CATWALKOPERATIONS

2020.07.17

COMPANYWIDE INFORMATION MANAGEMENT POLICY – R03

01 DETAILS

Title: Information Management Policy
Date & Place: Sao Paulo, June 27th, 2020
Reach: Mandatory for all internal procedures. Mandatory for all employees, in all segments, despite salary, role, time or any other conditions.

02 POLICY OBJECTIVES

The main goal of this policy is to allow our organization and its individuals to ensure information is processed legally, securely, efficiently and effectively. It enables individuals to have access to all the need-to-know information for an efficient work, as well as protecting sensitive and intellectual property to be kept safe, avoiding financial loss to investors and clients and, thus, to the entire company. Our guidelines are set on the following tenets:

(1) To establish the role of our information assets and information management in delivering the organization's objectives;

(2) To recognize and exploit opportunities to capitalize on our information assets for our advantage and manage information effectively as a strategic organizational asset across the organization – by providing timely, appropriate, accurate and up-to-date information at the point of need;

(3) To make information available as quickly and easily as possible;

(4) To take appropriate measures to protect information, by assessing and manage risks to the confidentiality, quality, integrity and availability of information;

(5) To create an information management culture where employees take personal responsibility for managing information and comply with all relevant statutory and regulatory requirements;

(6) To encourage the adoption of good practice in information management as set out in these guidelines.

By means of these tenets, we envision to treat information as a corporate asset by making them accessible to those who require it to fulfil their duties. We understand that information is critical in creating and leveraging value and we are committed to ensure that everyone is always aware of and respect the confidentiality of information they produce, share or receive.

03 CLASSIFYING INFORMATION

Information can be classified according to the sensitivity of their data and potential to create negative financial and/or intangible damage. Information always carry a risk for harm to the company's interest or to individuals and must be properly handled, stored and transmitted. The purpose of classifying information is to ensure that information is only

shared with the appropriate people in appropriate circumstances, so as to to keep intellectual property and strategic information under control. The purpose of classifying information is:

(1) **To protect confidential information from unauthorized access.** In the normal course of business, certain information must remain confidential. Examples of such information include the annual budget, human resources files or financial statements. Applying proper security classification and practices can safeguard against unauthorized access to confidential information;

(2) **To protect intellectual property.** We have significant investments in intellectual property. The Information Management Framework requires that these investments be protected to benefit the company, users and investors. Appropriate security practices are needed to ensure an adequate level of protection.

(3) **To protect personal data from clients, customers, or information from individuals that we might handle, manage, store or transact**. Personal information might contain very sensitive data regarding individuals, such as age, identification numbers, address or telephone numbers. Such information must be kept as secure and protected as current technology allows.

There are 3 (three) levels of information in the organization. Each level requires a specific set of precautions to be taken when dealing with its handling, storage and transmission.

LEVEL	CONDITION	RISKS	REQUIREMENTS
LEVEL 1 (L1)	UNRESTRICTED - Information that is created in the normal course of business that is unlikely to cause harm	No impacts If lost, changed or denied would not result in legal or financial risk	Must be adherent to branding requirements
LEVEL 2 (L2)	RESTRICTED - Information that is sensitive outside the company and could impact service levels or performance, or result in low levels of financial loss. Includes financial information or details concerning operations	Could offer unfair competitive advantage to others Disruption to business if not available	Cannot be shared or transferred outside of the company
LEVEL 3 (L3)	CONFIDENTIAL - Information that is sensitive and could cause serious loss of privacy, competitive advantage, loss of confidence, damage to investors, partnerships, relationships and reputation	Loss of reputation or competitive advantage Loss of trade secrets or intellectual property Financial loss	Cannot be transferred without authentication (i.e., the use of a log, encryption or personal password or key) Require a MoU or a NDA signed before transmission
LEVEL 4 (L4)	USER DATA – Information that is sensitive and can identify people, such as address, phone number or email.	Financial Loss due to security breaches. Credibility loss.	Must be depersonalized and segregated in such a way that is hard to reconcile data from the user. Require distinctive database, with managed control access, 2FA, an role mapping.

04 HANDLING INFORMATION

It is important to consider how much confidential information is needed before disclosing it and only the minimal amount necessary is disclosed. There are three process required for dealing with information:

Labeling: classifying information according to their risk potential;

Storing: providing proper storage and media to the information that must be shared;

Transmission: assessing how to transmit the information according to its classification and content.

The table below offer general rules to ensure the best information governance is being met:

LEVEL	CONDITION	STORING	TRANSMISSION	EXAMPLES
LEVEL 1 (L1)	Unrestricted	No special storage required	Must be adherent to branding requirements before any publishing	Company adverts, teasers, public reports, social media material
LEVEL 2 (L2)	Restricted	All media must be under a safe zone (i.e., must require authorized access, such as the company server)	Cannot be shared or transferred outside the company or the company's devices Requires Labeling	Management Plans, Budgets, Financial Statements
LEVEL 3 (L3)	Confidential	All media must be stored safely with trail auditing (if hard media) or under a high level zone, with restricted access and	Cannot be transferred without authentication (i.e, encryption and personal password or key) Require a MoU or a NDA signed before transmission	Business Plans and annexes , Social Contracts, Personal Records, User data
LEVEL 4 (L4)	User Data	All data must be stored in specific user data base. Access must be regulated by 2FA and role mapping. User personal data and user behavior must not be recorded in same transactional object.	Requires security protocols to be transmitted (such as TLS or sFTP). Only High-level technical leads can interact with this information. Bulk files cannot be stored for more than 30 days.	User data only. See specific **Data Protection Security Guidelines** for Technical Handling.

05 SAFETY PRECAUTIONS

Some guidelines are general and apply to all information and its storage and processing, and deserve to be highlighted:

(4) **Passwords**: do not create passwords with less than 8 characters. Add at least a number and a upper case letter. Do not share passwords. Do not write passwords on electronic medium, such as emails, files or equivalen with corresponding creditiall access;

(5) **WIFI access**: Avoid accessing WIFI in public places with any of the company's devices. Use your mobile's personal hotspot to access the internet;

(6) **USB devices**: Do not insert USB devices into the company's devices, unless it is a company authorized USB. Do not mix personal and company's USB files;

(7) **Emails**: Forwarding emails to personal accounts is strictly forbidden. Do not share emails and do not print emails. Use a different password in your email account from your personal email account. Do not set "reply to all" as standard in your email configuration. Double check email sender address so as to avoid confusion.

(8) **Notebooks:** Do not leave computers unattended in any public place.

(9) **Hard media**: Do not leave hard media unattended, do not leave confidential information lying around unattended, such as telephone messages, computer printouts or management plans;

(10) **Accounts**: Do not leave accounts logged on when getting away from devices. Do not log in on public computers;

(11) **Conversations and Meetings**: Do not hold conversation with sensitive information on public places or crowded places, such as cafeterias or restaurants. Do not make presentations with sensitive information on table on such places.

Staff may be held personally liable for a breach of confidence if these guidelines are not followed.

08 COMPLIANCE

An open communication channel is open to ensure doubts, suggestions and complaints regarding this policy.

auditing@mycatwalk.com

We must investigate any inquiries and non-compliant reports, resulting on a report within the maximum 14 (fourteen) day period, including a response to the inquirer.

We must maintain an open database to record all inquiries and reports, including non-compliant events and follow ups, its description, the solution and all related accountability.

09 VALIDITY

This policy is valid and enforceable through our entire operations by means mandatory status.

X
Andre Borges
Managing Director