LiveTiles

INFORMATION SECURITY POLICY

Code:	D3B
Version:	4.0
Date of version:	27 July 2022
Created by:	Daniel Goss
Approved by:	Karl Redenbach
Confidentiality level:	For Internal Use – this version can be shared with select customers and partners who are under NDA.

Change history

Date	Version	Updated by	Description of change
19 Nov 2020	0.1	Daniel Goss	First draft
7 Jan 2021	1.0	Daniel Goss	First release to business
14 Jan 2021	2.0	Daniel Goss	Updated to include interested parties
10 Jan 2022	3.0	Daniel Goss	Reviewed policy and accepted accuracy of version as per section 4.1 of this document
27 July 2022	4.0	Daniel Goss	Updated DPO

Table of contents

1. Purpose, scope and users

The aim of this top-level Policy is to define the purpose, direction, principles and basic rules for information security management.

As a modern, forward-looking business, LiveTiles recognises at senior levels the need to ensure that its business operates smoothly and without interruption for the benefit of its customers, shareholders and other stakeholders.

This Policy is applied to the entire Information Security Management System (ISMS), as defined in the ISMS Scope Document.

Users of this document are all employees of LiveTiles, as well as relevant external parties.

2. Reference documents

- ISO/IEC 27001 standard, clauses 5.2 and 5.3
- ISMS Scope Document
- Risk Assessment and Risk Treatment Methodology
- Statement of Applicability
- Legal, Regulatory and Contractual Obligations
- Data Breach Response and Notification Procedure
- Sub policies identified in Appendix 1

3. Basic information security terminology

Confidentiality – characteristic of the information by which it is available only to authorized persons or systems.

Integrity – characteristic of the information by which it is changed only by authorized persons or systems in an allowed way.

Availability – characteristic of the information by which it can be accessed by authorized persons when it is needed.

Information security – preservation of confidentiality, integrity and availability of information.

Information Security Management System – part of overall management processes that takes care of planning, implementing, maintaining, reviewing, and improving the information security.

4. Managing the information security

4.1. Policies and objectives

General objectives for the information security management system are the following:

- Implement and maintain an effective and auditable Information Security Management System.
- Set a baseline for information security and continue to improve the management system.
- Implement controls for identified risks, threats and vulnerabilities.
- Obtain industry recognised certification(s) including ISO27001
- Protection of revenue streams and company profitability
- Ensuring the supply of goods and services to customers
- Maintenance and enhancement of shareholder value
- Compliance with legal and regulatory requirements
- By request, be in a position to provide our clients with the documented controls, and supporting operating evidences, around how we manage security for our products and services
- Fundamentally obtain the trust of our clients, that we make all reasonable efforts to maintain data privacy, and support their needs to maintain compliance with their regulatory obligations.

The measures by which we will use to ensure the ISMS meets its objectives are as follows:

A) LiveTiles has the ability to respond to any question in relation to anything within our ISMS or in relation to how we manage data, within 24 business hours; and

B) In 90% or greater cases, our responses to A) are accepted outright as reasonable measures and controls by our client; and

C) In 100% of cases, our responses to A) are accepted by clients, albeit with minor adjustments that can be implemented in under 2 weeks.

D) Zero data breach as a direct result of a security Incident

The Information Security Officer is responsible for reviewing these general ISMS objectives and setting new ones.

Objectives for individual security controls or groups of controls are proposed by the owners of systems/domains and approved by the CEO in the Statement of Applicability.

All the objectives must be reviewed at least once a year.

The Information Security Officer is responsible for setting the methods for measuring the achievement of the objectives – the measurements will be performed at least once a year and the Information Security Officer will analyse and evaluate the measurement results and report them to top management as input materials for the Management review. The Information Security Officer is responsible to record the details about measurement methods, periodicities and results in the Measurement Report.

