GCC Grupo Cementos de Chihuahua	CORPORATE CYBERSECURITY POLICY		No. Review: 0
Document Key: PO-DTI-TI-25	Issue Date: June 2025	Publication Date: August 2025	Leaf 1 of 5

1. PURPOSE

1.1 This policy establishes the principles, guidelines and responsibilities in cybersecurity with the aim of protecting the company's information, digital assets and technological systems. Cybersecurity is an essential pillar to ensure business continuity, prevent incidents and protect our employees, customers and partners.

1.2 This policy is based on the regulatory and operational framework of Information Technology (IT) established by the company. IT-specific policies provide detailed guidance and controls that reinforce and complement this cybersecurity policy. A list of these policies is included in the References section

2. SCOPE

2.1 This policy is applicable to all GCC employees, as well as contractors, vendors, and third parties who interact directly or indirectly with the organization's computer systems and information, at all of our locations.

3. RESPONSIBLE

3.1 Manager/Supervisor: Responsible for ensuring that their team is aware of and complies with the policy, identifying training needs, and timely reporting of incidents.

3.2 Madata / IT Committee (responsible for Cybersecurity): Design, coordinate and supervise the implementation of controls, programs and reports ensuring compliance with the policy, as well as make key decisions in the event of critical incidents.

3.3 All Users must strictly comply with this policy, attend training, maintain safe practices in their daily activities, and immediately report incidents or suspicious situations.

4. DEFINITIONS

4.1 Cybersecurity: A set of practices, technologies, and processes aimed at protecting systems, networks, programs, and data from attacks, damage, or unauthorized access.

4.2 Information asset: Any resource that stores, processes or transmits information.

4.3 Security incident: Event that compromises the confidentiality, integrity or availability of information.

4.4 SIEM: Security Information and Event Management System that allows detecting and responding to threats in real time.

4.5 Third Parties: contractors, vendors, and third parties who have access to the Company's information or systems.

5. CONTENT

5.1 At GCC we are committed to the comprehensive protection of our information and technological systems against cyber risks, the following principles represent the foundations that guide our organizational posture in the face of cybersecurity. These are the guiding ideas on which controls and procedures are designed:

5.2 Comprehensive Protection: Ensure the confidentiality, integrity and availability of information, considering the IT infrastructure.

5.3 Risk Management: Apply a systematic approach based on ISO/IEC 27001 and NIST to identify, assess, treat, and monitor cyber risks.

5.4 Active Governance: Ensure senior management participation through formal approval of this policy and periodic reviews, assigning specific responsibilities.

5.5 Awareness and Training: Develop competencies through continuous training programs, attack drills, communication campaigns and reinforcement of safe behavior.

5.6 Technical and Organizational Controls: Implement measures such as encryption, access management, multi-factor authentication, firewalls, antivirus, network segmentation, and data backup.

5.7 Incident Response: Have a formalized security incident response and recovery plan, including notification, containment, investigation, recovery, and lessons learned.

5.8 Auditing and Continuous Improvement: Perform internal and external audits, vulnerability assessments, and penetration tests on a regular basis to validate the effectiveness of controls.

5.9 Regulatory Compliance: Ensure compliance with local laws and international frameworks of reference (ej. ISO/IEC 27001, NIST CSF, IEC 62443).

5.10 General Guidelines These guidelines define the practical actions that must be followed to comply with the defined principles:

1. Maintain an up-to-date and classified inventory of digital assets.
2. Apply patches and updates in a timely manner.
3. Control access using principles of least privilege.
4. Segment networks between IT and OT environments.
5. Monitor events and alerts through SIEM tools.
6. Conduct phishing drills and awareness exercises.
7. Maintain protected backups and perform restore tests.
8. Establish metrics and reports of key indicators.

5.11 Specific policies:

5.11.1 Access and password management: Passwords must have a minimum of 12 characters, including letters, numbers and symbols, it is mandatory to change passwords every 90 days. Multi-factor authentication will be used for critical access. (Password sharing is prohibited.)

5.11.2 Protection of sensitive information: All sensitive information must be stored and transmitted with encryption.

5.11.3 Control over software: The installation of unauthorized or illegal software is prohibited.

5.11.4 Proper Use of Technological Resources - The installation of unauthorized or illegal software is strictly prohibited. - Internet access is limited to work activities. - It is forbidden to connect unauthorized external devices to the corporate network.

5.11.5 Awareness and Training

- All staff must mandatorily participate in cybersecurity training.
- Periodic simulations of attacks such as phishing will be carried out to evaluate and improve the response of the staff.
- There will be constant communication about new threats and best practices through newsletters and workshops.

