SECURITY AND USE OF INFORMATION POLICY

Below is a summary of the main contents of this policy which is described in detail in intranet, Policies and Procedures section:

The purpose of this "Security and use or information Policy" is to define the general guidelines of SQM, in order to provide confidentiality, integrity and availability of the information, as well as its secure use and management.

The information security policies must fit within the framework of the valid legal regulations of the place where they are applied.

Intellectual Property Rights	❖ SQM owns the intellectual property of all information that their users create and manage ❖ People cannot assume that they have a right just because they have access to the information.
Access Privilege	❖ The use of information in SQM is differentiated based on the functions people have and only authorized people should have access to the information and for the purposes set by SQM. ❖ In this regard, each user must be identified and authenticated in a unique manner, applying the segregation of functions principle in the access and treatment of information
Person in charge	❖ It is responsibility of every Department that all of their assigned personnel know and understand their obligations regarding Information Security and Use ❖ Each area is responsible for implementing corporately defined security policies internally.
Information Classification	❖ At SQM, the information is appropriately classified according to its importance and critical nature: o Confidential. o Restricted. o Internal Use. o Public.

Confidential Information	❖ **Example:** market and business information, research, strategy and objectives, prices, processes, wages and benefits, computer programs, list of employees, clients and suppliers, mining, water and environmental rights, legal processes, contracts, contingencies and other related information. o The directors, executives and employees of SQM with access to this confidential information must keep it confidential, even after the end of those functions or even after the end of the contractual relationship. o Confidential information cannot be modified without authorization, used out of context or misused. o At SQM, all the confidential information or the information critical for the business that is transmitted electronically has protection means defined by the Department of Information Technologies that must be used by its users.
Restricted Information	❖ **Example:** Information that has not yet been disclosed to the market and knowledge of which, due to its nature, could influence the market price of those securities. It also includes information about acquisitions or disposals of securities by institutional investors in the securities market. o Any director, executive or employee of SQM who due to their position, activity or relationship has access to inside information must, even if they ceased the exercise of their duties or work, maintain strict discretion about it and cannot use it for their personal benefit or that of others, or acquire for themselves or for others, directly or indirectly, the securities that could be affected by that information. o In addition, directors, executives and employees must refrain from communicating this information to third parties and from recommending the acquisition or disposal of the cited securities or assets.

Information Retention	❖ Although at SQM information is recognized as any other asset of the Company, part of it loses validity after a certain period of time goes by, for this reason the documentation managed by the users, regardless of the storage media (email, printed paper, files or others), has been assigned a retention or obsolescence period according to its classification. After the documentation retention period has expired, it must be deleted or destroyed by the responsible people, using the means that the Company has available for this purpose. ❖ It is important to know SQM's policy and regulations in this matter. Ignorance of these policies and regulations might have legal or tax consequences that could adversely affect SQM. ❖ In general terms and as an example: o When there is an investigation underway (legal, criminal, or tax), a trial or arbitration, no information that might relate to this situation may be altered, deleted, or erased (if in doubt consult SQM's legal counsel) o All accounting and tax information, or their backups, must be saved for at least 6 years.

Security Violations and Sanctions	❖ SQM, upon detecting any use of the information resources for illegal activities or activities violating the internal regulations and/or that are punishable by Law, will apply the appropriate sanctions, in addition to taking the civil and legal actions that the Law authorizes.. ❖ At SQM, users of information resources should not use them for purposes prejudicial to the interests, honor or image of the Company, its employees, or others. ❖ At SQM, the security violations that cause damage to the Company or loss of business will receive the maximum sanctions, including the immediate termination of the implicated employee's employment contract. ❖ Access passwords are personal and it is strictly prohibited to share them with other users.
Facilities Access	❖ Al SQM, all areas containing sensitive information must have restricted access. ❖ At SQM, no information asset should leave the Company's facilities without proper authorization.
Software Use	❖ At SQM, all users must work with the software and computer tools that the Company makes available. ❖ It is strictly prohibited for users to install unlicensed or unauthorized software on their computers or server work areas.

Security Policies	❖ Availability: SQM will maintain contingency plans appropriately updated and tested, with clearly defined responsible people, who will ensure that the information assets are available for the daily performance of the users' duties. ❖ Data Backup Storage of Computer Systems: At SQM, there will be periodic backups of the information contained in the computer systems according to their criticality (this is an IT responsibility). ❖ The backup of printed information or in computers, external devices (CDs, pen drives, external drives, etc.) is the responsibility of each user, however, SQM will provide means to perform these backups in central systems or other defined by IT. ❖ Data Backup Storage of Critical Information: users should not keep critical information in their computers or external devices without proper backup. ❖ Similarly, at SQM remote connections include security and authentication mechanisms in order to ensure that only authorized users have access, and to not allow the data that flows through the network to be viewed by unauthorized persons. ❖ At SQM, each employee should have access to information based on the needs to exercise his or her duties, in that regard each authorized user must be identified and authenticated in a unique way. ❖ SQM must have control mechanisms to identify unusual actions and to monitor the proper operation of its technological platform. ❖ At SQM, all the information that is accessible through the intranet, Internet or any other public domain network must have the Information Technologies security risk analysis done and the authorization of the area responsible for it.