ICT MANAGEMENT

General Information Security Policy 2025

Last updated 01/13/2025

UENAVENTURA

Peruvian miners working for the country

Introduction

Objective

Scope

Responsibility

Definitions and Abbreviations

General Rules

BUENAVENTURA

Objective

The objective is to establish an information security framework for Buenaventura, based on business needs and inherent risks. The objective is to comply with national and international regulations by implementing controls and standards, primarily Law 29733 and the Sarbanes-Oxley Act.

Objective of the Security Framework

- Achieving the security levels required by Buenaventura
- Based on business needs and inherent risks

Compliance with Regulations and Standards

- National and foreign laws
- Establishment of a regulatory framework
- Implementation of controls

Main Laws Involved

- Law 29733 Protection of Personal Data
- Sarbanes-Oxley Act

Scope

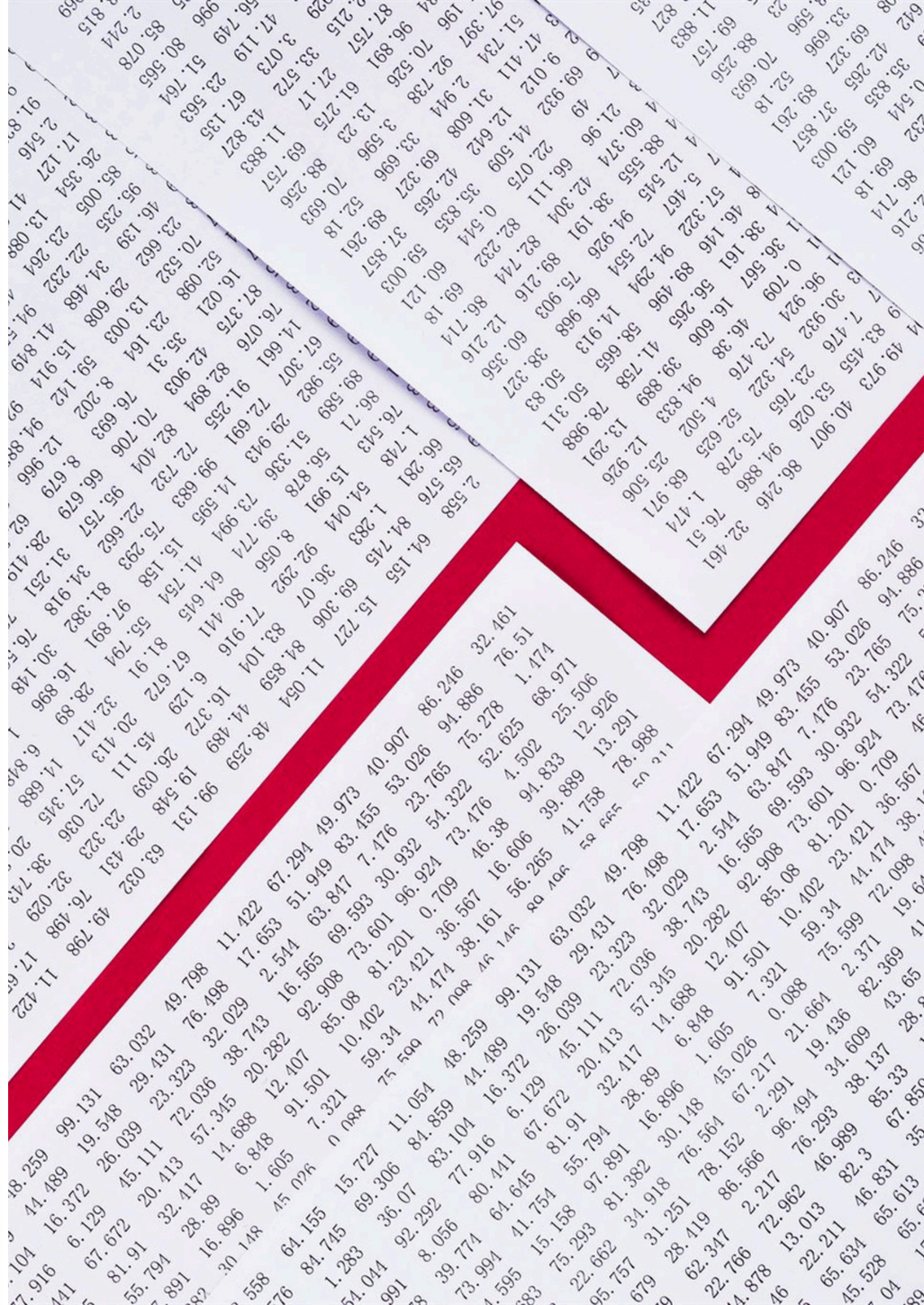
The standards in this document must be known and followed by Buenaventura staff, both permanent and temporary, as well as by the staff of contracted companies.

