LOJAS AMERICANAS S.A.

RISK MANAGEMENT POLICY

1. Goal

1.1. This Risk Management Policy ("Policy") aims to establish principles, guidelines and responsibilities to be observed in the risk management process inherent in the business activities of Lojas Americanas S.A. ("Company"), in order to identify and monitor the risks related to the Company or its area of activity.

2. Scope

2.1. This Policy applies to the Company and its subsidiaries, as well as to all employees, managers, statutory and non-statutory directors, members of the Board of Directors, members of committees, members of the Fiscal Committee, when established, representatives and third parties, direct or indirectly related to the Company and its subsidiaries.

3. Concepts

3.1. For the purposes of applying this Policy, the following concepts should be used:

Risk limit (or appetite): the exposure and/or maximum impact of the risk that the Company is willing to accept, in the pursuit of its objectives and generation of value. Not all types of risks are acceptable. Therefore, proposed limits should be substantiated and formalized by the following analyses: (i) evaluation of the tangible and intangible return in relation to the proposed Risk limit; (ii) the Company's ability to withstand the impact of the proposed Risk limit; (iii) decision on whether or not the Risk should be accepted according to its type; (iv) feasibility of the implementation of mitigation initiatives (cost and effort) versus effect on risk mitigation and the respective return; and (v) availability of resources (investment and effort) for deployment.

Risk Matrix/Modeling: this aims to establish an individual risk comparison based on impacts and probabilities of occurrence for prioritization and management purposes. The risk matrix is an organization that is constantly evolving and updated, at least annually, during the

review of the Company's strategic planning and in a timely manner with the appearance of emerging risk events.

Definition of Risk(s): the possibility that an event may occur and adversely affect the achievement of the Company's objectives or the probability of failure, failure of a certain thing, due to an eventual, uncertain event whose occurrence does not depend exclusively on the interested parties.

3.1.1. For the purposes of applying this Policy, Risks will be classified in the following categories:

Priority Risks: These are risks that have a likely and potentially high impact for the business, whose management should be prioritized and whose indicators should be monitored regularly.

Strategic Risks: Risks associated with senior management decision-making that can generate a substantial loss in the organization's economic value.

Operational Risks: Risks associated with the possibility of losses of assets, customers or revenues, resulting from failures, deficiencies or inadequate internal processes, people and systems, as well as from external events such as natural disasters, fraud, strikes and terrorist acts. Operational Risks generally entail total or partial reduction or interruption of activities.

Compliance Risks: These are Risks related to the lack of ability or discipline of the Company to comply with the legislation and/or external regulations applicable to the business, as well as internal rules and procedures. Compliance Risks also include internal business rules, having a broader character than the concept usually attributed as legal or regulatory risk, arising from the application of labor, fiscal, tax and contractual legislation, among others.

Conduct Risks: Risks associated with the Company's moral and ethical injury, breach of the Code of Ethics and Conduct and associated policies, such as: actions that characterize harassment, corruption, conflicts of interest, discrimination, political or religious stance, inappropriate use of Company resources, among others.

Technology and Information Risks: these are risks associated with weaknesses and/or obsolescence of the Company's information, control and management systems. This category includes possible external intrusions to systems for capturing data and internal information and/or information on the value chain (customers, suppliers, business partners, etc.). Risks of internal and/or external fraud resulting from such failures, use or inadequate distribution of information and systemic failures that undermine the assertiveness of the Company's indicators.

Credit Risks: These are risks arising from cash and cash equivalents, derivative financial instruments, deposits with banks and other financial institutions, as well as credit exposures to customers.

Liquidity Risks: Risks related to the possibility of the Company not being able to efficiently honor its expected and unexpected obligations, current and future, including cases arising from collateral, without affecting its daily operations and without incurring significant losses.

Market Risks: Risks related to losses resulting from fluctuations in the market values of the Company's own options, including Risks of operations subject to exchange variation, interest rates, stock prices and commodity prices.

Macroeconomic and Social Risks: These are Risks that involve factors external to the Company arising from economic instability and changes in the social environment. Examples include the security risk associated with the problem of public safety in a given region, which may prevent the continuation or expansion of a particular business in that territory.

Environmental Risks: Risks associated with the inadequate management of environmental issues, causing effects such as contamination of soil, water or air, resulting from the operation or improper disposal of waste. Environmental Risks also include the effects of global warming on business, which can make business expansion unfeasible.

Image Risks: Risks associated with the Company's reputation, when the bad management of the other Risks becomes public.

4. References

4.1. This Policy refers to: (i) the corporate governance rules of the Company's Bylaws; (ii) the Company's Code of Ethics and Conduct; (iii) Disclosure and Use of Information and Securities Trading Policy; and (iv) the Brazilian Code of Corporate Governance - Publicly Traded Companies.

5. Guidelines

5.1. The Company is committed to the dynamics of risk management in order to preserve and develop its values, assets, reputation, competitiveness and business continuity.

