

Incident Response Plan

Owner	Andrew Smith, Security Owner (Incident Commander)
Security contact	andrew@swaptqr.com
Version	1.1, effective October 19, 2026
Part of	Swapt Information Security Policy

1. Purpose and scope

This plan covers any event that threatens the confidentiality, integrity or availability of Swapt systems or data. Examples include unauthorized access, leaked credentials or tokens, malware, lost devices, data exposure, and service attacks or outages.

2. Roles and responsibilities

Role	Person	Responsibilities
Incident Commander	Andrew Smith	Leads the response; decides severity, containment and escalation; owns all external communication
Technical responders	Engineering staff	Investigate, contain, fix and recover; keep evidence
All personnel	Everyone	Report suspected incidents right away; never investigate or delete evidence on their own

If the Incident Commander can't be reached, the most senior available engineer takes the role until handover.

3. Reporting channels

- **Internal.** Anyone who suspects an incident reports it immediately to andrew@swaptqr.com and by phone or direct message to the Incident Commander.
- **External.** Sellers, partners and security researchers can report issues to andrew@swaptqr.com.
- **Automated.** Alerts from Sentry, Google Cloud, AWS and Cloudflare go to the engineering team.

4. Severity levels

Severity	Definition	Response target
Critical	Confirmed or likely exposure of Restricted or Confidential data (including TikTok Shop data), compromised production credentials, or a full outage	Respond immediately, within 1 hour
High	Suspected unauthorized access, a vulnerability being actively exploited, or a major feature unavailable	Within 4 hours
Medium	A contained security event with no evidence of data exposure	Within 1 business day
Low	Policy deviation or minor issue	Within 5 business days

5. Response procedure

1. **Detect and report.** Log the incident in the incident log with the time, who reported it, what was seen and the affected systems.
2. **Triage.** The Incident Commander assigns a severity and brings in responders.
3. **Contain.** Stop the damage from spreading. Steps can include:
 - revoking or rotating exposed credentials, API keys and partner tokens, including disconnecting affected TikTok Shop authorizations;
 - disabling compromised user accounts and ending their sessions;
 - blocking malicious IPs or traffic at the edge;
 - taking affected features offline;
 - isolating or wiping compromised devices.
4. **Preserve evidence.** Keep logs (application, Sentry, cloud audit logs) and snapshots before making destructive changes.
5. **Eradicate.** Remove the root cause, for example by patching the vulnerability, removing malicious code or fixing the misconfiguration.
6. **Recover.** Restore service from known-good deployments and backups, check data integrity, and watch closely for the problem coming back.
7. **Escalate and notify** (section 6).
8. **Post-incident review.** Within 10 business days of a Critical or High incident, write a review covering the timeline, root cause, impact and corrective actions. Track the actions to completion.

6. Escalation and notification

- **Internal escalation.** Critical and High incidents go to the Incident Commander immediately, and to company leadership within 1 hour.

- **Sellers.** Affected sellers are notified by email without undue delay, and within 72 hours of confirming a breach that involves their data. The notice describes what happened, the data involved, what we have done, and what they should do.
- **TikTok Shop and other partners.** If an incident involves data obtained through a partner's API, or that partner's credentials, we notify the partner through its designated security or partner support channel without undue delay, and within 72 hours of confirmation. If the partner requires a shorter timeframe, we meet it.
- **Regulators and individuals.** Where the law requires it (for example GDPR, CCPA or US state breach laws), we notify the relevant authorities and affected individuals within the legal deadlines.
- **Law enforcement.** We involve law enforcement where appropriate and as advised by legal counsel.

7. Records

Every incident is recorded in the incident log with its timeline, severity, actions taken, the notifications sent and their timestamps, and the review. Records are kept for at least 3 years.

8. Testing

The plan is reviewed every year, and a tabletop exercise (for example, a leaked TikTok Shop token) is run at least once a year. The plan is updated with what we learn.