GENESIS
International Group

Information Security Policy

VERSION 4.5
Jul. 25, 2024

TABLE OF CONTENTS

1. Revisions and authorizations

Change Log:

Date	Author(s)	Version	Comments
11/11/2020	Felipe Ramírez – Chief Technology Officer	1.0	First version of the integrated document
30/10/2021	Felipe Ramírez – Chief Technology Officer	2.0	Policy update
01/11/2022	Felipe Ramírez – Chief Technology Officer	3.0	Policy update
30/10/2023	Felipe Ramírez – Chief Technology Officer	4.0	Policy update
25/07/2024	Felipe Ramírez – Chief Technology Officer	4.5	Policy update including new documents related to DRP procedures and Access Control.

2. Introduction.

The Information Security Policy (hereinafter referred to as "the Policy") aims to adopt a set of measures intended to preserve the confidentiality, integrity, and availability of information. These constitute the three basic components of information security and aim to establish the requirements to protect the information, equipment, and technological services that support most of the business processes of Genesis International Group.

3. Company description.

Genesis International Group is a conglomerate specializing in the acquisition and management of distressed credit portfolios with experience in Latin America and the Caribbean, based in Miami, FL.

4. Mission and vision.

Identify high-yield and low-risk investment opportunities by analyzing and studying the economic structure of our investment portfolios and applying our professional management skills to generate attractive returns and create a positive impact on the economy.

Successfully become one of the leading investment firms in the distressed asset market, offering not only consulting to future or current investors but also effective tools and training in the management process from start to finish.

5. Policy scope.

This Policy is applicable to the entire Genesis Group and must be followed by all areas of the company. It must be available on Genesis's corporate website genesisintgroup.com to be accessible by all members of the group. The scope of this Policy covers all information of the Group's subsidiaries, regardless of how it is processed, who accesses it, the medium that contains it, or where it is located, whether it is printed or electronically stored information.

6. Information policy principles.

This Policy responds to the recommendations of best practices in Information Security collected in the ISO 27001 International Standard, as well as the compliance with the current legislation on data protection and the regulations that may affect Genesis Group in the field of Information Security. The basic principles of the policy include:

- **Strategic Scope:** Information security must have the commitment and support of all management levels.
- **Comprehensive Security:** Information security will be understood as an integral process consisting of technical, human, material, and organizational elements.
- **Risk Management:** The analysis and management of risks will be an essential part of the information security process.
- **Proportionality:** Protective measures must be proportional to the risks and criticality of the information.
- **Continuous Improvement:** Security measures will be re-evaluated and updated periodically.

7. IT Management commitment.

The IT Management of Genesis Group commits to:

- Promote roles and responsibilities in the field of information security.
- Provide the necessary resources to achieve information security objectives.
- Promote the dissemination and awareness of the Policy among employees.
- Enforce compliance with the Policy, current legislation, and regulatory requirements.
- Consider information security risks in decision-making processes.

8. Roles and responsibilities

- **Security Strategy Manager:** CTO.
- **Daily Operations Manager and Information Security Officer**: IT Manager.
- **Responsibilities of all Managers:** Managers are individually responsible for security in their environments where information is processed or stored. Additionally, they are responsible for:
    - Ensuring that all permanent, temporary, and/or contractor personnel are aware of the information security policies, procedures, and user obligations applicable to their work area, as well as their personal responsibilities in terms of information security.
    - Determining the level of access to be granted to specific individuals.
    - Ensuring that personnel receive adequate training for the systems they use.
    - Ensuring that personnel know how to access advice on information security matters.
- **Responsibilities of all employees:** All personnel are responsible for information security and must therefore understand and comply with this policy and associated guidelines. Non-compliance with this policy may result in disciplinary action. In particular, all personnel must understand:
    - What information they are using, how it should be used, stored, and transferred in terms of data security.
    - What standard procedures and protocols exist for exchanging information with other parties.
    - How to report a potential information security breach within the organization.
    - Their responsibility to raise any concerns related to information security.
- All Genesis Group users are responsible for complying with the provisions of this Policy and all related standards, guidelines, and procedures and must report any incidents of misuse or abuse of which they are aware as described in Genesis Group's Security Incident Management Policy.

