity messages. Use posters, newsletters, emails, and other internal communication channels to promote awareness.
- **Training Tracks:** Implement a tiered training approach, offering foundational training for all and more specialized training for those with specific security responsibilities.

9.4. Compliance and Reporting

- **Mandatory Training:** Ensure that cybersecurity training is mandatory for all employees, contractors, and third parties. Tie compliance to employment contracts and vendor agreements.
- **Progress Tracking:** Implement a system to track training progress and completion. This can help identify individuals or groups that may require additional support or attention.
- **Reporting and Metrics:** Collect data on the effectiveness of the training program through metrics like phishing simulation results, incident reports, and user feedback. Use this information to continuously improve the program.

10. REFERENCES TO CYBERSECURITY STANDARDS

10.1. **NIST Cybersecurity Framework:** The National Institute of Standards and Technology (NIST) Cybersecurity Framework provides guidelines and best practices for managing cybersecurity risk. NIST Cybersecurity Framework

10.2. **ISO 27001:** ISO/IEC 27001 is an international standard for information security management systems (ISMS). It provides a systematic approach to managing information security risks. ISO 27001

10.3. **Insurance Authorities:** The Financial Sector Conduct Authority (FSCA) and Prudential Authority (PA) under section 107 read with sections 105, 106 and 108 of the Financial Sector Regulations Act, 2017 (Act No. 9 of 2017) hereby make the Joint Standard 2 of 2004 – Cybersecurity and cyber resilience requirements for Financial Institutions as per the schedule issued

11. CLOSING

11.1. The Group may amend this Policy from time to time and shall be reviewed no less than once within each calendar year cycle. Reasonable efforts will be made to inform all employees of any amendments to the policy. Non-compliance with this policy will be dealt with as described in the Disciplinary Code of Conduct.

12. REVISION HISTORY

Version	Date	Author	Organisation	Revision
1.0	September 2024	R. Kok	Ops Manager	Created policy

CRIH Cybersecurity Policy-Sept 2024-Final For Signature

Final Audit Report 2024-11-07

Created:	2024-10-02
By:	Rene Kok (renek@conduitcapital.co.za)
Status:	Signed
Transaction ID:	CBJCHBCAABAACymI0oVsZgFxZp87h0rJ13WGhAIjsKvh

"CRIH Cybersecurity Policy-Sept 2024-Final For Signature" History

Document created by Rene Kok (renek@conduitcapital.co.za)
2024-10-02 - 12:04:57 PM GMT- IP address: 41.193.162.150

Document emailed to Themba Baloyi (thembab@gmail.com) for signature
2024-10-02 - 12:05:02 PM GMT

Document emailed to Lusani Mulaudzi (lusani.mulaudzi@gmail.com) for signature
2024-10-02 - 12:05:02 PM GMT

Email viewed by Themba Baloyi (thembab@gmail.com)
2024-10-02 - 7:45:58 PM GMT- IP address: 104.28.82.93

Email viewed by Lusani Mulaudzi (lusani.mulaudzi@gmail.com)
2024-10-09 - 6:33:06 PM GMT- IP address: 66.249.93.164

Email viewed by Themba Baloyi (thembab@gmail.com)
2024-10-09 - 7:14:11 PM GMT- IP address: 196.192.169.198

Document e-signed by Themba Baloyi (thembab@gmail.com)
Signature Date: 2024-10-09 - 7:15:10 PM GMT - Time Source: server- IP address: 196.192.169.198

Email viewed by Lusani Mulaudzi (lusani.mulaudzi@gmail.com)
2024-10-17 - 4:01:51 AM GMT- IP address: 66.102.9.133

Email viewed by Lusani Mulaudzi (lusani.mulaudzi@gmail.com)
2024-10-24 - 2:27:24 AM GMT- IP address: 66.249.93.163

Email viewed by Lusani Mulaudzi (lusani.mulaudzi@gmail.com)
2024-11-07 - 10:38:39 AM GMT- IP address: 66.249.93.166

Document e-signed by Lusani Mulaudzi (lusani.mulaudzi@gmail.com)

Signature Date: 2024-11-07 - 10:39:41 AM GMT - Time Source: server- IP address: 196.47.246.31

Agreement completed.

2024-11-07 - 10:39:41 AM GMT