4.2. Interested Parties

LiveTiles determines the following interested parties relevant to the ISMS and their requirements relevant to information security:

Interested Party	Internal / External	Needs & Expectations
Decision makers and top management	Internal	• Confidence that the business is adhering to all internal and external policies and legislation
Process and systems owners	Internal	• Clear guidelines when developing new products, processes and systems
Support functions (People & Experience and IT)	Internal	• Clear guidelines and process when performing their roles • Have access to requisite resources
Employees	Internal	• Clear instructions on how to handle sensitive data • Have the correct resources to perform their roles
Shareholders	External	• Expect that trust and confidence is maintained and does not impact shareholder value
Customers	External	• Maintain trust and confidence in LiveTiles to handle their data securely • Trust that LiveTiles products meet the desired quality levels and outcomes
Partners and Suppliers	External	• Achievable contractual agreement and clear delivery outcomes
Regulators and legislators	External	• Expect that a proportionate level of control are in place to protect assets

4.3. Information security requirements

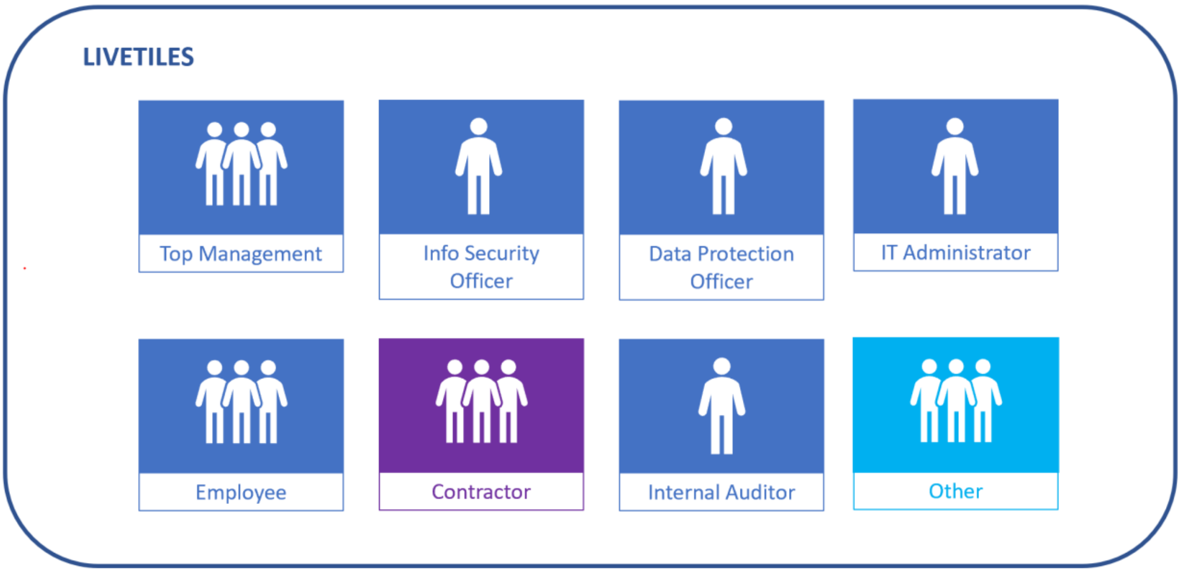
This Policy and the entire ISMS is compliant with legal and regulatory requirements relevant to the organization in the field of information security and personal data protection, as well as with contractual obligations.

4.4. Information security controls

The process of selecting the controls (safeguards) is defined in the Risk Assessment and Risk Treatment Methodology.

The selected controls and their implementation status are listed in the Statement of Applicability.

