CYBERSECURITY CULTURE

CYBERSECURITY GUIDELINES
OPERATIONAL TECNOLOGY
SOUTHERN PERU COPPER CORPORATION

The Superintendencia de Sistemas Control y Comunicaciones (SsCcCo) is in charge of providing support to Áreas Operativas de Southern Perú for the use of tecnología operativa (**OT**), such like as hardware and software for monitoring, control and communications of the processes, the devices and the infrastructure; within the main functions is protect against cybersecurity attacks on operative networks.

The main types of attacks are:

- **Cybercrime**: is the impersonation of identity of any person or business with economic objectives (bank fraud or withdrawal of money from the bank).
- **Hacktivism**: attack for political and social purposes, carry out a protest through access to their systems or equipment.
- **Cyber espionage**: Its actions is direct at cybersecurity of companies, stealing information.
- **Cyberterrorism**: It is aimed at affecting important government or city infrastructures, such as for health or defense.

A cyber-attack **can act by accessing the databases, connections, confidential documents, etc., of any person, company, or organism (public or private).** Mainly, **intervening in system information or interconnected equipment, in such way that it can alter, destroy and/or bring to light any type of important information** for the company or organization.

As an organization, we are interested in protecting, to both the information and our systems form cyber threats and other possible risks. That is why Southern Peru has developed cybersecurity guidelines and procedures of cybersecurity ("Guidelines") to be protected from any cyber-attack and, in turn, to be aligned with the requirements of mining 4.0.

Below, we state the Guidelines applicable to both Southern Peru personnel and third parties (contractors, suppliers, etc.):

- Guidelines for Vulnerability Management.
- Guidelines for Physical Access Management.
- Guidelines for Remote Access Management.
- Guidelines for Identification and Authentication – Logic Security.
- Guidelines for the Management of Key Risks of Third Parties
- Internal Guidelines Installation, configuration, and security of network equipment.
- Internal Guideline Installation of Servers, PC, Workstation.

Previously to any implementation, maintenance that involves hardware and software, the third must communicate through its contract operator to the Superintendencia de Sistemas Control y Comunicaciones (SsCcCo) for the evaluation of compliance with the cybersecurity guidelines and policies.

Likewise, the main responsibilities of third parties are the following:

- Confidentially manage and not disclose the information received to Southern Perú about its operations in Perú, including those carried out in explorations areas with potential mining recourses, data in general, informs, property titles, financial information or any data or general information about Southern Peru, with the exception of (I) the information that is currently available to the general public, other than that disclosed by Southern Peru, its agents, representatives or employees in reason of this Agreement, or (II) the Information that is currently available on non-confidential basis from any source that is not prohibited to make such disclose based in legal requirement or contractual or any order of competent authority, or (III) that can be show in writing that it was known on the date of disclose by Southern Peru.
- Access information of Southern Peru with the proper authorization by the corresponding Technology area following the Guidelines of Southern Peru.
- No disclose information of Southern Peru to any person, with exception of its employees, agents, representatives or advisors that require to know it for the development of the contracted service and who have instructions from Southern Peru to with all the terms of confidentiality.

- Do not disclose information of Southern Peru to third persons, unless required by express legal mandate, and/or without the prior written authorization of Southern Peru.
- Defend, indemnify or hold Southern Peru harmless for any damage or loss that mat by incurred, whether direct or indirect, including all kind of expenses for professional fees that maybe can generate by breach of the Guidelines or the bad use of receptor for the information.
- Know the guidelines established for the configuration of passwords and the MFA's definition (include 2FA) in the case that they been implement.

In the case that the third party requires more details, they can request the Guidelines and make any coordination whit the Superintendencia de Sistemas Control y Comunicaciones (SsCcOo) of Southern Peru.

Ignorance of the Guidelines does not exempts the worker and/or third party from their compliance and the responsibilities arising from an action contrary to established in the documents.