Policy manual

Creation of policies to solve the problems presented by the fictitious company, using common frameworks and cybersecurity frameworks to guarantee the security of the fictitious company's data and operations.

Common legal frameworks or frameworks used:

- ISO/IEC 27000 and derivatives (ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005)
- NIST Cybersecurity Framework (CSF)
- Personal Data Protection Act
- General Data Protection Regulation (GDPR)
- National Institute of Standards and Technology (NIST)
- Occupational Safety and Health Administration (OSHA)
- Payment Card Industry Data Security Standard (PCI DSS

Description of the Fictitious Company

The fictitious company is an entrepreneurship project with ten members, aimed at promoting the culture, history, and art of Río Blanco. Its structure is based on a space built with shipping containers, where each entrepreneur exhibits and markets products related to the three key aspects of Río Blanco: culture, history, and art. Pastry has become the main source of income, and the company also organizes training and sessions for the entrepreneurs.

Despite the diversity and focus on local culture, the company faces a challenge in the marketing of clay crafts, which have not met sales expectations. The main issues identified include poor marketing, unattractive designs, and inflation, which affects the purchasing power of buyers. Additionally, the lack of understanding of the utility of these pieces also influences the low demand.

Problem Statement

The company faces a significant challenge in the sale of clay crafts, a key product in its offerings. Despite the wide range of products and the influx of tourists, the sales of these crafts do not meet expectations. It is necessary to identify the causes behind this low demand by evaluating factors such as the marketing strategy, competition in the local market, and consumer preferences.

More effective marketing strategies must be implemented, the designs of the crafts should be adjusted, and promotional activities should highlight the cultural value of the product. Furthermore, an integrated approach addressing both internal causes and external factors affecting sales will be crucial to ensure the economic sustainability of the project.

Fictitious Company

White River
2415-0001

POLICY NAME	**Online presence and digital marketing**	POLICY NO.	1
		VERSION NO.	1.0
RESPONSIBLE ADMINISTRATO R	Stanley Martinez	EFFECTIVE DATE	06/20/202 4
CONTACT INFORMATION	cvd.respon.com	DATE OF LAST REVIEW	06/15/202 4

VERSION HISTORY				
VERSION	APPROVED BY	REVIEW DATE	DESCRIPTION OF CHANGE	AUTHOR
1.0	Senior Management	11 / 06 /2024	Creation of the policy	Stanley Martinez

AIM

Establish and maintain an online presence and digital marketing framework that ensures the proper promotion of the Shell Company's products and services, guaranteeing the consistency, integrity and effectiveness of all digital activities.

POLICY STATEMENT

The Fictional Company is committed to protecting and enhancing its online presence by implementing appropriate digital marketing strategies. Practices and controls will be adopted to ensure the effectiveness and consistency of promotional messages, and that data relating to digital activities is managed responsibly.

SCOPE

This policy applies to all employees, contractors, and third parties involved in the digital marketing activities and online presence of the Fictitious Company. It includes all social media platforms, websites, blogs, email campaigns, and any other form of digital communication used to promote the organization's products and services.

TERMS AND DEFINITIONS

TERM	DEFINITION
Online Presence	Visibility and representation of the Fictitious Company on the Internet and digital platforms.
Digital Marketing	Strategies and practices used to promote products and services in digital media.
Department Managers	Coordinate with the marketing team to ensure that digital activities are aligned with the organization's objectives.
Marketing Auditor	Periodically review the effectiveness of digital marketing strategies and conduct impact assessments.

ROLES AND RESPONSIBILITIES

ROLE	RESPONSIBILITY
Marketing Staff	Implement and monitor security controls, perform security audits, and manage security incidents.
Department Managers	Ensure that the security policy is properly implemented in their areas, identify information assets and coordinate with IT.
Security Auditor	Periodically review the effectiveness of security controls and conduct risk assessments.

BUSINESS PROCESSES AFFECTED.

Content Management

Creation, publication and management of content on websites and social networks.

Digital Advertising

Planning and execution of advertising campaigns on digital platforms.

Data Analysis

Monitoring and analysis of metrics and statistics related to online presence and digital campaigns.

Customer Relations

Management of interactions and communications with clients through digital platforms.

Web Development

Design, development and maintenance of websites and web applications.

EXCEPTIONS

In exceptional cases, certain areas or activities may be excluded from this policy due to technical or commercial restrictions. These exceptions must be approved by the Marketing Manager and properly documented. Exceptions may include:

- Experimental digital marketing activities with controlled risks.
- Emerging platforms that have not yet been fully evaluated.
- Data that is subject to other specific marketing policies due to legal or regulatory requirements.

RELATED DOCUMENTS AND OTHER REFERENCES

- This policy should be read in conjunction with the following documents and policies:
- Privacy and Data Protection Policy
- Online presence and digital marketing procedure

CONTACTS MATRIX

CONTACT TYPE	CONTACT	PHONE	EMAIL
Technical Support	Jose Perez	7845 6321	jperez@undominio.com
Systems Administrator	Maria Lopez	6459 2549	mlopez@empresa.com
Digital Marketing Specialist	Sofia Fernandez	7459 8215	sfernandez@empresa.com
Social Media Specialist	Ana Garcia	5214 6934	agarcia@empresa.com
Marketing Auditor	Laura Martinez	7458 3625	lmartinez@empresa.com
SEO Specialist	Javier Gomez	2548 6934	jgomez@empresa.com

REGULATORY REFERENCES AND LEGAL FRAMEWORK

This policy is aligned with the following rules and regulations:

- Control 5.1 of ISO/IEC 27002:2013 Information security policies.
- ISO/IEC 27001 Standard: International standard for information security management.

Fictitious Company

White River
2415-0001

POLICY NAME	Information Security	POLICY NO.	1
		VERSION NO.	1.0
RESPONSIBLE ADMINISTRATOR	Stanley Martinez	EFFECTIVE DATE	06/20/2024
CONTACT INFORMATION	cvd.respon.com	DATE OF LAST REVIEW	06/15/2024

VERSION HISTORY				
VERSION	APPROVED BY	REVIEW DATE	DESCRIPTION OF CHANGE	AUTHOR
1.0	Senior Management	11 / 06 /2024	Creation of the policy	Stanley Martinez

AIM

Establish and maintain an information security framework that ensures adequate protection of the Shell Company's information assets, guaranteeing the confidentiality, integrity and availability of the information.

POLICY STATEMENT

The Fictional Company is committed to protecting the confidentiality, integrity and availability of the information it handles. Appropriate security controls will be implemented to manage and mitigate the risks associated with the information, ensuring that data is protected against accidental loss and security risks.

