Non-Negotiable SaaS Security Checklist

Use this checklist to confirm your SaaS app meets the five must-have security standards before the next release or audit. Tick each box as you verify the control is in place.

1. End-to-End Encryption

- [ ] Force HTTPS everywhere with HSTS
- [ ] Encrypt data at rest with AES-256 or better
- [ ] Store secrets in a secure vault (e.g., HashiCorp Vault, AWS KMS)
- [ ] Implement per-tenant keys / BYOK (optional)

2. Compliance Audits & Certifications

- [ ] Maintain a current SOC 2 Type II report
- [ ] Track ISO 27001 control status
- [ ] Schedule annual external penetration tests
- [ ] Run quarterly internal policy reviews
- [ ] Use compliance automation (e.g., Vanta, Drata)

3. Authentication & Access Controls

- [ ] Mandate MFA for every user and employee
- [ ] Apply RBAC with the principle of least privilege
- [ ] Provide SSO via a trusted IdP (Okta, Microsoft Entra)
- [ ] Enforce session timeouts & geo-velocity checks
- [ ] Automate secrets rotation

4. Incident Response Plan

- [ ] Document roles and escalation paths
- [ ] Enable 24/7 alerting (PagerDuty / Opsgenie)
- [ ] Run a tabletop drill at least twice a year
- [ ] Prepare a blameless post-mortem template

5. Continuous Monitoring & Threat Detection

- [ ] Centralize logs in a SIEM
- [ ] Enable cloud-native threat detection (GuardDuty, Defender)
- [ ] Automate dependency vulnerability scanning
- [ ] Review and triage alerts weekly or faster

Bonus Best Practices

- [ ] Integrate SAST / DAST into CI pipeline
- [ ] Deliver quarterly security awareness training
- [ ] Complete vendor risk assessments annually