5.11.6 Incident Management - In the event of an incident, it should be reported immediately to the IT Service Desk.

- Strict protocols aligned with international standards will be followed to contain and resolve the incident quickly.
- There will be clear and timely communication about the status and resolution of the incident to all affected parties.

6. CONSEQUENCES FOR NON-COMPLIANCE.

6.1 Any breach of this policy will be handled according to the Consequences Matrix established by GCC, which ranges from written warnings and additional training to major sanctions such as temporary suspension or immediate termination of employment, depending on the severity of the incident.

7. REFERENCES

- ISO/IEC 27001:2013
- NIST Cybersecurity Framework
- IEC 62443
- Federal Law on the Protection of Personal Data in Possession of Private Parties (Mexico)
- PO-DTI-TI-01 Computer Network Administration
- PO-DTI-TI-03 Use of E-mail
- PO-DTI-TI-06 Acquisition of Technological Resources
- PO-DTI-TI-09 Installing and Using Instant Messaging
- PO-DTI-TI-10 User ID Assignment
- PO-DTI-TI-16 Information Retention
- PO-DTI-TI-17 Change Management
- PO-DTI-TI-18 Coordination of Change Implementation
- PO-DTI-TI-20 Service Level Management
- PO-DTI-TI-21 Problem Management
- PO-DTI-TI-22 AM Service Request Source
- PO-DTI-TI-23 Daily Operation Support – Help Desk (Altiris)
- PO-DTI-TI-26 SENSIBLE INFORMATION MANAGEMENT AND PROTECTION POLICY
- PO-DTI-TI-27 Provisioning and Removal of Users
- PO-DTI-TI-28 Supplier Access Control
- PO-DTI-TI-29 Data Center Access Control
- PO-DTI-TI-30 ARTIFICIAL INTELLIGENCE (AI) USE POLICY
- PO-DTI-TI-31 Passwords
- PO-DTI-TI-32 Control over Unauthorized Authorized Licensed Software.
- PO-DTI-TI-34 Server Backups
- PO-DTI-TI-35 Computer Equipment Management
- PO-DTI-TI-36 Encryption of Information in End-User Assets

- PO-DTI-TI-37 Control of Software Development or Modifications
- PO-DTI-TI-39 Use of Instant Messaging Services
- PO-DTI-TI-40 Policy for the Use of Two-Factor Authentication Tools
- PO-DTI-TI-41 Security Incident Management
- PO-DTI-TI-42 Bring Your Tech Resource (BYOD)
- PO-DTI-TI-45 GCC Network Management
- PO-DTI-TI-46 VPN Installation and Use
- PO-DTI-TI-49 Classification of Information
- PO-DTI-TI-51 Mobile Device Security
- PO-DTI-TI-53 ACQUISITION AND ALLOCATION OF TECHNOLOGICAL RESOURCES

8. ANNEXES

Annex 1. Traceability Table between Cybersecurity Policy and IT Policies

Section of this Policy	Related IT Policies
5.1 Comprehensive Protection	PO-DTI-TI-01, PO-DTI-TI-45, PO-DTI-TI-41, PO-DTI-TI-46
5.2 Risk Management	PO-DTI-TI-26, PO-DTI-TI-49
5.3 Active Governance	PO-DTI-TI-20, PO-DTI-TI-30
5.4 Awareness and Training	PO-DTI-TI-03, PO-DTI-TI-09, PO-DTI-TI-39
5.5 Technical Controls	PO-DTI-TI-06, PO-DTI-TI-17, PO-DTI-TI-01, PO-DTI-TI-10, PO-DTI-TI-27, PO-DTI-TI-31, PO-DTI-TI-42, PO-DTI-TI-51, PO-DTI-TI-40, PO-DTI-TI-47, PO-DTI-TI-46, PO-DTI-TI-29
5.6 Incident Response	PO-DTI-TI-41, PO-DTI-TI-21
5.7 Auditing and Improvement	PO-DTI-TI-17, PO-DTI-TI-18, PO-DTI-TI-37
5.8 Regulatory Compliance	PO-DTI-TI-32, PO-DTI-TI-07, PO-DTI-TI-35, PO-DTI-TI-26
5.9 General Guidelines	PO-DTI-TI-16, PO-DTI-TI-49, PO-DTI-TI-34, PO-DTI-TI-36, PO-DTI-TI-22, PO-DTI-TI-23, PO-DTI-TI-28, PO-DTI-TI-20, PO-DTI-TI-53

9. DOCUMENT REVISION TABLE

Review No.	Date	Description of the Change
0	June 2025	Original Document

10. AUTHORIZATIONS

Developed	Revised	Authorized
	Maria Elena Rojas/Internal Control	Ramón Velazco Unzueta/Corporate Controller