SCOPE

This policy applies to all employees, contractors and third parties who have access to the information of the Fictitious Company. It includes all systems, platforms, applications and networks used to store and process data, both on-premises and in the cloud.

TERMS AND DEFINITIONS

TERM	DEFINITION
Information Assets	Data and information resources critical to the operations of the Shell Company.
Security Control	Measures implemented to protect information against threats and vulnerabilities.
Security Risk	Possibility of a threat exploiting a vulnerability, causing damage to information.

ROLES AND RESPONSIBILITIES

ROLE	RESPONSIBILITY
IT Staff	Implement and monitor security controls, perform security audits, and manage security incidents.
Department Managers	Ensure that the security policy is properly implemented in their areas, identify information assets and coordinate with IT.
Security Auditor	Periodically review the effectiveness of security controls and conduct risk assessments.

BUSINESS PROCESSES AFFECTED.

Inventory Management

Protection and backup of inventory databases and product movement records.

Accounting and Finance

Backups of financial records, audit reports and banking transactions.

Sales and Marketing

Backup of sales records, customer databases and marketing campaigns.

IT Management

Administration and operation of IT systems and networks.

Software Development

Development and maintenance of secure applications.

Security Operations

Monitoring and response to security incidents.

EXCEPTIONS

In exceptional cases, certain areas or types of data may be excluded from this policy due to technical or business restrictions. These exceptions must be approved by the IT Manager and appropriately documented. Exceptions may include:

- Data that is not critical to daily operations and can be easily reconstructed.
- Obsolete systems that are in the process of being retired.
- Data that is subject to other specific backup policies due to legal or regulatory requirements.
- Low-risk vulnerabilities that do not have a significant impact on the security of the organization.

RELATED DOCUMENTS AND OTHER REFERENCES

This policy should be read in conjunction with the following documents and policies:

- Information Security Policy
- Information Security Incident Policy

CONTACTS MATRIX

CONTACT TYPE	CONTACT	PHONE	EMAIL
Technical Support	Jose Perez	7845 6321	jperez@undominio.com
Systems Administrator	Maria Lopez	6459 2549	mlopez@empresa.com
Recovery Specialist	Sofia Fernandez	7459 8215	sfernandez@empresa.com
Vulnerability Specialist	Ana Garcia	5214 6934	agarcia@empresa.com
Security Auditor	Laura Martinez	7458 3625	lmartinez@empresa.com
Network Specialist	Javier Gomez	2548 6934	jgomez@empresa.com

REGULATORY REFERENCES AND LEGAL FRAMEWORK

This policy is aligned with the following rules and regulations:

- Control 5.1 of ISO/IEC 27002:2013 Information security policies.
- ISO/IEC 27001 Standard: International standard for information security management.
- Personal Data Protection Legislation: Compliance with local and regional data protection laws.
- Organization's Information Security Policy: Internal document that establishes specific guidelines and requirements for the protection of information.
- Sector Agreements and Regulations: Compliance with specific regulations applicable to the organization's sector.

Fictitious Company
White River
2415-0001

POLICY NAME	Information Security Training	POLICY NO.	2
		VERSION NO.	1.0
RESPONSIBLE ADMINISTRATO R	Stanley Martinez	EFFECTIVE DATE	06/20/202 4
CONTACT INFORMATION	cvd@respon.com	DATE OF LAST REVIEW	06/17/2024

VERSION HISTORY				
VERSIO N	APPROVED BY	REVIEW DATE	DESCRIPTION OF CHANGE	AUTHOR
1.0	Senior Management	11 / 06 /2024	Creation of the policy	Stanley Martinez

AIM

Establish guidelines and procedures to ensure information security education and training at the Fictitious Company in Rio Blanco, in order to protect information assets and reduce the risks associated with potential security breaches.

POLICY STATEMENT

Establish and maintain a high level of information security to protect the organization's assets and reputation. In this regard, an information security awareness, education and training policy is established to ensure that all staff, suppliers and interested parties understand and comply with security requirements.

The main objective of this policy is to foster a culture of information security throughout the organization, promoting the importance of confidentiality, integrity and availability of information. Through awareness and ongoing training, the aim is to ensure that all employees are aware of security risks and are prepared to prevent, detect and respond to potential security incidents.

SCOPE

This policy applies to all employees, contractors, business partners and third parties who interact with information from the Fictitious Company in Rio Blanco. It includes all activities related to information security awareness, education and training. The objective is to ensure that all persons who handle confidential information are adequately informed and trained to protect it against potential security threats and risks.

ROLES AND RESPONSIBILITIES

ROLE	RESPONSIBILITY
Information Security Manager	Responsible for overseeing the implementation and compliance of the policy.
Human Resources Department	Responsible for coordinating initial and ongoing information security training for all employees.
All Employees	Responsible for actively participating in information security training and awareness activities provided by the company.

BUSINESS PROCESSES AFFECTED.

Production of artisanal products

This process is affected by the need to raise staff awareness about the importance of information security at all stages of production, from design to distribution.

Marketing and Sales

Information security awareness is crucial in this process to protect customer data as well as to ensure the integrity and authenticity of information related to artisanal products.

Inventory Management

Information security training is essential to ensure that inventory data is protected from unauthorized access and to ensure the accuracy of stored information.

Customer Service

This process benefits from information security awareness and training to ensure the confidentiality of customer information and to provide a quality service that generates trust in the brand.

EXCEPTIONS

When significant changes are made to information security policies, additional or specific training may be required to ensure that staff are aware of the changes and how they affect their daily tasks.

CONTACTS MATRIX

CONTACT TYPE	CONTACT	PHONE	EMAIL
Technical Support	Jose Perez	7623- 2342	jperez@undominio.com

REGULATORY REFERENCES AND LEGAL FRAMEWORK

ISO 27002 Domain 7:

- Control 7.2 on information security awareness, education and training.

ADDITIONAL NOTES

It is recommended that information security training and awareness be carried out on an ongoing basis, adapting to new threats and technologies.

Fictitious Company
White River
2415-0001

POLICY NAME	Risk Assessment and Treatment	POLICY NO.	3
		VERSION NO.	1.0
RESPONSIBLE ADMINISTRATOR	Stanley Martinez	EFFECTIVE DATE	06/20/2024
CONTACT INFORMATION	cvd.respon.com	DATE OF LAST REVIEW	06/15/2024

VERSION HISTORY				
VERSION	APPROVED BY	REVIEW DATE	DESCRIPTION OF CHANGE	AUTHOR
1.0	Senior Management	11 / 06 /2024	Creation of the policy	Stanley Martinez

AIM

Identify, assess and address information security risks to minimize the impact of potential threats to the Shell Company.