- Knowledge and Mandatory Compliance
  - Permanent staff of Buenaventura
  - Temporary staff from Buenaventura
- Contracted Companies
  - Staff from companies hired by Buenaventura

Responsibility

Responsibility for compliance with this policy rests with all Buenaventura employees and service providers. The Human Resources Department and Logistics Department are responsible for its dissemination, while the Director of ICT Infrastructure and Security is responsible for its control and monitoring.

- Responsibility of Staff and Suppliers
  - All Buenaventura staff must comply with the policy
  - Suppliers that provide services to the organization must also comply
- Dissemination of Policy
  - Responsibility of Human Resources Management
  - Responsibility of the Logistics Management
- Control and Monitoring
  - Responsibilities of the Director of ICT Infrastructure and Security



Signing and Publication of the Policy

The policy must be signed by the ICT Manager, the Director of ICT Infrastructure and Security, and the Vice President of Finance and Administration. It will take effect after its diffusion and publication on the organization's website, for the information of all Buenaventura staff.

- Signatories of the Policy
  - Information and Communications Technology Manager
  - Director of ICT Infrastructure and Security
  - Vice President of Finance and Administration
- Entry into Force
  - Dissemination and publication on the organization's portal
  - Knowledge of all Buenaventura staff

Staff Responsibilities

Every employee must understand their information security responsibilities. Buenaventura must have a support structure. Area leaders must ensure compliance with controls. Users must use information only for authorized purposes and prevent unauthorized disclosure.

Employee Responsibilities

Know your responsibilities regarding information security Additional daily work for all employees Receive regular induction talks

Support structure

Buenaventura must have a structure that supports information security

Area managers

Ensure compliance with information security controls Ensure compliance with strategic objectives

Responsibilities of information users

Use information only for the authorized purpose Comply with established controls

Critical and Sensitive Information

Buenaventura must inform third parties about its security policies through confidentiality agreements. Maintaining an up-to-date inventory of information assets is essential. Security classifications must be respected and aligned with regulations. Sensitive data must be masked before sending equipment to third parties.

Trust of critical information to third parties

Signing of written confidentiality agreement Annex of general conditions of service

Information Asset Inventory

Periodic update by information owners Minimum annual review

Information security classification

Confidential, Restricted or Internal Use Compliance with security measures according to classification Alignment with regulations such as Law 29733 and Sarbanes-Oxley Act

Masking of personal, confidential and/or sensitive data

Removal or masking before sending equipment to third parties

Intellectual Property and Use of Resources

Buenaventura retains rights over the information created by its employees and reserves access to it. The information resources provided should be used solely for work purposes, and no personal information should be stored.

Intellectual property rights of Buenaventura

Includes all information invented, created or discovered as a result of fulfilling work obligations Files maintained or transmitted through systems or networks Buenaventura reserves the right to access such information

Use of information resources by employees

Resources available to internal and external employees Facilities provided only for business purposes Employees should not store or handle personal information on these resources

Compliance with the Policy

All employees must comply with information security requirements. HR Management conducts induction talks and documents are signed. Ignorance or failure to comply with these requirements does not exempt employees from sanctions, and Technology Management conducts periodic training.

Control and security requirements

They apply to contracted and temporary employees specified in the General Information Security Policy

Induction talks by HR Management

They include information security, signing of acknowledgment and acceptance documents.

Penalties for non-compliance

Lack of knowledge does not exempt from penalties. Technology Management conducts periodic training.

Protection of Information and Assets

Buenaventura must protect information and physical assets from unauthorized access. Employees must report people without visible identification. Workstations and mobile devices must be locked when not in use, and IT Management must establish automatic locking policies.

