Security Policy

Recovered Hours — Data Protection & Security

Last updated: March 16, 2026 | hello@recoveredhours.com | RecoveredHours.com

Our Commitment

Recovered Hours takes security seriously. We implement industry-leading practices to protect your data and maintain your trust.

Data Protection

Encryption

- In transit: TLS 1.3 on all data
- At rest: AES-256 encryption
- Backups: Encrypted, geographically distributed

Access Control

- Role-based access control (RBAC)
- Multi-factor authentication required
- Minimum necessary access principle
- Quarterly access reviews

Network Security

- Web Application Firewall (WAF) on all endpoints
- DDoS protection
- Regular penetration testing (quarterly)
- Intrusion detection systems

Compliance

GDPR

- Data Processing Agreement (DPA) available
- Right to deletion guaranteed
- Data portability supported
- Processing logs maintained

Industry Standards

- SOC 2 Type II in progress
- ISO 27001 certified infrastructure
- PCI DSS compliant for payment processing

Incident Response

Step	Action	Timeline
1. Detection	Automated monitoring	24/7

2. Analysis	Security team alert	Within 15 minutes
3. Containment	Isolation of affected systems	Immediate
4. Notification	You are notified of any breach affecting your data	Within 72 hours
5. Resolution	Root cause analysis and full remediation	Complete report provided

Security issues? Contact security@recoveredhours.com — response within 24 hours.

Your Responsibilities

While we secure our systems, please also:

• Use strong, unique passwords

• Enable two-factor authentication on all accounts

• Never share credentials

• Report suspicious activity immediately to security@recoveredhours.com

Policy Updates

We update this policy periodically. Significant changes will be communicated via email with at least 30 days notice.