Internal Security Audit Report

Conducted on 03/03/2026 by the Cybersecurity team

1. Scope of the engagement

This audit was led by Emily Carter (emily.carter@example.com), at the request of the Chief Information Security Officer, Kevin Brooks, who can be reached at (646) 555-0187.

The audit covered the Riverside site, located at 4800 Harbor Drive, Oakland, CA 94607, United States.

2. Findings on digital access

Log analysis revealed the use of service account SVC-C781029EDB, with logins coming successively from IP addresses 47.196.149.159 and 110.22.94.189 within ten minutes, an anomaly that requires investigation.

An active API key was found in clear text in a configuration file: sk_test_2101b370d037c6fbdec396ef. An access token (tok_unh29fMPMkhKzWCHd2Twg4tZ3KTLJfIl) and a generic secret value (fAFaC5AaFd4d362AE550) were also stored unencrypted.

These items were revoked and regenerated on 05/22/2026 at 12:00 a.m. A new review is scheduled before 07/18/2028.

3. Related financial finding

During the same period, a corporate card transaction (4000 0446 3263 2113) was matched with bank routing number 021000021 and account 000987654321, although the expense had not been approved by management.

Finding	Severity	Status
API key in clear text	High	Fixed
Suspicious IP logins	Medium	Under investigation
Unapproved transaction	Medium	In progress

4. Conclusion

This report has been sent to Kevin Brooks for action. Any questions may be sent to Emily Carter at emily.carter@example.com.