

Information Security Policy

Last updated October 23, 2026

This policy sets out the information security program of Bump The DSL, LLC, the company that builds and operates Relay (“we”). It applies to everyone who works for or on behalf of us, including employees and contractors, and to every company device, account and system, including Relay and the cloud services it runs on.

SUMMARY

Multi-factor sign-in, a password manager, locked and encrypted computers with active anti-malware, production systems isolated and monitored, and a standing process to find and fix vulnerabilities.

Responsibilities

- **The business owner** is accountable for the security program, approves this policy, and also serves as our Data Protection Officer and incident lead.
- **Everyone with access** to company systems or data must follow this policy and report a suspected security incident immediately (see our Incident Response Policy).

Security baseline for daily work

Every person and device that handles company data follows this baseline:

- **Multi-factor authentication.** Required on every business account (email, Shopify, TikTok Shop, hosting, database, code repository and domain management), using an authenticator app or passkey. Text-message codes are used only where a service offers nothing stronger.
- **Strong, unique passwords.** At least 14 characters, generated and stored in a password manager, never reused across services and never shared.
- **Screen lock.** Computers lock automatically after no more than 5 minutes of inactivity and are locked by hand whenever left unattended.

- **Full-disk encryption.** Turned on for every company computer (BitLocker on Windows, FileVault on macOS).
- **Updates.** Automatic updates stay on for operating systems, browsers and security software; critical updates are installed promptly.
- **Clear desk and clear screen.** Passwords, credentials and personal data are never written on paper or left visible; any printed personal data is kept out of sight and shredded when no longer needed.
- **Approved tools only.** Company data stays in approved business systems. Personal data is not copied into personal email, chat apps, personal storage or unapproved AI tools.
- **Lost or stolen devices** are reported immediately, and the sign-ins and credentials on them are revoked.

Endpoint protection

Every company computer runs anti-malware software with real-time protection and automatic updates (at minimum the operating system's built-in protection, such as Microsoft Defender), together with the operating system firewall. These protections must not be disabled.

Network security and monitoring

- **Segregated production environment.** Production systems run on managed cloud infrastructure in the United States, separate from staff computers and office networks. Staff devices are never part of the production network.
- **Separate environments.** Development and testing use separate databases and never use production personal data.
- **Minimal exposure.** Only HTTPS endpoints are exposed to the internet, and plain HTTP is redirected to HTTPS. The database accepts only encrypted, authenticated connections.
- **Verified integrations.** Incoming notifications from platforms such as Shopify and TikTok Shop are checked by cryptographic signature before they are processed; anything that fails is rejected.
- **Abuse protection.** Public endpoints are rate limited, and failed sign-in attempts are recorded.
- **Monitoring and alerts.** Health checks run continuously, and failures and errors raise automated alerts to the owner. Sensitive actions, such as viewing an order or changing a setting, are written to an audit log.
- **Clean logs.** Application logs are designed to exclude passwords, access tokens and personal data.

Secure development

- Source code is kept in a private repository. Every change runs automated type checks, linting, tests and a build before it can be released.
- Every change, and the full repository history, is scanned for leaked credentials. A finding fails the build, and the credential is rotated.
- Secrets live only in the hosting provider's secret manager. They are never placed in code, container images, documents or chat.
- Third-party packages are pinned to exact versions, checked for known vulnerabilities on every build, and updated through reviewed changes.

Vulnerability and threat management

We identify, prioritize and fix security weaknesses through a standing procedure:

1. **Identify.** Sources include automated dependency vulnerability audits on every build, weekly automated dependency update proposals, credential scanning, security notices from our providers, regular engineering audits, and reports from anyone.
2. **Assess.** Each finding is rated Critical, High, Medium or Low by its impact and how easily it could be exploited.
3. **Fix.** Target times: Critical within 7 days (immediately if it is being actively exploited), High within 30 days, Medium within 90 days, and Low at the next scheduled maintenance. Any exception is recorded together with a temporary safeguard.
4. **Verify.** Each fix is tested and confirmed before the finding is closed. Any credential that may have been exposed is rotated immediately.

Service providers

We use established providers that run their own security programs, give each one only the access it needs, and review the list at least once a year. The providers that process personal data are listed in our Personal Data Protection Policy.

Awareness

Everyone with access reads this policy when they join and again every year, and is reminded of changes when they happen.

Enforcement

Breaking this policy can lead to access being removed and to further action. Exceptions must be approved by the owner and recorded.

Review of this policy

This policy is reviewed at least once a year and whenever we add a system, change how we use personal data, or learn something from an incident. The next scheduled review is October 2027. Version 1.0, first published October 23, 2026.

Contact

Questions about this policy can be sent to privacy@bumptheds1.com.