POLICY STATEMENT

The Shell Company will conduct an ongoing assessment of information security risks, implementing appropriate risk management measures to reduce such risks to an acceptable level. The purpose of this policy is to ensure that risks are proactively managed to protect critical information.

SCOPE

This policy applies to all employees, contractors and third parties who have access to the Shell Company's information and systems. It includes all systems, platforms, applications and networks used to store and process data, both on-premises and in the cloud.

TERMS AND DEFINITIONS

TERM	DEFINITION
Security Risk	The possibility that a threat will exploit a vulnerability, causing damage to information or systems.
Risk assessment	Process of identifying, analyzing and evaluating risks to determine their impact and probability.
Risk Treatment	Process of selecting and implementing measures to mitigate, transfer, accept or avoid risks.
Security Control	Measures implemented to protect information against threats and vulnerabilities.
Impact	Consequence or effect of a security incident in the organization.
Probability	Possibility of a security incident occurring.

ROLES AND RESPONSIBILITIES

ROLE	RESPONSIBILITY
IT Staff	Conduct risk assessments, document results, and develop risk treatment plans.
Department Managers	Identify specific risks in your areas and collaborate with IT staff to implement security controls.
Security Auditor	Periodically review the effectiveness of security controls and the implementation of risk treatment plans.

BUSINESS PROCESSES AFFECTED.

Inventory Management

Evaluating and treating risks associated with inventory databases and product movement records.

Accounting and Finance

Evaluating and treating risks related to financial records, audit reports and banking transactions.

Sales and Marketing

risk assessment and treatment of sales records, customer databases and marketing campaigns.

IT Management

Risk assessment and treatment in the administration and operation of IT systems and networks.

Software Development

Risk assessment and treatment in application development and maintenance processes.

Security Operations

Risk assessment and treatment in security incident monitoring and response processes.

EXCEPTIONS

In exceptional cases, certain risks may be excluded from this policy due to technical or business restrictions. These exceptions must be approved by the IT Manager and appropriately documented. Exceptions may include:

- Risks that are not critical to daily operations and that can be mitigated with other controls.
- Obsolete systems that are in the process of being retired.
- Risks subject to other specific policies due to legal or regulatory requirements.
- Low-impact risks that do not have a significant probability of occurring.

RELATED DOCUMENTS AND OTHER REFERENCES

- Information Security Policy
- Physical and Environmental Security Policy

CONTACTS MATRIX

CONTACT TYPE	CONTACT	PHONE	EMAIL
Technical Support	Jose Perez	7845 6321	jperez@undominio.com
Systems Administrator	Maria Lopez	6459 2549	mlopez@empresa.com
Risk Assessment Specialist	Sofia Fernandez	7459 8215	sfernandez@empresa.com
Risk Treatment Specialist	Ana Garcia	5214 6934	agarcia@empresa.com
Security Auditor	Laura Martinez	7458 3625	lmartinez@empresa.com
Network Specialist	Javier Gomez	2548 6934	jgomez@empresa.com

REGULATORY REFERENCES AND LEGAL FRAMEWORK

This policy is aligned with the following rules and regulations:

- Control 8.2 of ISO/IEC 27002:2013 Classification of information
- ISO 31000 Standard: Risk management - Principles and guidelines.
- ISO/IEC 27005 Standard: Information security risk management.
- Applicable legislation on security and data protection: Compliance with local and regional laws related to risk management.
- Internal policies of the organization: Specific guidelines established by the organization for the evaluation and treatment of risks.
- Sector regulations: Compliance with specific regulations according to the organization's sector.

Fictitious Company

White River
2415-0001

POLICY NAME	Identity and Access Management	POLICY NO.	4
		VERSION NO.	1.0
RESPONSIBLE ADMINISTRATO RAND	Stanley Martinez	EFFECTIVE DATE	06/20/2024
CONTACT INFORMATION	cvd.respon.com	DATE OF LAST REVIEW	06/15/2024

VERSION HISTORY				
VERSION	APPROVED BY	REVIEW DATE	DESCRIPTION OF CHANGE	AUTHOR
1.0	Senior Management	11 / 06 /2024	Creation of the policy	Stanley Martinez

AIM

Ensure that only authorized individuals have access to Shell Company systems and data, thereby protecting sensitive and critical information. Ensure that access rights are consistent with business requirements and job responsibilities within Shell Company.

POLICY STATEMENT

User access management will be rigorously controlled to protect the sensitive and critical information of the Shell Company. Strict controls will be implemented for the creation, modification and deletion of user accounts, ensuring that access is granted according to the principle of least privilege and managing access permissions in a controlled manner consistent with business needs and job functions.

SCOPE

This policy applies to all employees, contractors and third parties who require access to the Fictitious Company's systems and data. It includes all systems, platforms, applications and networks used to store and process data.

TERMS AND DEFINITIONS

TERM	DEFINITION
Identity and Access Management (IAM) of information.	Processes and technologies used to manage and protect identities and control access to information resources.
Principle of least privilege	Assign users only the permissions necessary to perform their specific tasks.
Strong Authentication multifactor.	Identity verification mechanisms that provide a high level of security, such as authentication
Access Review	Periodic process of verifying and validating user access permissions to ensure their adequacy.

Role-Based Access Control (RBAC)	Access control method that assigns permissions to users based on their roles within the organization.
Role	Set of job responsibilities and access permissions assigned to a user or group of users.
Access Permissions	Rights granted to a user to access certain information resources or systems.
Review of current business roles.	Process of verifying and updating roles and their associated permissions to ensure they reflect requirements

ROLES AND RESPONSIBILITIES

ROLE	RESPONSIBILITY
IT Staff	Implement and monitor identity and access management procedures, including the creation, modification, and deletion of user accounts. Define, document, and manage roles and access permissions. Implement changes to roles and conduct periodic reviews.
Department Managers	Request and review necessary access for your team members, ensuring compliance with the principle of least privilege. Identify the access needs of your teams and work with IT Staff to define appropriate roles. Review and approve changes to roles and access permissions.
Security Auditor	Conduct periodic reviews of access permissions and assess the effectiveness of authentication and authorization controls. Conduct periodic audits of access roles and permissions to ensure compliance with this policy.

BUSINESS PROCESSES AFFECTED.

Inventory Management

Access control to inventory databases and product movement records based on specific roles.

Accounting and Finance

Management of access to financial records, audit reports and banking transactions assigned according to roles.

Sales and Marketing

Role-based access control to sales records, customer databases and marketing campaigns.

IT Management

Access management in systems and networks according to defined roles.