4.5. Responsibilities



Responsibilities for the ISMS are the following:

- The CEO has the overarching responsibility for all aspects of the ISMS and its implementation across the organisation.
- the Information Security Officer is responsible for ensuring that the ISMS is implemented and maintained according to this Policy, and for ensuring all necessary resources are available
- the Information Security Officer is responsible for operational coordination of the ISMS and personal data protection as well as for reporting about the performance of the ISMS
- the Information Security Officer is responsible for the overall compliance of personal data processing;
- CEO and top management must review the ISMS at least once a year or each time a significant change occurs and prepare minutes from that meeting. The purpose of the management review is to establish the suitability, adequacy and effectiveness of the ISMS.
- the Information Security Officer will implement information security training and awareness programs for employees
- the protection of integrity, availability, and confidentiality of assets is the responsibility of the owner of each asset
- all data breaches, security incidents or weaknesses must be reported to the Information Security Officer
- the Information Security Officer will define which information related to information security will be communicated to which interested party (both internal and external), by whom and when
- the Information Security Officer is responsible for adopting and implementing the Training and Awareness Plan, which applies to all persons who have a role in information security management
- All employees staff need to abide by the ISMS, and provide attestations in relation to their comprehension of the ISMS.

4.6. Policy communication

The Information Security Officer has to ensure that all employees of LiveTiles, as well as appropriate external parties are familiar with this Policy. Policies and acknowledgment will be managed in the LiveTiles Document Hub.

5. Support for ISMS implementation

Hereby the Information Security Officer declares that ISMS implementation and continual improvement will be supported with adequate resources in order to achieve all objectives set in this Policy, as well as satisfy all identified requirements.

Appendix 1: Related Policies & Procedures

Policy Title	Areas addressed	Target audience
Bring Your Own Device Policy (BYOD)	Care and security of mobile devices such as laptops, tablets and smartphones, whether provided by the organization or the individual for business use.	All users
Mobile Device and Teleworking Policy	To prevent unauthorized access to mobile devices both within and outside of the organization's premises.	All users
IT Security Policy	Define clear rules for the use of the information system and other information assets in LiveTiles.	All users
Information Classification Policy	Ensure that all information is protected at an appropriate level. This document is applied to the entire Information Security Management System (ISMS) scope, i.e. to all types of information (including personal data), regardless of the form – paper or electronic documents, applications and databases, people's knowledge, etc.	All users
Access Control Policy	User registration and deregistration, provision of access rights, external access, access reviews, password policy, user responsibilities, system and application access control and physical access control.	All users
Password Policy	Prescribe rules to ensure secure password management and secure use of passwords	All users
Encryption Policy	Risk assessment, technique selection, deployment, testing and review of cryptography, and key management.	Employees involved in setting up and managing the use of cryptographic technology and techniques
Anonymization and Pseudonymization Policy	Establishing and maintaining pseudonymization and encryption of personal data.	Data Protection Officer, IT/IT Security Officer, Product Team and the

Policy Title	Areas addressed	Target audience
		representatives of the business units responsible for processing personal data.
Risk Assessment and Risk Treatment Policy	The purpose of this document is to define the methodology for assessment and treatment of information risks in LiveTiles, and to define the acceptable level of risk.	All employees of LiveTiles who take part in risk assessment and risk treatment.
Security Procedures for IT Department	Internal IT services, monitoring and security management, including the disposal and destruction of equipment and media.	Employees responsible for protecting the organization's IT infrastructure and services.
Change Management Policy	Define how changes to information systems are controlled.	All employees that manage information systems including 3rd party applications or SaaS.
Backup Policy	Manage how backup copies are created at defined intervals and regularly tested.	All users
Cross Border Personal Data Transfer Procedure	Create a common approach throughout LiveTiles regarding instances of transfers of personal data to a country outside of the LiveTiles operating entities.	All employees
Secure Development Policy	Define basic rules for secure development of software and systems.	All users responsible for the development and maintenance of LiveTiles Software Products.
Supplier Security Policy	Define the rules for relationship with suppliers and partners	Top Management and users responsible for suppliers and partners in LiveTiles.
Data Breach Response and Notification Procedure	Process for managing the response to a data breach.	All employees

Policy Title	**Areas addressed**	**Target audience**
Records Retention and Protection Policy	Retention period for specific record types, media selection, record retrieval, destruction and review.	Employees responsible for creation and management of records