Information Security Policy

DCA 004/2018 Rev.: 04-31/01/2018 Nº: POL-0007-G INTERNAL USE

Objective: To establish principles and guidelines on information security in Vale and its subsidiaries. This Policy reflects the commitment of Vale's senior management to the confidentiality, integrity and availability of information and technology resources.

Application:

- This Policy applies to Vale and its wholly owned subsidiaries (100% Vale). For the other entities in which Vale holds interest, it is recommended to reproduce it in accordance with Planning, Development and Management Standard (NFN-0001).

References:

- POL-0001-G – Code of Ethics and Conduct
- POL-0009-G – Corporate Risk Management Policy
- POL-0011-G – Information Disclosure Policy
- NFN-0001 – Planning, Development and Management Standard
- NFN-0014 – Information Technology Standard
- NFN-0017 – Corporate Affairs Standard

Principles and Guidelines:

- Information is understood as any content (digital or otherwise) related to Vale or that is circulating in an environment (physical or digital) controlled by the company.
- It is everyone's[1] responsibility to protect information and technology resources under their responsibility, thus preventing information from being disclosed or used inappropriately, interfering with Vale's objectives and causing damages to its employees, service providers, business partners, customers and third parties.
- All purchases of technology resources must comply with Information Security standards.
- Access to Vale's information and technology resources must follow the principle of segregation of duties and should be controlled and restricted for those who have the legitimate need for knowledge and use, according to the function assigned to them.
- Information Security policy violations should be reported, immediately and confidentially, to the Ethics and Conduct Office, according to Code of Ethics and Conduct (POL-0001-G). Some examples include: non-authorized disclosure of information, violation or usage of another employee credential, loss or theft of information, and sharing of password.
- All information and technology resources produced or acquired by Vale or its subsidiaries, as well as information produced by third party under Vale's responsibility, are considered part of its assets (except in cases expressly described in contract), and should be properly protected and in compliance with the law and any other existing legal requirements.
- Vale's Internal Audit and Vale´s Ethics and Conduct Office reserve the right to access and audit, at their own discretion, occasionally or continually, technology resources and information processed by or stored on them, in compliance with applicable legal restrictions.
- Additionally, Information Security area may monitor technology resources, without previous notification, restricted to the identification of potential cyber-threats, such as malicious code, unauthorized access account, loss or theft of information. In case the monitored content is subject to an investigation, the affected user must be informed or an authorization by Internal Audit or Ethics and Conduct Office requested. Any other business situation identified during the monitoring, not linked to cybersecurity risks and in disregard with Vale´s Code of Ethics and Conduct, must be immediately reported to Ethics and Conduct Office and/or Internal Audit.
- To ensure total privacy of personal information, it is highly recommended not to use Vale's technology resources to store it.
- Credentials, such as badge and access accounts, are unique, individual and non-transferable.

[1] Any person with access to Vale´s information, such as employee or service provider, in a corporate or external environment, inside or outside a Vale site.

- To ensure information availability, a Business Continuity Plan should be created, communicated, and updated, with the support of any other area if so necessary, for those departments that identify critical activities and events that may lead to operational and productive process interruption, observing directives available on other normative documents.
- Managers and Contract Managers should disseminate this Policy principles among employees and service providers, and encourage their participation on Information Security awareness campaigns and trainings.
- Procurement and Delegated Areas should ensure that compliance with this Policy is requested by contract.
- It is Human Resource responsibility to assure that all employees are aware of this Policy during hiring process.

Final Provisions:

- Vale’s Information Security Committee is coordinated by Vale’s IT Department, works under the rules established on its Bylaws, and has the objective of seeking for Information Security directives, policies and processes continuous improvement.
- Omitted or non-detailed cases in this Policy should be forwarded to Vale’s Information Security Committee for validation purposes.
- Noncompliance with any item of this Policy will be considered as misuse of information or technology resources and it is considered contractual violation, liable to administrative and legal sanctions where appropriate according to the seriousness of the circumstances.