9. Risk Management.

- **Risk Assessment**:
    - Risk assessment is conducted every six months through an internal seven-step process:
        1. Establish and define a risk assessment framework.
        2. Inventory information assets.
        3. Identify vulnerabilities and potential threats.
        4. Determine the impact of threats.
        5. Create a risk management plan.
        6. Prepare and compile information security risk assessment reports.
        7. Review, monitor, and test the effectiveness of risk management.

- **Risk Mitigation**:
    - Avoidance: Eliminate the root cause of the problem whenever possible and financially feasible.
    - Mitigation: Reduce the likelihood of occurrence, the potential damage, or both..

10. Security Controls

- **Access Control**:

All Genesis Group information systems must have an access control system. Additionally, access control focuses on ensuring user access and preventing unauthorized access to information systems, including measures such as password protection.

- **Business Requirements for Access Control**:
    - Users must be unique and cannot be shared. User privileges will initially be assigned based on the principle of least privilege.
    - The use of generic users is prohibited. Instead, user accounts will be associated with the nominal identity of the associated person.
    - Whenever possible, multi-factor authentication (MFA) must be provided for accessing information systems, which is mandatory for those accessible from public networks.

- **Access Rights**:
    - Genesis Group must implement access controls that ensure users are granted only the privileges and rights necessary to perform their function.
    - Access rights should be established based on:
        - Role-Based Access Control (RBAC): Profiles or access roles for applications and/or systems must be established to assign them to different users.
        - Need to Know: Access to a resource will only be allowed when there is a legitimate need for business purposes.
        - Minimum Privileges: Permissions granted to users must be minimal.
        - Separation of Duties: Proper separation of duties must be ensured to develop and assign access rights.

- **Logical Access Control**:
    - Genesis Group must establish a password policy aligned with best practices in security. The password policy will define password requirements and maintenance timelines.
    - The password policy must be known to all Genesis Group employees.

- **Remote Work**:

Remote access to the Genesis Group network in teleworking mode, i.e., from outside the company's facilities, must be controlled.

The remote work connection services will be exclusively for Genesis Group personnel. Their use by any other type of collaborator requires authorization from the security officer.

The equipment used for remote work may be owned by the employee or provided by Genesis Group. In any case, the equipment must meet the following security requirements:

- Ability to connect through a VPN.
- Updated operating system with the latest patches and security updates.
- Installed antivirus software.
- Installed personal firewall software.

Teleworking from an employee's personal equipment requires all appropriate security measures to ensure that remote work does not pose a threat to Genesis Group's information security. Additionally, additional security measures may be established to ensure a more reliable secure remote connection.

The teleworking service will be monitored and controlled, logging both the connection and activity according to security protocols.

11. Incident response.

All Genesis Group employees have the obligation and responsibility to identify and notify the company's security officer of any incident or crime that could compromise the security of its information assets as soon as possible by sending an email to security@genesisintgroup.com. Additionally, to ensure an effective incident response, Genesis Group must implement the following procedures:

- **Incident management procedures**:
  - A detailed procedure for incident response management must be defined.
  - The procedure must include an incident categorization process, business impact analysis, and escalation by the information security and cybersecurity function for any incident related to information security.
  - This procedure must be known and understood by all employees and must include the following steps:

    1. **Incident Identification:** Immediate detection and reporting of any unusual or suspicious activity that may represent a threat.
    2. **Incident Classification:** Initial assessment to determine the severity and potential impact of the incident.
    3. **Notification and Escalation:** Communication of the incident to appropriate levels within the organization, including senior management if necessary.
    4. **Containment and Mitigation**: Immediate actions to contain and limit the effects of the incident, minimizing damage.
    5. **Eradication and Recovery:** Elimination of the root cause of the incident and restoration of affected systems to their normal state.

