Digital Accessibility: It's All We Do

Level Access Information Security Policy

Washington, D.C. Office
1600 Spring Hill Road, Suite 400
Vienna, VA 22182

Silicon Valley Office
114 Sansome Street, Suite 950
San Francisco, CA 94104

Table of Contents

Version Control

Title	Level Access Information Security Policy
Description	Company-wide document outlining the top-level policy for information security at Level Access
Author	Jeremy Sumner
Owner	Director of Information Security
Approval	CEO & SVP of Engineering

Version	Modified By	Modifications Made	Date
1.0	Tim Springer	Last pre-ISMS company policy	December 1, 2017
2.0	Jeremy Sumner	Major updates following ISMS implementation	August 6, 2018
2.1	Jeremy Sumner	Updates to objectives, addition of Supplemental Policies section; copied into new Level template.	August 14, 2019

Policy

Level Access (Level) is committed to protecting its information assets to satisfy our business objectives and meet the information security requirements of our customers while maintaining the safety of individuals and their right to privacy. To achieve these goals, we have established an ISO 27001 Information Security Management System (ISMS).

This document outlines the highest-level security policy by describing:

1. How we are committed to information security.
2. The scope of what is covered by our ISMS.
3. Our information security objectives.

There are additional supplemental policy documents which provide more detail about specific areas which are enumerated in a later section. All policy documents are reviewed for opportunities for improvement once per year, or when major changes occur that affect the context of the ISMS.

Deviations from policy may be allowed under exceptional circumstances. Contact infosec@levelaccess.com before deviating if you believe an exception is necessary. Observed deviations should be raised as an incident (see below).

Commitment

The CEO and SVP of Engineering set Information Security as a priority for the business through the approval and availability of this policy. The currently active policy is made available to all employees and interested parties by either direct communication or by request to infosec@levelaccess.com.

The SVP of Engineering sponsors the ISMS and owns the information security risks. Reporting to the SVP of Engineering, the Director of Information Security is responsible for the implementation and operation of the ISMS, including reporting on its performance. Other dedicated and competent staff are responsible for implementing specific controls as needed.

Commitment is required from everyone at Level as described below:

1. All employees are required to acknowledge they have read, understand, and agree with this policy and others in the Employee Handbook.
2. Employees will report any suspected security incidents, vulnerabilities, or threats to information assets to infosec@levelaccess.com.
3. Suppliers working on behalf of Level will be required to meet a minimum level of security as determined by Level.

Level conducts regular performance reviews of the ISMS that include senior management. This ensures both the ISMS achieves its intended outcomes as well as demonstrates our commitment to continually improving our information security posture.

Scope

The effective scope of the ISMS covers the Level applications delivered through Software-as-a-Service (SaaS) and their supporting operations. This includes the people and processes who directly contribute to the delivery of those services and operations, the physical and digital information assets which the services and operations depend on, and the management of third parties involved in their delivery. In addition, Level complies with relevant laws and industry regulations which relate to information security.

Other information security activities occur at Level but are not within the effective scope of the ISMS at this time.

Information Security Objectives

Our strategic information security objectives are to:

1	Protect the information assets and systems that have been entrusted to us
2	Create, deliver and maintain trusted and reliable software and services
3	Respect the privacy rights of all individuals with whom we interact

4	Realize our commitment to continually enhance our security and privacy controls

Figure 1 – Table of Information Security Objectives

The strategic objectives are underpinned by operational and tactical objectives that change more frequently. All objectives are reviewed and measured to track progress and performance of the ISMS. Planning, review and measurement cadences vary depending on the level of objective.

Supplemental Policies

The operation of the ISMS is supported by topic-specific policies, plans and other formal documentation. These are internal-only documents and generally not available to external parties, though exceptions may be granted under certain circumstances.

Our current list of formal documents is as follows:

1. Risk Management Methodology
2. Acceptable Use Policy
3. Information Classificaiton Policy
4. Access Control Policy
5. Operational Security Policy
6. Secure Development Policy
7. Supplier Security Policy
8. Incident Response Plan
9. Business Continuity Plan
10. Data Protection Policy

The ISMS is also supported by several other documents such as standards, procedures and agreements. These are not enumerated above for the sake of brevity.