

Incident Response Policy

Last updated October 23, 2026

This policy explains how Bump The DSL, LLC, the company that builds and operates Relay (“we”) detects, reports, contains and recovers from security and privacy incidents. It also covers how we notify sellers, TikTok Shop, regulators and affected people.

SUMMARY

Report anything suspicious straight away. We contain the problem first, keep the evidence, work out who is affected, and tell affected partners without undue delay, and within 72 hours at most.

What counts as an incident

- Personal data reaching, or possibly reaching, someone who should not have it.
- A leaked or misused password, API key, access token or encryption key.
- Unauthorized access to, or changes in, any of our accounts or systems.
- Personal data or a secret found somewhere it should not be, such as a log, an email or a spreadsheet.
- A lost or stolen device that holds company data or sign-ins.

Roles and responsibilities

Role	Responsibilities
Incident lead (the business owner, who is also our Data Protection Officer)	Declares the incident, sets its severity, owns the timeline, and decides on and signs off notifications
Technical responder	Contains the incident, investigates it and restores service

Role	Responsibilities
Communications	Notifies sellers, TikTok Shop, regulators and affected people, and handles their questions

In our small team one person may hold more than one role. The incident lead names a deputy for when they are unavailable.

Reporting channels

- **Staff and contractors** report a suspected incident to the owner immediately, by phone or direct message, and must not try to investigate it alone.
- **Anyone else** (sellers, TikTok Shop, creators, customers, security researchers) can email privacy@bumpthedsll.com with "Security incident" in the subject line. These reports are treated as urgent.

Severity levels

Level	Meaning	Response
SEV1	Confirmed or likely exposure of personal data or a live credential, or an unauthorized change	Start immediately; contain within one hour
SEV2	A security control failed but there is no evidence of exposure	Same business day
SEV3	Service disruption with no risk to data	Normal operations

Response steps

1. **Record.** Note the time, who found the problem and what they saw. The record uses identifiers and counts, never personal data itself.
2. **Contain.** Do the minimum that stops the exposure: rotate credentials, revoke tokens, disconnect the affected integration (for example, revoke Relay's TikTok Shop authorization), or stop the affected service.
3. **Preserve evidence.** Export the logs and audit records before anything is changed or deleted.

4. **Assess.** Establish what data was involved, how many people were affected, for how long, and how it happened.
5. **Notify.** Follow the notification rules below, and record each decision with the time it was made.
6. **Recover.** Restore normal service and confirm the cause is fixed.
7. **Review.** Write a post-incident report within 5 business days.

Notifying sellers, TikTok Shop and others

- **Sellers and TikTok Shop.** If a suspected or confirmed incident affects personal data that we received from TikTok Shop or a seller, we notify TikTok Shop and the affected sellers without undue delay, and no later than 72 hours after we become aware of it, or sooner if an agreement requires. The notice says what happened, which data and how many people are involved, what we have done, and who to contact. We send updates as we learn more.
- **Regulators and individuals** are notified where the law requires it, within the legal deadline.
- **Service providers** are notified when the incident involves their systems.

Evidence handling

Original logs and records are kept read-only, with a note of who collected them and when. Personal data, tokens and secrets are never pasted into chat, tickets or email. Any secret that appeared somewhere it should not have is treated as leaked and rotated.

Testing

Once a year we rehearse this policy with a made-up scenario, such as a leaked access token, and update it with what we learn.

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.