Security Research & Responsible Disclosure Policy

Effective Date: August 15, 2025

1. Purpose

At Skybriz, security is a top priority. We invite good-faith security research and provide clear rules, safe harbor, and rewards for responsible disclosures that help protect our customers and systems.

2. Scope

I. In Scope (examples):
- Skybriz main website (https://www.skybriz.com)
- SKYNEST mobile apps (iOS & Android)
- SkyCast web and mobile integrations
- APIs hosted under *.skybriz.com
- Any official Skybriz-owned cloud services or subdomains

II. Out of Scope (non-exhaustive):
- Third-party services we do not control (e.g., payment processors, external SaaS)
- Social media or marketing platforms
- Denial-of-Service (DoS), spam, brute-forcing, or stress testing
- Findings that require physical device access or rooted/jailbroken devices only
- Issues in unsupported OS/browser versions

3. Eligibility

- You must comply with applicable laws and this policy.
- You must be the first reporter of a unique vulnerability.
- Current Skybriz employees/contractors are excluded unless explicitly authorized.
- Participants in sanctioned regions or on restricted lists may be ineligible for payment.

4. Rules for Testing (Allowed)

- Only test assets in scope.
- Use test accounts you own or that we provide.
- Minimize impact; access only the data required to demonstrate an issue.
- Stop immediately if you access data belonging to others; include high-level evidence only (redact PII).

5. Prohibited Activities

- Service disruption (DoS, DDoS, traffic flooding, load testing)
- Social engineering (phishing, vishing), physical intrusions, or spam campaigns
- Planting malware/backdoors, maintaining persistence, mass data exfiltration beyond proof
- Automated scanning that degrades availability
- Selling, publicizing, or abusing vulnerabilities

6. Reporting Guidelines

I. Please include:
   - Title, affected asset/URL/endpoint
   - Clear, reproducible Steps to Reproduce (numbered)
   - Expected vs. Actual behavior
   - Impact assessment and plausible abuse scenarios
   - Proof-of-Concept (curl/HTTPie/Postman, minimal video if helpful; no real-user data)
   - Optional: CVSS vector/score
   - Researcher name/handle and contact email

7. Triage Workflow & Statuses

I. We use transparent states to show progress:
   - Needs Info → Triaged → In Progress → Fix Ready → Resolved → Verified
   - Closed—No reward: Duplicate, Out of Scope, Informational, Can't Reproduce, Won't Fix

   You’ll receive email updates on status changes.

8. Severity & Rewards (Startup Phase)

I. We calibrate rewards using impact, exploitability, and report quality (CVSS v3.1 as a guide):
   - Gold (critical): $100 — e.g., auth bypass, mass data exfiltration, RCE
   - Silver (high): $50 — e.g., privilege escalation, cross-tenant data access, stored XSS in sensitive flows
   - Bronze (med/low): $25 — e.g., IDOR on limited data, reflected XSS with impact, exploitable misconfig

   Notes: Rewards may be adjusted for root-cause depth, exploit reliability, or defense-in-depth value. Duplicate reports are not rewarded (see §10).

9. Recognition (Hall of Fame & Badges)

- Reward-eligible closures (Resolved/Verified) with credit=yes are added to the Security Hall of Fame.
- Each honoree receives a tier badge (Gold/Silver/Bronze). Recognition-only items may receive a non-monetary badge.
- Public credit is optional and can be anonymous if preferred.

10. Duplicates & Previously Known Issues

- First valid report of a root cause is eligible for reward.
- Duplicates (same root cause) are closed as Duplicate (no payout). High-quality dupes may be acknowledged at our discretion.

11. Validity Criteria (Examples Not Rewarded)

- Self-XSS; clickjacking on non-sensitive pages
- Missing security headers without proven impact
- SPF/DMARC alone without exploitability
- Best-practice suggestions without a concrete vulnerability
- Vulnerabilities in third-party platforms we don’t control

12. Coordinated Disclosure & Embargo

- Do not publicly disclose until we confirm a fix or provide written permission.
- For critical issues affecting many users, we may request a reasonable embargo to allow safe rollout.

13. Communication & SLAs

- Acknowledgement: within 3 business days
- Status updates: weekly until closure
- Payouts: within 14 days of Resolved/Verified (see §14)

14. Payment Process

- Methods: USD via PayPal or ACH/wire (where available). We’ll confirm details during closure.
- Compliance: We may require tax forms (e.g., W-9/W-8BEN) and identity verification where applicable.
- Sanctions: We cannot pay individuals in embargoed/sanctioned regions or on restricted lists.
- Timing: Target within 14 days of closure once compliance steps are complete.
- Currency/fees: USD; fees or FX may be deducted by your provider.

15. Taxes

You are responsible for any taxes, fees, or reporting obligations related to your reward in your jurisdiction.

16. Legal Safe Harbor

I. If you follow this policy in good faith:
   - We will not pursue legal action for your research on in-scope assets.
   - If a third party raises a legal claim, we will clarify that your testing was authorized under this policy.

   This safe harbor does not cover actions that are malicious, cause harm, or break the law.

17. Privacy & Data Handling

- Do not store or share sensitive data obtained during testing beyond what's necessary for the report.
- Redact PII or secrets in screenshots/logs.
- Upon closure, securely delete any non-public data you accessed.

18. Program Changes & Termination

Skybriz may modify or pause this program at any time. Changes will not retroactively affect already accepted, valid submissions.

19. Contact

Report vulnerabilities to security@skybriz.com. For urgent, high-risk issues, use the subject line: "URGENT: Security Vulnerability".

20. Definitions (Simplified)

- Resolved: We've deployed a fix.
- Verified: We've confirmed the fix is effective and the issue is closed.
- Duplicate: Same root cause previously reported.
- Informational: Best-practice or low-impact note without a concrete vulnerability.

This document governs the Skybriz Security Research & Responsible Disclosure Program. Where conflicts exist between this and the website bounty page, this document prevails.

Last Updated: August 15, 2025