Protection of Information and Physical Assets

Establish controls to prevent disclosure and modification by unauthorized personnel

Workers' Responsibility

Proactive attitude to identify people without visible identification. Report to immediate superior

Security on Workstations and Mobile Devices

Turn off or lock devices when not in use. Configure automatic lock policies on servers

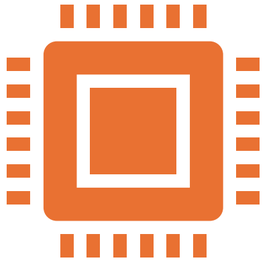
Access to Critical Areas

Access to critical areas such as the Data Center, Control Rooms, and Information Technology Office is restricted to authorized personnel. Contractors and third parties must be supervised by Buenaventura or supplier personnel.

- Restricted access
  - Only authorized personnel can access
  - Contractors and third parties must be supervised
- Specific areas
  - Data Center
  - Control Rooms
  - Office of Information and Communications Technologies
- Supervision
  - Buenaventura staff supervises
  - Suppliers supervise on a case-by-case basis

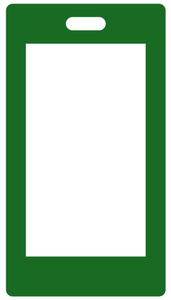
Use of Software and Social Networks

Users must use only approved and licensed software, with the exception of specialized software. They should not use social media to transfer information from Buenaventura; they must use email and corporate OneDrive.



Use of software

Only software approved by the Technology Management Must have corresponding licensing Exception: highly specialized software



Use of social networks

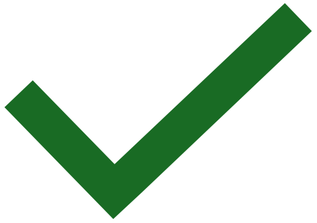
Do not use social networks to transfer information from Buenaventura. Prohibited social networks: Telegram, WhatsApp Web, Slideshare. Use authorized channels: email and corporate OneDrive.

Ban on AI Tools

The use of AI tools such as Read.ai and Otter.ai is prohibited. The ICT department will evaluate and propose a secure application to ensure the confidentiality and integrity of the information.

Ban on AI tools

Read.ai and Otter.ai are banned. Other similar tools are also banned.



Evaluating secure applications

The ICT area will carry out evaluations. A secure application will be proposed. Objective: to ensure confidentiality and integrity of the information.

Use of Passwords

At Buenaventura, information is accessed through personal and confidential usernames and passwords. Passwords must not be predictable or stored in visible locations. The password policy includes a minimum length of eight characters, the use of numbers and letters, and changes every 30 days.

Access to information resources

Personal usernames and passwords
Confidentiality and non-transferability
Sharing credentials is a serious offense

Password Recommendations

Do not use predictable passwords Avoid dictionary words and personal data Do not store passwords in visible places

Password Configuration Policy

Minimum length of eight characters Include numbers, letters and special characters Do not repeat the last five passwords

Safe Development

Security requirements must be analyzed, defined, and incorporated before beginning any development, whether internal or external, to ensure the confidentiality, integrity, and availability of information.

Security requirements analysis

Must be done before the start of development
Applies to internal and external developments

Definition of security requirements

It is essential for the protection of information. It includes confidentiality, integrity and availability.

Incorporation of security requirements

It must be integrated into the development process. It guarantees information security.

Security Incident Management

Users must contact Buenaventura in the event of security incidents. Buenaventura must have a Business Continuity and Disaster Recovery Plan. The Technology Department monitors compliance with the policy. Area managers ensure awareness and compliance with the policies. Disciplinary measures are applied for non-compliance. Security incidents are evaluated based on their impact. High-impact incidents are reported to the Investor Relations Department and General Management. Cybersecurity incidents are prioritized according to document P-COR-TI-14.01.

- Email: seg_ti@buenaventura.pe
- Telephone: 123
- Service Desk controls and reports incidents

- Objective: Continue critical services in the event of a disaster

Annual Policy Review

The policy will be reviewed annually or when there are significant changes, to ensure its continued suitability, adequacy and effectiveness.

- Review Frequency
  - The policy will be reviewed at least once a year
- Conditions for Additional Review
  - It will be reviewed when significant changes occur.
- Objective of the Review
  - Ensure continued suitability, adequacy and effectiveness