Level Access Information Security Policy

INFOSEC@LEVELACCESS.COM

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
Version Effective Date	August 15, 2018
Scope	Company – can be shared publicly
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

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 whilst 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 in specific areas.

This and other policy documents will be reviewed for opportunities for improvement annually, or when major changes occur which 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 current 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. The Director of Information Security is responsible for the implementation and operation of the ISMS, including reporting on its performance. Other dedicated, 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 and 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 made aware of this policy and are required to comply with it.

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

Scope

The 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 scope of the ISMS at this time.

Information Security Objectives

The Information Security Objectives described below have been established after considering:

- The context, purpose, and internal, as well as external issues affecting the organization.
- Determining the requirements of the interested parties.
- The boundaries of the ISMS.
- The outputs of the risk assessment and risk treatment processes.

To deliver reliable cloud applications for users and other interested parties who need confidence and assurance the platform is fit for their purpose of sharing and working with sensitive information
To provide a pragmatic digital paperless ISMS for staff and other interested parties who need to access it which is integrated into their day to day work practices to ensure it becomes a habit for good performance not an inhibitor to getting their work done
To identify and manage risks of assets within the scope of the ISMS
To continually strengthen and improve the overall capabilities of the information security management system
To establish quantified information security goals annually through management and review meetings
To design, conduct and run an Application Security Program following best practices to give interested parties the confidence we deliver secure software
To protect the privacy of individuals who use, actively or passively, our hosted software products
To improve the resilience of our hosted software services
To maintain a highly secure hosted software platform
To certify an ISMS against the ISO 27001 standard, and maintain the certification

Table of Information Security Objectives

Measurements of these objectives are established as KPIs and reviewed in the management review meetings.