Software Development

Access control in the development and maintenance processes of applications assigned to specific roles.

Security Operations

Access management in security incident monitoring and response processes based on roles.

EXCEPTIONS

- In exceptional cases, certain access may be excluded from this policy due to technical or business restrictions. These exceptions must be approved by the IT Manager and appropriately documented. Exceptions may include:
- Temporary access required for specific, time-limited projects.
- Access to obsolete systems that are in the process of being retired.
- Low-risk accesses that do not have a significant impact on the security of the organization.

RELATED DOCUMENTS AND OTHER REFERENCES

This policy should be read in conjunction with the following documents and policies:

- Information Security Policy.
- Information Security Incident Policy
- Operations Security Policy

CONTACTS MATRIX

CONTACT TYPE	CONTACT	PHONE	EMAIL
Technical Support	Jose Perez	7845 6321	jperez@undominio.com
Systems Administrator	Maria Lopez	6459 2549	mlopez@empresa.com
Access Management Specialist	Sofia Fernandez	7459 8215	sfernandez@empresa.com
Information Security Specialist	Ana Garcia	5214 6934	agarcia@empresa.com
Security Auditor	Laura Martinez	7458 3625	lmartinez@empresa.com
Network Specialist	Javier Gomez	2548 6934	jgomez@empresa.com

REGULATORY REFERENCES AND LEGAL FRAMEWORK

This policy is aligned with the following rules and regulations:

- Control 9.1 and 9.2 of ISO/IEC 27002:2013 Identity and Access Management and Role-Based Access Control.
- ISO/IEC 27001: International standard for information security management systems.
- Personal Data Protection Act: Local and national regulations on the protection of personal data.
- General Data Protection Regulation (GDPR): European regulation on the protection of personal data and privacy.
- National Institute of Standards and Technology (NIST): Standards and guidance on identity and access management and cybersecurity.

Fictitious Company
White River
2415-0001

POLICY NAME	Physical and environmental security	POLICY NO.	5
		VERSION NO.	1.0
RESPONSIBLE ADMINISTRATOR	Stanley Martinez	EFFECTIVE DATE	06/20/2024
CONTACT INFORMATION	cvd.respon.com	DATE OF LAST REVIEW	06/15/2024

VERSION HISTORY				
VERSION	APPROVED BY	REVIEW DATE	DESCRIPTION OF CHANGE	AUTHOR
1.0	Senior Management	11 / 06 /2024	Creation of the policy	Stanley Martinez

AIM

Protect the organization's physical assets, critical information and IT equipment by implementing physical and environmental security measures in all sensitive areas and restricted access zones.

POLICY STATEMENT

Establish guidelines to protect secure areas and IT equipment against physical damage, adverse environmental conditions and unauthorized access, in order to ensure the integrity and availability of the organization's assets.

SCOPE

This policy applies to all physical areas and computing equipment in the organization, including servers, desktop computers, mobile devices (laptops, tablets), and any other critical equipment. It includes all employees, contractors, and third parties who have access to these areas and equipment.

TERMS AND DEFINITIONS

TERM	DEFINITION
Safe Areas	Protected areas within the organization that require additional security measures due to the information or assets they contain.
Restricted Access Areas	Areas where access is limited to authorized personnel.
Access Controls	Systems and mechanisms used to control and limit access to secure areas and computer equipment.
Monitoring	Continuous monitoring of secure areas and equipment to detect and record unauthorized access or incidents.

ROLES AND RESPONSIBILITIES

ROLE	RESPONSIBILITY
Physical Security Manager	Monitor and implement physical and environmental security controls.
IT Manager	Monitor the protection of computer equipment and the implementation of security measures.
Safety Equipment	Install and maintain access control systems, monitoring and protection measures for computer equipment.
Department Managers	Identify critical areas that require additional protection and ensure policy compliance.
Equipment Users:	Comply with established security policies and report any related incidents.

BUSINESS PROCESSES AFFECTED.

Facility Management

This process covers the management and operation of the organization's physical facilities, ensuring that they are adequately protected and comply with physical and environmental security regulations.

Security Management

It includes the processes related to monitoring, incident response and the implementation of physical and computer security controls to ensure the protection of the organization's assets.

Inventory Management

It refers to the protection of records and inventory stored in secure areas, ensuring that they are available and protected against unauthorized access and physical damage.

Information Management

It covers the protection of sales records, sensitive data and critical documentation stored in secure areas, ensuring their integrity and confidentiality.

IT Management

Related to the administration and operation of the organization's IT equipment, ensuring its physical and environmental protection, as well as the implementation of appropriate security measures.

Daily Operations

It involves the safe and appropriate use of mobile devices and equipment in the day-to-day operations of the organization, following established policies to ensure operational safety and efficiency.

EXCEPTIONS

In exceptional cases, certain areas or equipment may be excluded from this policy for technical or commercial reasons. These exceptions must be approved by the relevant Manager and adequately documented.

RELATED DOCUMENTS AND OTHER REFERENCES

This policy should be read in conjunction with the following documents and policies:

- Information Security Policy
- Incident Management Procedures

CONTACTS MATRIX

Lists contacts related to the policy.

CONTACT TYPE	CONTACT	PHONE	EMAIL
Facilities Manager	Carlos Ramirez	5588 2841	cramirez@empresa.com
Physical Security Manager	John Perez	1474 5484	jperez@empresa.com
Security Coordinator	Maria Lopez	2514 8057	mlopez@empresa.com
IT Manager	John Perez	1547 4059	jperez@empresa.com
Systems Administrator	Maria Lopez	2548 6395	mlopez@empresa.com
Security Auditor	Laura Martinez	9905 2589	lmartinez@empresa.com
Monitoring Specialist	Javier Gomez	5278 3642	jgomez@empresa.com
Physical Security Analyst	Sofia Fernandez	5894 7526	sfernandez@empresa.com

REGULATORY REFERENCES AND LEGAL FRAMEWORK

This policy is aligned with the following rules and regulations:

- Control 11.1 of ISO/IEC 27002:2013 Physical and environmental security
- Control 11.2 of ISO/IEC 27002:2013 Safety of equipment
- ISO/IEC 27001
- Personal Data Protection Act
- General Data Protection Regulation (GDPR)
- National Institute of Standards and Technology (NIST)
- Occupational Safety and Health Administration (OSHA)
- Payment Card Industry Data Security Standard (PCI DSS)

Fictitious Company
White River
2415-0001

POLICY NAME	Security of operations	POLICY NO.	6
		VERSION NO.	1.0
RESPONSIBLE ADMINISTRATO RAND	Stanley Martinez	EFFECTIVE DATE	06/20/2024
CONTACT INFORMATION	cvd.respon.com	DATE OF LAST REVIEW	06/15/2024

VERSION HISTORY				
VERSION	APPROVED BY	REVIEW DATE	DESCRIPTION OF CHANGE	AUTHOR
1.0	Senior Management	11 / 06 /2024	Creation of the policy	Stanley Martinez

AIM

Ensure the availability, integrity, and confidentiality of information critical to the organization's operations by implementing a robust backup system and effectively managing technical vulnerabilities. This includes identifying critical data, assessing vulnerabilities, implementing appropriate backup and security plans, and conducting regular testing to verify data recoverability and integrity, as well as correcting vulnerabilities.

