

# Service Level Agreement

Foyer LLC  
Version 3.0 · 2026-05-05



## 1. Introduction

---

This Service Level Agreement (“SLA”) defines the service commitments, support standards, and operational responsibilities that Foyer LLC (“Foyer”) provides to its customers. This SLA applies to the Foyer platform accessible at usefoyer.com and its regional domains.

## 2. Service Availability

---

### 2.1 Availability Target

Foyer targets a service uptime of 99.9% measured over each calendar month, excluding scheduled and emergency maintenance windows. Uptime is measured as the percentage of total minutes in a calendar month during which the Foyer platform is accessible to customers.

### 2.2 Scheduled Maintenance

Planned maintenance that may cause service interruption will be communicated to affected customers no less than 48 hours in advance through appropriate channels. Scheduled maintenance will typically be performed during off-peak hours to minimize disruption.

### 2.3 Emergency Maintenance

In rare cases where immediate action is required to protect the security or integrity of the platform, Foyer may perform emergency maintenance without advance notice. Customers will be notified as soon as practical through appropriate channels with a description of the issue and the expected duration.

## 3. Support

---

### 3.1 Support Channels

Foyer provides support through the following channels:

- **Email:** support@usefoyer.com
- **In-app chat:** Available on the Foyer platform (powered by Tawk)
- **Phone:** +1 414-215-0898

### 3.2 Operating Hours

Support is available Monday through Friday, 9:00 AM to 5:00 PM Central Time, excluding U.S. public holidays.

### 3.3 Response Time Targets

Response times vary by plan tier. Customers on Ultimate and Enterprise plans receive priority support with faster response commitments.

#### STANDARD AND PREMIUM PLANS

Severity	Description	Target Response Time
Critical	Complete service outage or confirmed security incident affecting customer data	4 hours during business hours
High	Significant degradation in service functionality with no available workaround	1 business day
Medium	Non-critical issue affecting limited functionality; workaround available	2 business days
Low	General inquiries, feature requests, or minor cosmetic issues	3 business days

#### ULTIMATE AND ENTERPRISE PLANS (PRIORITY SUPPORT)

Severity	Description	Target Response Time
Critical	Complete service outage or confirmed security incident affecting customer data	4 hours during business hours
High	Significant degradation in service functionality with no available workaround	8 hours during business hours
Medium	Non-critical issue affecting limited functionality; workaround available	1 business day
Low	General inquiries, feature requests, or minor cosmetic issues	2 business days

Response time is measured from receipt of the support request during business hours. Requests received outside business hours begin accruing response time at the start of the next business day.

### 3.4 Escalation

If a support issue is not resolved within the defined response times, customers may request escalation by replying to the existing support thread or contacting Foyer directly. Escalated issues will receive attention within 2 hours during business hours.

## 4. Data Protection

---

### 4.1 Encryption

All customer data is encrypted in transit using TLS 1.2 or higher and encrypted at rest using AES-256. Deprecated protocols such as SSL, TLS 1.0, and TLS 1.1 are not permitted.

### 4.2 Tenant Isolation

Customer data is logically separated within the Foyer platform. Access controls ensure that customers can only access data belonging to their own organization.

### 4.3 Data Residency

Foyer operates in three independent Azure regions. Customer data is stored exclusively in the region associated with the customer's account and does not replicate between regions.

Region	Domain
United States (Central US)	usefoyer.com
Europe (West Europe)	eu.usefoyer.com
Australia (Australia Central)	au.usefoyer.com

### 4.4 Payment Data

Foyer does not store, process, or transmit payment card data directly. All payment processing is handled by Stripe, a PCI DSS Level 1 certified service provider.

## 5. Backup and Recovery

---

Production databases are backed up daily with point-in-time restore capability. Backups are retained for no less than 14 days. All backups are encrypted at rest to the same standard as source data.

## 6. Incident Notification

---

### 6.1 Security Incidents

In the event of a confirmed security incident involving unauthorized access to customer data, Foyer will notify affected customers through appropriate channels with a description of the incident, the data involved, and remediation steps taken. Notifications will be made in compliance with all applicable legal and regulatory timeframes.

## 6.2 Service Disruptions

During unplanned service disruptions, Foyer will provide status updates to affected customers through appropriate channels until the issue is resolved.

## 7. Customer Responsibilities

---

### 7.1 Issue Reporting

Customers are responsible for promptly reporting any issues or disruptions through the support channels listed in Section 3.1. Clear and detailed descriptions, including relevant screenshots or error messages, facilitate faster resolution.

### 7.2 Access Management

Customers are responsible for managing their own users' access rights, including provisioning, removal, and periodic review to ensure access remains appropriate.

### 7.3 System Requirements

Customers must ensure that their systems meet the minimum requirements specified for using Foyer. Compatibility issues arising from unsupported configurations are not covered by this SLA.

## 8. Review and Amendment

---

### 8.1 SLA Review

This SLA will be reviewed annually to ensure its continued relevance and effectiveness.

### 8.2 Amendment

Foyer reserves the right to amend this SLA with reasonable notice to customers. Amendments will be communicated through appropriate channels and updated on the Foyer website.

## 9. Revisions

---

Version	Date	Description
1.0	2022-08-28	Initial version
2.0	2026-04-14	Added incident notification and data protection sections
3.0	2026-05-05	Introduced tiered support response times by plan (Priority Support for Ultimate and Enterprise)