5.2. The objective of risk management is to understand them, evaluate and define response actions so that any losses are foreseen and reduced, in order to keep risks at acceptable levels. Risk analysis should aid the decision-making process at the various management levels of the Company.

5.3. Risk management contributes to the monitoring and achievement of the Company's objectives. The Company's approach is to integrate day-to-day risk management into the conduct of its business by:

(a) conscious decision-making through better knowledge and consideration of Risks, contexts, direct and indirect impacts in all its activities;
(b) adequately allocation of resources to better control Priority Risks;
(c) transfer to the insurance market of certain risks and a retention policy adapted to each type of risk; and
(d) adequate and coordinated management of incidents by providing reliable and prompt information to the Board in case of major events that may impact the Company.

5.4. The system adopted by the Company is mainly based on:

(a) identification of the factors (causes) of Risks and implications in the projected objectives (goals and results);
(b) evaluation of the main Risks and uncertainties that may affect its objectives, by calculating the impact and likelihood of occurrence of Risks;

(c) proposed Risk limits that the Company and its shareholders are willing to take in the search for return and generation of value;
(d) integration of risk management into decision-making processes, including strategic planning, investment decisions and project management, from the moment they are created and throughout their development; and
(e) use of tools and mechanisms that aim at risk mitigation, through initiatives defined and implemented by the Board of Directors, with the help of the Company's Risk Management area, in order to adjust the Company's exposure to the limits of the approved risk.

5.5. Risk Modeling should comprise the analysis and support tools for the decisions of the Board of Directors, and the Company's Risk Committee should provide the necessary support to the Board for the development of Risk Management.

5.6. It is essential to understand and disseminate, among the organs and executives involved, the correct differentiation of impacts caused by events and situations that do not directly involve the management of Risks such as: (i) internal control failures in processes; (ii) unsuccessful strategic decisions; or (iii) governance failure. This understanding aims to improve and strengthen the Company's corporate governance model.

5.7. All Risks, as well as the approved limits, should be formalized in detailed, explanatory reports, with action plans, as the case may be, as well as the identification of those responsible and deadlines for completing the action plans.

6. Risk Treatment:

6.1. The Risks identified should be approached according to their criticality. The Company's Internal Controls area, together with the areas related to the identified Risk, must determine how to respond to the Risk, and define the protection instruments for the Company, balancing the effects of response to Risk with the possible cost/benefit ratio resulting from legal, regulatory or any other requirements that are relevant to the Company. The Risk Committee, formed by the Risks, Legal, Internal Controls and Internal Audit areas permanently, and by areas invited according to the Risk analyzed, will observe the following alternatives for the treatment of Risks:

(i) Accept the Risk. No action is taken to influence the probability of occurrence and/or

severity of the Risk. Risks whose impact is less than the cost/benefit of its management can be maintained, as long as they are known and accepted by the Risk Committee. However, the monitoring of these Risks must be continuous in order to ensure that, in case of a change of circumstances that justifies a change in the treatment of the Risk, the Company implements said treatment.

(ii) Rejecting the Risk. If it is determined that the Company should not cope with Risk under the conditions in which it presents itself, the Risk Committee will apply one of the following treatments:

(a) *Avoid*: not running the Risk and discontinuing the activities that generate it. Avoiding Risks can lead to the discontinuation of a product line, business division or process.

(b) *Mitigate*: actions are taken to reduce the likelihood of materialization and/or the severity of the Risk. This response involves the enhancement or creation of controls and process improvements.

(c) *Share*: activities that aim to reduce the probability of occurrence and/or severity of Risk, through the transfer or sharing of a part of Risk to third parties, such as insurance policies, outsourcing and hedging.

7. Positions and Responsibilities

7.1. The Company's Board of Directors must:

(a) approve the policies, guidelines, Risk Matrix/Modeling, exposure limits and impacts as presented by the Board;
(b) provide the company's Executive Board, when necessary, with its perception of the Company's degree of Risk exposure and influence the prioritization of the Risks to be treated;
(c) assess, where necessary, changes in risk exposure limits that have been approved by the Board; and
(d) evaluate the adequacy of the operational structure and internal controls in evaluating the effectiveness of this Policy.

7.2. It is incumbent upon the Company's Board of Executive Officers to:

(a) validate the guidelines, Risk Matrix/Modeling, determine the limits of exposure, impacts, and tolerance of exposure to risks;
(b) define the structure for the risk management system within the Company;
(c) define, together with the Risk Committee, action plans for risk mitigation;
(d) supervise the process of risk assessment and monitor the evolution of exposure to risks and risk management systems;
(e) disseminate the risk management culture throughout the Company; and
(f) evaluate at least on an annual basis the effectiveness of the policies and risk management systems and internal controls as well as the Company's compliance program, and report to the Board of Directors on this evaluation.