POLICY STATEMENT

It establishes the guidelines for the creation, maintenance and protection of backup copies of critical information and the evaluation and management of technical vulnerabilities in the organization's systems and networks. The purpose of this policy is to protect data against accidental loss and security risks, ensuring that it can be recovered efficiently and that vulnerabilities are detected and corrected before being exploited.

SCOPE

This policy applies to all employees, contractors and third parties who have access to the organization's critical information and systems. It includes all systems, platforms, applications and networks used to store and process data, both on-premises and in the cloud.

TERMS AND DEFINITIONS

TERM	DEFINITION
Critical Data	Information essential to the organization's operations including sales records, financial information, and inventory and production data.
Backups	Replicas of data stored on an alternative medium for recovery in the event of data loss.
Backup Frequencies	Frequency with which backups are made (daily, weekly, monthly).
Automation	Use of automated systems for creating and managing backup copies.
Data Integrity	Verification that the backups have not been altered or corrupted.
Vulnerability	Weakness in a system, application or network that can be exploited to compromise security.

Vulnerability Assessment	Process of identifying, classifying and analyzing vulnerabilities in systems and networks.
Security Audits	Periodic reviews carried out to assess the security of systems and networks.
Scanning Tools	Software used to detect vulnerabilities in software and network configurations.
Impact Analysis	Evaluating the potential effect of a vulnerability on the organization.

ROLES AND RESPONSIBILITIES

ROLE	RESPONSIBILITY
IT Staff	Configure and monitor automatic backups, perform recovery testing, and verify data integrity. Manage vulnerability identification and remediation.
Department Managers	Identify critical data in your areas and coordinate with IT staff to ensure proper backup. Implement security team recommendations.
Security Auditor	Periodically review procedure documentation and recovery test results. Validate vulnerability reports and corrective actions.

BUSINESS PROCESSES AFFECTED.

Inventory Management

Backup of inventory databases and product movement records.

Accounting and Finance

Backups of financial records, audit reports and banking transactions.

Sales and Marketing

Backup of sales records, customer databases and marketing campaigns.

IT Management

Processes related to the administration and operation of systems and networks.

Software Development

Application development and maintenance processes.

Security Operations

Security incident monitoring and response processes.

EXCEPTIONS

In exceptional cases, certain areas or types of data may be excluded from this policy due to technical or business restrictions. These exceptions must be approved by the IT Manager and appropriately documented. Exceptions may include:

- Data that is not critical to daily operations and can be easily reconstructed.
- Obsolete systems that are in the process of being retired.
- Data that is subject to other specific backup policies due to legal or regulatory requirements.
- Low-risk vulnerabilities that do not have a significant impact on the security of the organization.

RELATED DOCUMENTS AND OTHER REFERENCES

This policy should be read in conjunction with the following documents and policies:

- Information Security Policy
- Incident Management Procedures

CONTACTS MATRIX

CONTACT TYPE	CONTACT	PHONE	EMAIL
Technical Support	Jose Perez	7845 6321	jperez@undominio.com
Systems Administrator	Maria Lopez	6459 2549	mlopez@empresa.com
Recovery Specialist	Sofia Fernandez	7459 8215	sfernandez@empresa.com
Vulnerability Specialist	Ana Garcia	5214 6934	agarcia@empresa.com
Security Auditor	Laura Martinez	7458 3625	lmartinez@empresa.com
Network Specialist	Javier Gomez	2548 6934	jgomez@empresa.com

REGULATORY REFERENCES AND LEGAL FRAMEWORK

This policy is aligned with the following rules and regulations:

- Control 12.2 of ISO/IEC 27002:2013 Protection against malicious software (malware)
- Control 12.3 of ISO/IEC 27002:2013 Backups
- Control 12.6 of ISO/IEC 27002:2013 Technical vulnerability management
- ISO/IEC 27001: International standard for information security management systems.
- Personal Data Protection Act: Local and national regulations on the protection of personal data.
- General Data Protection Regulation (GDPR): European regulation on the protection of personal data and privacy.
- National Institute of Standards and Technology (NIST): Vulnerability management and cybersecurity standards and guidelines.

POLICY NAME	Communications security	POLICY NO.	7
		VERSION NO.	1.0
RESPONSIBLE ADMINISTRATOR AND	Stanley Martinez	EFFECTIVE DATE	06/20/2024
CONTACT INFORMATION	cvd.respon.com	DATE OF LAST REVIEW	06/15/2024

VERSION HISTORY				
VERSION	APPROVED BY	REVIEW DATE	DESCRIPTION OF CHANGE	AUTHOR
1.0	Senior Management	11 / 06 /2024	Creation of the policy	Stanley Martinez

AIM

Ensure the protection, integrity, and confidentiality of the organization's networks and information by implementing network controls such as firewalls and intrusion detection and prevention systems (IDS/IPS), proper network segmentation, and encryption of data in transit using secure protocols such as HTTPS and VPN.

POLICY STATEMENT

Establish guidelines for the control, security and protection of networks and information during its exchange within the organization. This includes preventing unauthorized access, detecting and responding to intrusion attempts, segmenting networks to minimize security risks, and protecting transmitted information through the use of encryption and secure protocols.

SCOPE

This policy applies to all networks and systems within the organization that engage in communications and information exchange, including web connections, internal communications, and remote connections. It applies to all devices connected to these networks and to all employees, contractors, and third parties who have access to them.

TERMS AND DEFINITIONS

TERM	DEFINITION
Firewall	A network security appliance that controls incoming and outgoing traffic based on a set of security rules.
IDS (Intrusion Detection System)	System that monitors the network for suspicious activities and issues alerts when possible intrusions are detected.
IPS (Intrusion Prevention System)	System that not only detects suspicious activities but also takes measures to block or prevent these intrusions.
Network Segmentation	The process of dividing a network into smaller, isolated segments to improve security and performance.
Encryption in Transit	The process of encoding data as it is transmitted between systems to protect it from interception and alteration.
HTTPS (Hypertext Transfer Protocol Secure)	Secure communication protocol over a computer network that is primarily used for web browsing.
VPN (Virtual Private Network)	Virtual private network that extends a private network across a public network, allowing users to send and receive data across

	shared or public networks as if their devices were directly connected to the private network.

