INFORMATION SECURITY GUIDELINES

Purpose, scope and users
The goal of these highest-level guidelines is to define the purpose, direction, basis and basic rules for an information security concept. The users of this document are all employees of the Jung von Matt Group.
Contractors and suppliers who provide services for the Jung von Matt Group are obliged to comply with and implement the Information Security Guidelines.

Business model
In addition to traditional advertising, Jung von Matt AG also offers its customers services in the area of advertising, such as the development of brand strategies and concepts for digital platforms, via its subsidiaries.
Jung von Matt particular strength lies in the integration of traditional media and "new media". We currently satisfy of the complete communications needs of many customers.

Competition requires that, in addition to developing and implementing high-quality communications concepts, we demonstrate the quality and security of our internal processes. These Information Security Guidelines address this requirement with respect to the security of information processing within Jung von Matt. It therefore applies for the entire group.

Requirements, risks and goals
Our customers' trust and ultimately our business success require in particular that we
– adhere to legal stipulations including data protection laws (compliance),
– protect our business secrets,
– maintain the confidentiality of our customers' data,
– carry out our projects and services within the planned or assured period of time,
– provide and archive our services in a secure fashion.

Against this background, our business success depends on us recognising existing risks for the stated objectives, and avoiding or at least minimising these risks by means of suitable measures.
These risks include incomplete or inaccurate compliance with statutory provisions, unauthorised and possibly unnoticed disclosure of company secrets, violation of our customers' specifications due to system breakdowns, data loss, unauthorised disclosure of information.

Against the background of the external and internal requirements, and especially of our customers' security requirements, information security must be an integral component of our corporate culture.
Every employee must be aware of the necessity of information security and understand the impact of risks on our business success. If Jung von Matt's Information Security Guidelines are violated, disciplinary action may be taken, ranging from written warnings to dismissal
These guidelines shall be applied to the entire information security plan, as defined above under "Purpose, scope and users".

INFORMATION SECURITY TASK

Goals and measurement
The information security concept's general goals are as follows:
– To increase protection of Jung von Matt and its employees from damage.
– To attain competitive advantages through security concepts.
– To meet statutory and individual client specifications.
These goals conform to Jung von Matt's business goals and strategy, as we work primarily for international enterprises for whom information security is of great importance. Our information security officer is responsible for checking these general goals and defining new goals.

Goals concerning individual or groups of security measures are proposed by the respective information security officer in the subsidiaries and approved by management or the Executive Board. All of these goals must be reviewed at least once a year.

Jung von Matt measure and evaluates the fulfilment of these goals. The information security officer is responsible for determining the method by which fulfilment of these goals is measured. The information security officer analyses and evaluates the results and then submits them to Jung von Matt's authorised representative.

Information security requirements
These guidelines and the entire information security concept must meet legal and statutory requirements, as well as the contractual obligations that are critical for information security.

Information security measures
The process for selecting measures is defined in the methodology for assessing and dealing with risk. The selected measures and their implementation status are listed within this methodology.

Responsibilities
The basic responsibilities for management of information security are as follows:
– The management of Jung von Matt is responsible for ensuring that information security is implemented and maintained in accordance with these guidelines and that all necessary resources are available.
– The information security officer is responsible for coordinating execution of the information security concept as well as for reporting about performance.
– The management of Jung von Matt must review the information security status at least once a year (and in any case of significant changes) and log the review accordingly. The purpose of this management review is to demonstrate that the measures are appropriate, suitable and effective.
– The information security officer is responsible for implementing information security training and programmes to raise employee awareness.
– Protection of the integrity, availability and confidentiality of assets is the responsibility of the owner of the respective assets.
– All security-related incidents or weak spots must be reported to the information security officer.
– The information security officer defines what information-security-related information is communicated to which interested parties (both internal and external), by whom and when.
– The information security officer is responsible for setting up and implementing the information security training and awareness plan, which applies for all individuals who play a role in information security management.

Communication of guidelines
The information security officer has to ensure that all Jung von Matt employees, as well as relevant external parties, are familiar with these guidelines.

Support for implementation
The Executive Board and authorised representative of Jung von Matt hereby declare that the implementation of these guidelines and their continuous further improvement will be supported with suitable resources, so that all goals named within them can be met.

Validity
This document is valid as of 05.02.2020.