7.3. The Company's Risk Area is responsible for:

(a) interacting with the Company's critical areas in order to anticipate risks arising from new projects or investigative processes;
(b) studying the current processes from the perspective of Risks;
(c) notifying the identified Risks to the Internal Controls area;
(d) presenting, when requested, its perception regarding exposure to risk (magnitude of impact and likelihood of occurrence), if possible, also based on market indicators;
(e) committing on a timely basis, Risk events that present a tendency for occurrence and/or eventual extrapolation of limits, for discussion in the forums and appropriate hierarchical levels;
(f) ensuring the information made available to the Board on Risks or incidents is legitimate, as well as coordinating the risk management system in crisis moments in case of major events.

7.4. It is incumbent upon the Company's Internal Controls department to:

(a) evaluate, implement and monitor actions in order to reduce exposure to risk;
(b) redesign the critical processes received from the Risks area or from other areas;
(c) standardize redesigned processes;
(d) establish the controls for each of the Risks mapped;
(e) meet, within these controls, the Risk limits approved by the Board of Directors;
(f) provide methodological support to the operational and functional departments of the

Company through on-demand tools and services;

(g) accompany the Executive Board in the implementation of this Policy through the dissemination of tools and good practices.

7.5. It is incumbent upon the Company's Internal Audit area to:

(a) audit the controls established by the Internal Controls area in each of the critical processes;

(b) assess the quality and effectiveness of the Company's risk management processes, suggesting changes to the Board of Directors and the Board of Executive Officers, when necessary;

(c) discuss the pros and cons of taking certain Risks on strategic projects and submit a final report to the Board and the Board of Directors, if necessary, for decision making.

(d) propose limits for exposure to risks.

(e) supervise the process of risk assessment and ensure constant monitoring of risks from external sources, with a prospective view on emerging risks.

(f) audit internal processes and controls, in accordance with established methodology, to verify compliance with standards, policies and procedures.

(g) evaluate the reliability and integrity of the information and the means used to identify, measure, classify and report such information.

(h) evaluate the systems established to ensure compliance with policies, processes, laws and regulations that could have a significant impact on the Company.

(i) analyze the controls adopted to ensure compliance with the goals and objectives established by the Company.

(j) monitor and evaluate governance processes.

(k) evaluate the notes made by the external auditors and the degree of coordination with the areas involved.

(l) periodically report to the Board of Directors the performance of the internal audit activity in relation to its plan.

(m) prepare an Annual Internal Audit Plan for review and approval and submit it to the Board on an annual basis.

(n) prepare a report after the conclusion of each work with the management response, containing duly formalized and approved action plans.

7.6. The Department of Prevention and Loss is responsible for:

(a) mitigating the risks and minimizing losses related to possible deviations of goods and also to the asset security of the Company.
(b) supervising the processes of physical movement of the merchandise, verifying if the procedures are being fulfilled, identifying weaknesses for possible deviations and proposing the necessary changes to eliminate them.
(c) seeking equipment and technology solutions when necessary to minimize identified risks related to the loss of goods and to the Company's equity security.

7.7. It is the responsibility of the Legal Department:

(a) to ensure the legality of the conduct of the Company's business, seeking to prevent Regulatory risks (in relation to the Consumer Defense Code, for example), Fraud risks and Risks inherent in the policies of the Company's websites (Privacy Policy, Use Policy, among others), Code of Ethics and Conduct and other related policies.
(b) to control the contracts, lawsuits and advise the Company on legal issues.
(c) to alert and assist other areas on labor and criminal risks, acting in the prevention of existing relationships between the Company, associates and business partners.

7.8. The Comptroller's Office is responsible for:

(a) ensuring the integrity and accuracy of the Company's financial records in accordance with applicable standards.
(b) periodically reviewing, through internal staff, the Company's financial records in order to guarantee information security.
(c) reporting any deficiencies found in the External Audit process to the Board of Directors and to the Board of Executive Officers.

7.9. The Department of Information Security is responsible for:

(a) monitoring key processes, financial flows, technology infrastructure, applications, and technology services by verifying that systemic procedures and/or controls are being met.
(b) identifying possible weaknesses or deviations of behavior, proposing the necessary changes to eliminate them and/or mitigate them.
(c) centrally managing vulnerabilities.

(d) ensuring frequent intrusion testing, denial of service protection, high availability and capacity Content Delivery Network (CDN) services, anti-phishing and anti-fraud solutions.
(e) ensuring the internal and formal process of continuing vulnerability management by including vulnerability scans and invasion tests (Pen Test) as well as traditional tools such as: IPS, Antivirus, Waff Firewalls and network monitoring.
(f) correlating all tools and business or technical events generated with its own integrated tool to the security operations center (SOC).

8. Validity

This Policy shall come into effect on the date of its approval and may only be modified by a resolution of the Company's Board of Directors.

*****