ROLES AND RESPONSIBILITIES

ROLE	RESPONSIBILITY
Information Security Officer	Oversee the implementation of network controls, network segmentation, data encryption and secure protocols, and ensure compliance with security and information sharing policies.
IT Team	Configure and maintain firewalls, IDS/IPS, perform network segmentation, implement HTTPS for all web connections, and establish VPNs for secure remote connections.
Department Managers	Ensure that your departments' systems and data are located on appropriately segmented networks and that staff comply with security and information sharing policies.
Network and Systems Users	Comply with network security and information sharing policies, and report any incidents or suspicious activity.

BUSINESS PROCESSES AFFECTED.

IT Management

Processes related to the administration and operation of networks and information exchange systems.

Security Management

Monitoring and response processes to security incidents related to networks and information exchange.

Daily Operations

Safe and appropriate use of networks and information exchange systems by the organization's staff.

EXCEPTIONS

In exceptional cases, certain networks, segments, systems or types of information may be excluded from this policy due to technical or business restrictions. These exceptions must be approved by the Information Security Officer and appropriately documented. Exceptions may include:

- Temporary networks that do not contain critical information or systems.
- Network segments used for testing or development that do not require the same levels of security.
- Legacy systems that do not support modern encryption and are in the process of being replaced.
- Public information that does not require encryption in transit.

RELATED DOCUMENTS AND OTHER REFERENCES

This policy should be read in conjunction with the following documents and policies:

- Information Security Policy
- Incident Management Procedures

CONTACTS MATRIX

CONTACT TYPE	CONTACT	PHONE	EMAIL
Information Security Officer	Ana Martinez	2451 6217	amartinez@empresa.com
Security Coordinator	Laura Gomez	8945 2571	lgomez@empresa.com
Security Auditor	Javier Fernandez	6851 0144	jfernandez@empresa.com
Network Administrator	Jesus Perez	3694 2151	jperez@empresa.com

REGULATORY REFERENCES AND LEGAL FRAMEWORK

This policy is aligned with the following rules and regulations:

- Control 13.1 of ISO/IEC 27002:2013 Network security management
- Control 13.2 of ISO/IEC 27002:2013 Information exchange
- ISO/IEC 27001: International standard for information security management systems.
- Personal Data Protection Act: Local and national regulations on the protection of personal data.
- General Data Protection Regulation (GDPR): European regulation on the protection of personal data and privacy.
- National Institute of Standards and Technology (NIST): Standards and guidance on cybersecurity and data encryption.
- Payment Card Industry Data Security Standard (PCI DSS): Regulations for data security in payment card transactions.

Fictitious Company

White River
2415-0001

POLICY NAME	Security in the system life cycle	POLICY NO.	8
		VERSION NO.	1.0
RESPONSIBLE ADMINISTRATOR	Stanley Martinez	EFFECTIVE DATE	06/20/2024
CONTACT INFORMATION	cvd@respon.com	DATE OF LAST REVIEW	06/15/2024

VERSION HISTORY				
VERSION	APPROVED BY	REVIEW DATE	DESCRIPTION OF CHANGE	AUTHOR
1.0	Senior Management	11 / 06 /2024	Creation of the policy	Stanley Martinez

AIM

Establish a comprehensive framework for the secure management of the information systems lifecycle. This involves protecting systems from unauthorized access, ensuring accuracy, and ensuring that services are available when needed. The policy also seeks to identify and mitigate risks.

POLICY STATEMENT

This policy establishes clear and detailed guidelines for securely and effectively managing the lifecycle of information systems at the Fictitious Company in Rio Blanco. Recognizing the importance of information as a critical asset, it focuses on protecting the confidentiality, integrity and availability of data throughout all stages of the system lifecycle, from development and acquisition to implementation, maintenance and eventual disposal. These controls include access management, protection against threats and vulnerabilities, security testing, continuous monitoring of systems, and response and recovery from security incidents.

Additionally, the importance of training and awareness is emphasized to promote a culture of continuous improvement in the management of information security, the adaptation of security controls to technological changes and new emerging threats, in order to protect the interests of the organization and its stakeholders.

SCOPE

This policy applies to all information systems, devices, applications, networks, and data owned or controlled by the organization. It also covers all stages of the information systems life cycle, from development and acquisition to implementation, maintenance, and eventual disposal. It is applicable to any activity that may impact information handled by the organization. All individuals and entities covered by this policy must strictly adhere to its guidelines to ensure the proper protection of information assets.

TERMS AND DEFINITIONS

TERM	DEFINITION
System life cycle	All the phases that an information system goes through, from its conception to its elimination.

Guidelines	Detailed guidance on how to implement and comply with information security policy in specific situations involving suppliers.
Critical asset	resource, system, or component of an organization whose loss, damage, or compromise would have a significant impact on the operations, security, or survival of the organization.

ROLES AND RESPONSIBILITIES

ROLE	RESPONSIBILITY
Information Security Manager	Responsible for overseeing policy implementation and ensuring security requirements are met at all stages of the system lifecycle.
Internal Auditor	Conduct periodic reviews to ensure that security controls and procedures are followed properly.
IT Manager	Monitor policy implementation and ensure compliance with safety standards.

BUSINESS PROCESSES AFFECTED.

RISK ASSESSMENT

This process involves identifying, analyzing, and assessing the security and operational risks associated with the system lifecycle. Potential risks must be considered at each stage of the lifecycle, from planning to system deployment, and measures must be applied to mitigate these risks.

SYSTEM IMPLEMENTATION

System implementation encompasses the development, testing, and deployment of the system itself.

MAINTENANCE AND UPDATE

It involves continuous monitoring of the system to detect and correct potential vulnerabilities and security flaws.

EXCEPTIONS

Exceptions will be considered in cases where strict application of the policy may cause a negative impact on the operability of the system. Exceptions must be adequately documented and must include alternative measures to mitigate the identified risks. These must be reviewed periodically to ensure that they remain necessary and that appropriate risk mitigation measures are maintained.

RELATED DOCUMENTS AND OTHER REFERENCES

This policy should be read in conjunction with the following documents:

- Security procedures in the system life cycle

CONTACTS MATRIX

CONTACT TYPE	CONTACT	PHONE	EMAIL
Information Security Manager	Pablo Diaz	7623- 2342	pdiaz@seguridad.com
Internal Auditor	Gonzalo Gonzales	8634-0010	ggonzale@auditor.com
IT Manager	Santiago Alone	4563-9809	ssolito@ti.com

REGULATORY REFERENCES AND LEGAL FRAMEWORK

ISO 27002 Domain 14:

- control 14.2 - Security in systems development and support.