6. **Post-Incident Analysis:** Detailed assessment of the incident to understand its cause and develop preventive measures to avoid future occurrences.
7. **Reporting and Documentation:** Complete documentation of the incident, the actions taken, and the lessons learned, and reporting to relevant stakeholders.

- **Roles and responsibilities**:
  - **Information Security Officer**: Coordinate the incident response, ensuring that all steps in the procedure are correctly executed.
  - **Employees:** Identify and report security incidents. Participate in containment and recovery as necessary.
  - **Senior Management:** Oversee the handling of critical incidents and make strategic decisions for risk management.

- **Training and Awareness**:
  Employees must receive regular training on detecting and reporting security incidents. This training must include:
  - Identification of common threats and suspicious behaviors.
  - Notification and escalation procedures.
  - Roles and responsibilities in incident management.

  Incident drills should be conducted to assess the effectiveness of procedures and the preparedness of employees.

- **Monitoring and Detection**:
  Implement continuous monitoring systems to detect and alert on potential security incidents.
  Use advanced intrusion detection tools and behavior analysis to identify suspicious activities.

- **Review and Continuous Improvement**:
  - Periodically review incident management procedures to ensure their effectiveness and update as necessary.
  - Incorporate lessons learned from past incidents to improve security policies and procedures.

These procedures are an integral part of Genesis Group's security strategy, ensuring a fast and effective response to any information security incident

12. Compliance and audit

- **Regulations and Standards**:
  - Compliance with ISO 27001.
  - Mexican Data Protection Law (LFPDPPP).

    - Semi-annual review to ensure continuous compliance.
    - GDPR (General Data Protection Regulation).
- **Security Audits**:
    - Conduct annual audits by internal personnel.
    - Annual audits by external suppliers.

13. Human Resource Security Management

The Human Resources department of Genesis Group must manage its processes considering the security criteria established in the Information Security Policy. The requirements set forth in this Policy must be safeguarded at all times, including the pre-employment phase, employment phase, and employee contract termination phase.

Training and Awareness:

- Genesis Group must ensure that all personnel receive an adequate level of training and awareness on Information Security every six months, especially regarding confidentiality and prevention of information leaks.
- Employees must be informed every three months about updates to security policies and procedures that affect them and about existing threats to ensure compliance with this Policy.
- Employees are obligated to act diligently with respect to information, ensuring that such information does not fall into the hands of unauthorized employees or third parties.

Clean Desk Policy:

- Workstations must be locked when the employee leaves the desk, both manually (user lock) and automatically through screen lock settings.
- The workspace must be tidied up at the end of the workday. This includes ensuring that all documents or information media are out of sight, with confidential or secret documents locked away.
- Workstations must be kept orderly and free of documents or information media that can be seen or accessed by others.

14. Asset management

All information assets necessary for the delivery of Genesis Group's business processes must be identified and inventoried. Additionally, the asset inventory must be kept up to date.

- **Asset Classification:**

  Assets must be classified according to the type of information they handle, in line with the provisions in Section 14, Information Classification.

- **Asset Responsibility:**

  A responsible individual must be assigned to manage information assets throughout their lifecycle. The responsible person must maintain a formal record of authorized users of the asset.

For each asset or information item, there must be a responsible owner who will ensure that the asset is correctly inventoried, classified, and adequately protected.

- **Asset Update:**

Asset configurations must be updated periodically to allow tracking and facilitate proper information updates.