Fictitious Company

White River
2415-0001

POLICY NAME	Relationship with suppliers	POLICY NO.	9
		VERSION NO.	1.0
RESPONSIBLE ADMINISTRATOR	Stanley Martinez	EFFECTIVE DATE	06/20/2024
CONTACT INFORMATION	cvd@respon.com	DATE OF LAST REVIEW	06/15/2024

VERSION HISTORY				
VERSION	APPROVED BY	REVIEW DATE	DESCRIPTION OF CHANGE	AUTHOR
1.0	Senior Management	11 / 06 /2024	Creation of the policy	Stanley Martinez

AIM

Establish and implement a set of guidelines to manage information security in Fictitious Company in Rio Blanco's supplier relationships. These guidelines ensure that sensitive data and critical systems are adequately protected, thereby reducing security risks and strengthening trust in business relationships with suppliers.

POLICY STATEMENT

You recognize that information security depends on both your internal practices and the information security practices of your suppliers. All contracts with suppliers should contain specific clauses on information security. These agreements will detail information protection requirements, responsibilities, and expected security measures. In addition, periodic assessment of suppliers' security practices will be performed to ensure ongoing compliance. Suppliers must allow security audits to be performed by the Shell Company or designated third parties.

Upon termination of a supplier relationship, all sensitive information will be ensured to be returned or securely destroyed. Supplier access to systems will be reviewed and updated to ensure no unauthorised access remains. This comprehensive approach ensures that sensitive information is protected at all stages of the supplier relationship.

SCOPE

This policy applies to all suppliers who interact with the Fictitious Company in Rio Blanco and who have access to confidential information or critical systems of the organization. All suppliers, regardless of their size or scope of services, are subject to these guidelines to ensure the appropriate protection of confidential data and critical systems. The application of this policy is mandatory and forms an integral part of any contractual agreement with suppliers of the Fictitious Company in Rio Blanco.

TERMS AND DEFINITIONS

TERM	DEFINITION
Audits	Systematic and objective evaluation of a supplier's information security practices to verify compliance with established standards and requirements.
Guidelines	Detailed guidance on how to implement and comply with information security policy in specific situations involving suppliers.

ROLES AND RESPONSIBILITIES

ROLE	RESPONSIBILITY
Senior Management	Provide the necessary support for the implementation and maintenance of the ISMS
Information Security Officer	Evaluate and monitor compliance with this policy by suppliers
Contract Manager	Ensure that supplier agreements include information security clauses
Suppliers	Comply with the information security policies and procedures established by the company

BUSINESS PROCESSES AFFECTED.

ACQUISITION OF SYSTEMS

A thorough assessment of the provider's information security practices will be conducted. This assessment will include a review of the security measures implemented by the provider on its systems, as well as its compliance with the security standards established by the Fictitious Company in Rio Blanco.

SYSTEMS DEVELOPMENT

These will be required to comply with the security protocols established by the company. This involves following appropriate procedures during the design and development of the systems, including the implementation of appropriate security measures. Periodic reviews will be conducted during the development process to ensure continued compliance with the company's security standards and to ensure that the resulting systems are secure and stable.

SYSTEMS MAINTENANCE

They will be required to adhere to the company's security standards. This includes managing patches, updates and repairs in a secure and efficient manner. Clear procedures will be established for managing changes to systems, ensuring that any modifications do not compromise information security. In addition, regular audits will be conducted to verify ongoing compliance with the company's security standards and ensure the integrity of systems and data.

EXCEPTIONS

In exceptional cases where a supplier demonstrates that it has implemented information security measures that are equivalent or superior to those required by the company, an exception to certain aspects of the policy may be considered. This exception must be evaluated on a case-by-case basis by the information security officer and will require management approval. Detailed records of the evaluation and approval of these exceptions must be maintained.

RELATED DOCUMENTS AND OTHER REFERENCES

This policy should be read in conjunction with the following documents:

- Supplier relationship procedures.

CONTACTS MATRIX

CONTACT TYPE	CONTACT	PHONE	EMAIL
Senior Management	Jose Perez	7623- 2342	jperez@undominio.com
Information Security Officer	Roberto Garcia	8634-0010	robgarcia@address.com
Contract Manager	Francisca Palma	4563-9809	frpalma@seguridad.com
Suppliers	Orlando Salas	7654-4353	orlsalas@provider.com

REGULATORY REFERENCES AND LEGAL FRAMEWORK

ISO 27002 Domain 15:

- Control 15.1 - Security in the relationship with suppliers.

ADDITIONAL NOTES

It is the responsibility of each department or business unit to ensure that the suppliers with whom they interact comply with the information security policies established by the company. Any breach or security incident must be reported to the information security department in a timely manner.

Fictitious Company

White River
2415-0001

POLICY NAME	Information Security Incident Management	POLICY NO.	10
		VERSION NO.	1.0
RESPONSIBLE ADMINISTRATOR	Stanley Martinez	EFFECTIVE DATE	06/20/2024
CONTACT INFORMATION	cvd@respon.com	DATE OF LAST REVIEW	06/15/2024

VERSION HISTORY				
VERSION	APPROVED BY	REVIEW DATE	DESCRIPTION OF CHANGE	AUTHOR
1.0	Senior Management	11 / 06 /2024	Creation of the policy	Stanley Martinez

AIM

Establish a comprehensive framework that enables the identification, management and effective response to information security incidents at the Fictitious Company in Rio Blanco. This policy aims to ensure the protection of information assets, the continuity of critical processes and the minimization of adverse impacts caused by security incidents.

POLICY STATEMENT

Establish a framework for action that allows for the timely and effective detection, analysis and response to any incident that may affect the company's information security. It also seeks to promote continuous improvement in information security processes by identifying and applying lessons learned from incidents, in order to strengthen the company's resilience against potential threats.

Furthermore, the policy seeks to promote a culture of information security throughout the company's staff, fostering awareness of the importance of security and individual responsibility in its protection. This policy is expected to be a key instrument for the efficient management of information security incidents, ensuring the continuity of operations and the protection of the information assets of the Fictitious Company in Rio Blanco.

SCOPE

It applies to all employees, suppliers and partners of the company who have access to, handle or process sensitive or critical information. This policy covers the detection, reporting, analysis, response and monitoring of information security incidents, as well as the implementation of continuous improvements in security processes. This policy includes information assets and information systems of the company, regardless of their physical location or type of technology used. In addition, it extends to continuous improvement processes based on lessons learned from incidents, to strengthen the company's security posture.

TERMS AND DEFINITIONS

TERM	DEFINITION
Information Security Incident	Any event that compromises the confidentiality, integrity or availability of information.
Continuous Improvement	Systematic and continuous process to improve the effectiveness and efficiency of information security controls and processes.

ROLES AND RESPONSIBILITIES

ROLE	RESPONSIBILITY
Project Manager	Responsible for the implementation and compliance of this policy.
Information Security Incident Management Team	Responsible for managing information security incidents and implementing improvements.

BUSINESS PROCESSES AFFECTED.

RISK ASSESSMENT

This process involves identifying and analyzing the security risks associated with the company's information system. The aim is to determine the probability of a security incident occurring and the impact it could have on the organization.

SYSTEM IMPLEMENTATION

The information security system is developed, tested and implemented. It is ensured that the necessary security controls are applied to protect the company's information.

MAINTENANCE AND UPDATE

This process involves continuous monitoring and updating of the information security system. Improvements and adjustments are made to maintain the security and functionality of the system in response to changes in threats and vulnerabilities.

RELATED DOCUMENTS AND OTHER REFERENCES

This policy should be read in conjunction with the following documents:

- Information security incident management procedures

CONTACTS MATRIX

CONTACT TYPE	CONTACT	PHONE	EMAIL
Project Manager	Laura Salas	7623- 2342	lsalas@gproyecto.com
Information Security Incident Management Team	Oscar Colocho	8634-0010	ocolocho@seguridad.com

REGULATORY REFERENCES AND LEGAL FRAMEWORK

ISO 27002 Domain 16:

- Annex A.16.1 - Information security incident management and improvements.

ADDITIONAL NOTES

The policy will be reviewed periodically to ensure that it remains relevant and effective in protecting information and continually improving processes related to information security.

Fictitious Company
White River
2415-0001

POLICY NAME	Legal compliance and information security	POLICY NO.	11
		VERSION NO.	1.0
RESPONSIBLE ADMINISTRATO R	Stanley Martinez	EFFECTIVE DATE	06/20/2024
CONTACT INFORMATION	cvd@respon.com	DATE OF LAST REVIEW	06/15/2024

VERSION HISTORY				
VERSIO N	APPROVED BY	REVIEW DATE	DESCRIPTION OF CHANGE	AUTHOR
1.0	Senior Management	11 / 06 /2024	Creation of the policy	Stanley Martinez

AIM

Ensure compliance with legal and contractual requirements related to information security in the Rio Blanco Fictitious Company. The aim is to identify, implement and maintain effective measures and controls, promoting a culture of security and establishing a process of continuous improvement.

POLICY STATEMENT

The information security policy of the Fictitious Company in Rio Blanco has as its main objective to establish a comprehensive framework for the protection of information, ensuring its confidentiality, integrity and availability, as well as compliance with applicable legal and contractual requirements. To achieve this objective, measures will be implemented to identify and manage information security risks, promoting a security culture throughout the organization and continuously improving security controls and processes. In addition, clear responsibilities are assigned for the management of information security.

SCOPE

It covers all aspects related to information security at the Fictitious Company in Rio Blanco, including the protection of confidential and sensitive information, the prevention of unauthorized access, the management of security risks, compliance with legal and contractual regulations, and the promotion of a security culture. Regardless of its location or the medium used for processing information. All those involved are expected to comply with this policy and actively contribute to its implementation and maintenance.

TERMS AND DEFINITIONS

TERM	DEFINITION
legal requirements	obligations that an organization must meet to operate legally and ethically in its environment.
contractual requirements	specific obligations and conditions established in a contract that the parties involved must comply with.

ROLES AND RESPONSIBILITIES

ROLE	RESPONSIBILITY
Information Security Manager	ensure that the company complies with all legal and contractual requirements related to information security.
Internal Security Review Team	An internal team responsible for conducting periodic information security reviews within the company.
Legal adviser	A legal advisor who provides guidance on legal issues related to information security. He or she must ensure that the company complies with all applicable laws and regulations in its operation.
Internal Information Security Auditor	Responsible for conducting periodic internal audits to assess compliance with information security policies and procedures, including legal and contractual compliance.
Head of Information and Technology	Responsible for supervising the security of information and technology used in the company.

BUSINESS PROCESSES AFFECTED.

Marketing and Promotion of Products

Compliance and security review policies can impact this process by establishing measures to ensure that the promotion is conducted ethically and complies with local and international regulations.

Information Management

It covers the collection, storage and management of information related to the company's products, customers, suppliers and operations. The information security policy can affect this process by establishing security protocols to protect sensitive information.

Supplier Management

This process involves the selection, contracting, and monitoring of suppliers who provide materials and services to the company. The legal compliance policy can affect this process by establishing legal requirements that suppliers must comply with.

Security Incident Management

This process relates to the identification, response to, and mitigation of information security incidents. The information security review policy may impact this process by establishing procedures for reporting and handling security incidents.

Internal Audit

This process involves conducting internal audits to assess compliance with information security policies and procedures. The legal compliance and security review policy may impact this process by establishing criteria and frequency for internal audits.

EXCEPTIONS

In the event of a natural disaster, such as an earthquake or flood, that impacts the availability of resources or the physical security of facilities, the information security review may be postponed until the situation has normalized and it is safe to conduct the review.

RELATED DOCUMENTS AND OTHER REFERENCES

This policy should be read in conjunction with the following documents and policies:

- Legal compliance procedures and information security

CONTACTS MATRIX

CONTACT TYPE	CONTACT	PHONE	EMAIL
Information Security Manager	Oscar Colocho	7623- 2342	ocolocho@seguridad.com
Internal Security Review Team	Manuel Portillo	8634-0010	mportillo@rvisionin.com
Legal adviser	Ana Gutierrez	4563-9809	agutierres@legal.com
Internal Information Security Auditor	Alfredo Pascal	7623- 2342	apascal@sinterno.com
Head of Information and Technology	Melvin Ortiz	8634-0010	mortiz@rinfotec.com

REGULATORY REFERENCES AND LEGAL FRAMEWORK

ISO 27002 Domain 18:

- Control 18.1 of ISO/IEC 27002:2013 - Compliance with legal and contractual requirements.
- Control 18.2 of ISO/IEC 27002:2013 - Information security reviews.

ADDITIONAL NOTES

This policy applies to all areas and processes of the Fictional Company in Rio Blanco, including the display, sale and promotion of artisanal clay products.