- **BYOD (Bring Your Own Device) or Personal Device Management:**
  - Genesis Group will allow a BYOD policy, enabling employees to use their personal mobile devices to access Genesis Group's resources or information.
  - Users must adhere to a series of requirements established in this Policy:
    - Apply the same security measures and configurations to BYOD devices that handle information as with other Genesis Group devices.
    - The user is responsible for the BYOD equipment.
    - Keep the BYOD device used for handling Genesis Group information up to date. Security applications must be installed via MDM (Mobile Device Management) software provided by the IT department to prevent security breaches on those devices.
    - Obtain authorization from their area manager to use BYOD devices.
    - Report any incidents that could affect the confidentiality, integrity, or availability of these devices to the security officer.
- **Information Lifecycle Management:**

  The lifecycle of an information asset consists of the following phases:

  1. Creation or Collection: Records at their point of origin, including correspondence, forms, reports, drawings, input/output from computers, or other sources.
  2. Distribution: Management of the information once created or received, including internal and external distribution.
  3. Use or Access: Performed after distribution, may generate business decisions, create new information, or serve other purposes.
  4. Storage: Organizing the information in a predetermined sequence and creating a management system to ensure its usefulness within Genesis Group.
  5. Destruction: Elimination of information that has met its defined retention periods and is no longer useful to Genesis Group, ensuring its confidentiality during the destruction process.

Identify security measures according to this Policy to ensure the proper management of the asset lifecycle.

- **Backup Management:**
  - Perform backups of information, software, and systems and periodically verify them.

  - Backup copies must receive the same security protections as the original data, ensuring their proper preservation and adequate access controls.
  - Periodically test backup restoration and document the restoration processes.
  - Establish a retention period for backups until their destruction once the existence period has ended.
  - Place backups in secure locations with restricted access, preferably in a center different from where they were generated.
  - Ensure an additional backup of sensitive information, protected against writing to guarantee its integrity in the event of security incidents.

15. Information classification

A classification model must be defined to allow the implementation of necessary technical and organizational measures to maintain the availability, confidentiality, and integrity of the information. The classification model must integrate the requirements and conditions established in this section of the Policy.

- **Types of Information:**
  - Logical Media: Information used through office tools, email, or custom-developed or third-party acquired information systems.
  - Physical Media: Information in paper, magnetic media such as USBs, Hard Drives, etc.
- **Classification Levels:**
  - Public Use: Information that can be known by anyone and whose fraudulent use does not pose a risk to Genesis Group's interests.
  - Limited Distribution: Information used by Genesis Group areas whose fraudulent use poses a minor risk to the Group's interests.
  - Confidential Information: Information that can only be known by a limited number of people and whose fraudulent use can have a significant impact on Genesis Group's interests.
  - Restricted Information: Information that should only be known by its owner and whose disclosure can cause serious harm to Genesis Group's interests.
  - Secret Information: Information whose unauthorized disclosure can cause exceptionally grave harm to Genesis Group's essential interests.
- **Privileged Information Management:**
  - Information considered restricted, confidential, or secret must be handled with special care. Additional or extraordinary security measures must be defined for the appropriate handling of privileged information.
  - This type of information must be sent encrypted and through secure protocols.
- **Information Labeling:**
  - Label information using manual methods or, where possible, automated methods to facilitate the appropriate processing of applicable security measures in each case.
  - Ensure that information labeling reflects the adopted classification scheme and is easily recognizable by all employees.

    - Guide employees on where and how to place or use labels based on the information access process or the assets that support it.
    - Define a process or procedure for information labeling, ensuring training and education for all employees on information labeling, and specifically train employees handling restricted or secret information.
- **Information Handling:**
    - Develop and implement appropriate procedures for the correct handling of information, protecting it according to its classification.
    - Privileged information will be safeguarded throughout its lifecycle.
- **Information Privacy:**
    - Ensure the privacy of personal data to protect the fundamental rights of individuals, complying with current personal data protection legislation according to applicable jurisdiction.

16. Information Leakage Prevention

Information leakage is an uncontrolled exit of information, whether intentional or not, that causes it to reach unauthorized people or causes its owner to lose control over third-party access to it.

To prevent information leakage, Genesis Group must implement the following measures:

- Leakage Vectors Analysis:
    - Analyze information leakage vectors based on the working conditions and operations of each Genesis Group entity.
    - Identify the assets whose leakage poses the greatest risk for each entity, based on the asset's criticality and the information classification level.
    - Identify possible avenues for theft, loss, or leakage of each asset in its different lifecycle states.
- Procedure Definition:
    - Define procedures to prevent situations that could cause information loss.
    - Establish procedures for action in case of an information leakage report.
- Training and Education:
    - Ensure the training and education of all employees on best practices for information leakage prevention.
    - The training must cover at least the following aspects:
        - Process for handling highly critical known devices.
        - Proper use of removable devices such as USBs, CD/DVDs, or similar.
        - Use of email.
        - Oral transmission of information.
        - Document printing.
        - Document exit.
        - Use of mobile devices.
        - Use of the internet.
        - Clean and organized desks.

- Unattended equipment.

17. Cloud computing security

Genesis Group, as a client of AWS Cloud Computing services, is committed to maintaining a robust cloud policy that ensures the confidentiality, integrity, and availability of information. Depending on the cloud service model (IaaS, PaaS, SaaS), different security measures will be applied. Below are some measures for each service model. For more details, refer to the document: "Guide_SharedControls."

17.1. Infrastructure as a Service (IaaS)

- **Environment Monitoring:**
  - Ensure that AWS as a provider monitors the environment for unauthorized changes and any anomalous activity.
  - Implement monitoring and alerting tools to detect and respond to security incidents in real-time.

- **Authentication and Access Control:**
  - Establish strong multi-factor authentication (MFA) levels for all administrators and users with privileged access.
  - Regularly control and audit accesses and actions performed by administrators and privileged users.
  - Manage access through role-based access control (RBAC) policies and the principle of least privilege.
- **Traceability and Logging:**
  - Maintain detailed logs of all installations, configurations, and changes in infrastructure elements.
  - Ensure that all logs and records are securely stored and retained according to data retention policies.

17.2. Platform as a Service (PaaS)

Software Lifecycle Security:

- Implement secure development practices (SDLC) including code reviews, penetration tests, and vulnerability analysis.
- Use security scanning tools and static code analysis (SAST) to identify and remediate vulnerabilities during development.

Configuration Controls:

- Ensure that all platform configurations are securely managed and regularly audited.
- Implement timely patch management and security update policies.

Data Protection:

- Use strong encryption for data at rest and in transit.
- Implement strict access controls for databases and other platform components.

17.3. Software as a Service (SaaS)

Application Security:

- Follow OWASP (Open Web Application Security Project) best practices for application security.
- Conduct regular security tests, including penetration testing and code audits.

Identity and Access Management:

- Implement identity and access management (IAM) solutions that include multi-factor authentication and role-based access control.
- Ensure that users have access only to the data and functionalities necessary for their specific role.

Customer Data Protection:

- Ensure that all customer data is encrypted both in transit and at rest.
- Implement privacy and data protection policies aligned with local and international regulations like GDPR and CCPA.

17.4. Cloud Incident Management

Detection and Response:

- Implement a cloud-specific incident response plan that includes detection, containment, eradication, and recovery.
- Use AWS services like AWS CloudTrail, AWS Config, and AWS GuardDuty for monitoring and incident response.

Coordination and Communication:

- Establish clear communication and escalation procedures in case of cloud security incidents.
- Maintain a trained and prepared incident response team (IRT) to act in the event of any security incident.

18. Security in the Software Development Lifecycle

Security in the Software development lifecycle is essential to ensure the protection of Genesis Group's information and technological systems. All stages of software development, from acquisition to maintenance, must meet minimum security requirements according to industry best practices. The following policies and procedures must be followed to ensure secure development:

18.1. Security Requirements in Software Development

- **Standards and Best Practices:**
  - Software development must follow the security standards established by OWASP (Open Web Application Security Project).
  - Implement secure development practices (SDLC) that include code reviews, penetration tests, and vulnerability analysis.
- **Risk Analysis:**

  - Conduct risk analyses before the start of any software development project to identify potential vulnerabilities and determine necessary security measures.
  - Update risk analyses at each development phase to address any new threats that may arise.
- **Security Requirements:**
  - Clearly define and document security requirements for each development project, ensuring they are included in all phases of the system development lifecycle.
  - Ensure that security requirements are aligned with Genesis Group's information security policies.

18.2. Test Management

- **Security Testing:**
  - Conduct security tests at each development phase, including penetration tests, static and dynamic code analysis, and vulnerability assessments.
  - Implement automated testing to verify software security during continuous development (CI/CD).
- **Test Environments:**
  - Use test environments representative of the production environment to ensure accurate test results.
  - Ensure that data used in test environments is anonymized or encrypted to protect privacy and confidentiality.

17.3. Change Tracking

- **Change Control:**
  - Establish a formal change management process that includes security risk assessments associated with any software or development environment changes.
  - Document and approve all changes before implementation, ensuring security tests are conducted to validate the system's integrity and security after changes.
- **Change Auditing:**
  - Maintain detailed records of all changes made to software and development environments.
  - Conduct periodic audits to ensure changes are managed according to established security policies.

17.4. Software Inventory

- **Inventory Management:**
  - Maintain an updated inventory of all software components used, including libraries, frameworks, and third-party tools.
  - Regularly evaluate software components to identify and mitigate potential vulnerabilities.
- **Updates and Patches:**
  - Ensure all software components are kept up to date with the latest patches and security updates.
  - Implement a patch management process to ensure security updates are applied promptly.

19. Disciplinary actions

Any violation of this Information Security Policy may result in the corresponding disciplinary actions according to Genesis Group's internal processes. All Genesis Group employees are responsible for notifying the affected entity's Information Security Officer of any event or situation that could lead to non-compliance with any of the guidelines defined in this Policy.

20. Business continuity

In response to quality requirements and best practices, Genesis Group has a Business Continuity Plan (BCP) as part of its strategy to ensure the continuity of its essential or critical services and the proper management of business impacts in potential crisis scenarios. This BCP is complemented by a Disaster Recovery Plan (DRP) that ensures the continuity of information and communication technologies.

20.1. Business Continuity Plan (BCP)

20.2. Disaster Recovery Plan (DRP)

- **Definition and Objective:**
  - The DRP is designed to ensure the quick and effective recovery of technology and communication operations after a disaster. This includes restoring critical systems, applications, and data needed for business continuity.
  - The DRP must be aligned with the BCP to ensure a coordinated and efficient response to severe incidents affecting the company's technology infrastructure.
- **DRP Components:**
  - Identification of Critical Assets: Identify and document essential technology assets for business operations, including servers, applications, and databases.
  - Recovery Procedures: Establish detailed recovery procedures for each critical asset, including specific steps to follow and necessary resources.
  - Assignment of Responsibilities: Assign responsibilities for each stage of the recovery process, ensuring effective coordination and clear accountability.

For more details, refer to the document **DISASTER_RECOVERY_PLAN.**

20.3. Continuity Strategies

- **Redundancy and Resilience:**
  - Implement redundancies in critical systems to avoid single points of failure. This includes using secondary data centers and backup systems.
  - Ensure IT infrastructure is resilient, capable of withstanding and recovering from interruptions with minimal impact on business operations.
- **Communication and Coordination:**
  - Establish clear and effective communication channels for coordination during continuity and recovery incidents. This includes communication with employees, customers, suppliers, and other relevant stakeholders.

  - Maintain a crisis communication plan detailing how and when critical information should be communicated during and after an interruption.

20.4. Review and Continuous Improvement

- Post-Incident Evaluation:
  - After each incident that activates the BCP or DRP, a detailed evaluation should be conducted to identify lessons learned and areas for improvement.
  - Incorporate lessons learned into future BCP and DRP updates to enhance the organization's preparedness and response capacity.

21. Documentation and Review

- **Policy Review**:
  - The information security policy must be reviewed and updated annually. However, if relevant changes occur within the company or significant changes are identified in the threat and risk environment, whether operational, legal, regulatory, or contractual, a review will be carried out whenever deemed necessary, ensuring the Policy always remains adapted to Genesis Group's reality.
  - Responsibility for the review lies with the individuals responsible for this policy..